# CYBER LAW IN UGANDA

First Edition


ISAAC CHRISTOPHER LUBOGO

7

# CYBER LAW IN UGANDA


*First Edition.*

ISAAC CHRISTOPHER LUBOGO

**COPYRIGHT © 2020 BY ISAAC CHRISTOPHER LUBOGO**

THE LAW OF SPORTS AND ENTERTAINMENT IN UGANDA

---

**First Printing Edition, 2021**
**ISBN: 978-9913-633-07-9**

The right of **Isaac Christopher Lubogo** to be identified as the author of this book has been asserted by him in accordance with the Copy right, Designs and Patents Act 1988.

**All rights reserved.** No part of this publication may be reproduced or transmitted in whole or in part in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without permission in writing from the author.

---

**Printed by:**
JESCHO PUBLISHING HOUSE

**A member of Jescho Group Ltd**
Maria's Galleria, Level 3 Room 17,
Luwum Street,
Kampala (U), East Africa.
**Tel:** +256 414 660 286, +256 782 395 293,
+256 702 055 211, +256 752 055 211
**E-mail:**jeschogroupltd@gmail.com
**Website:** www.jeschogroupltd.co.ug

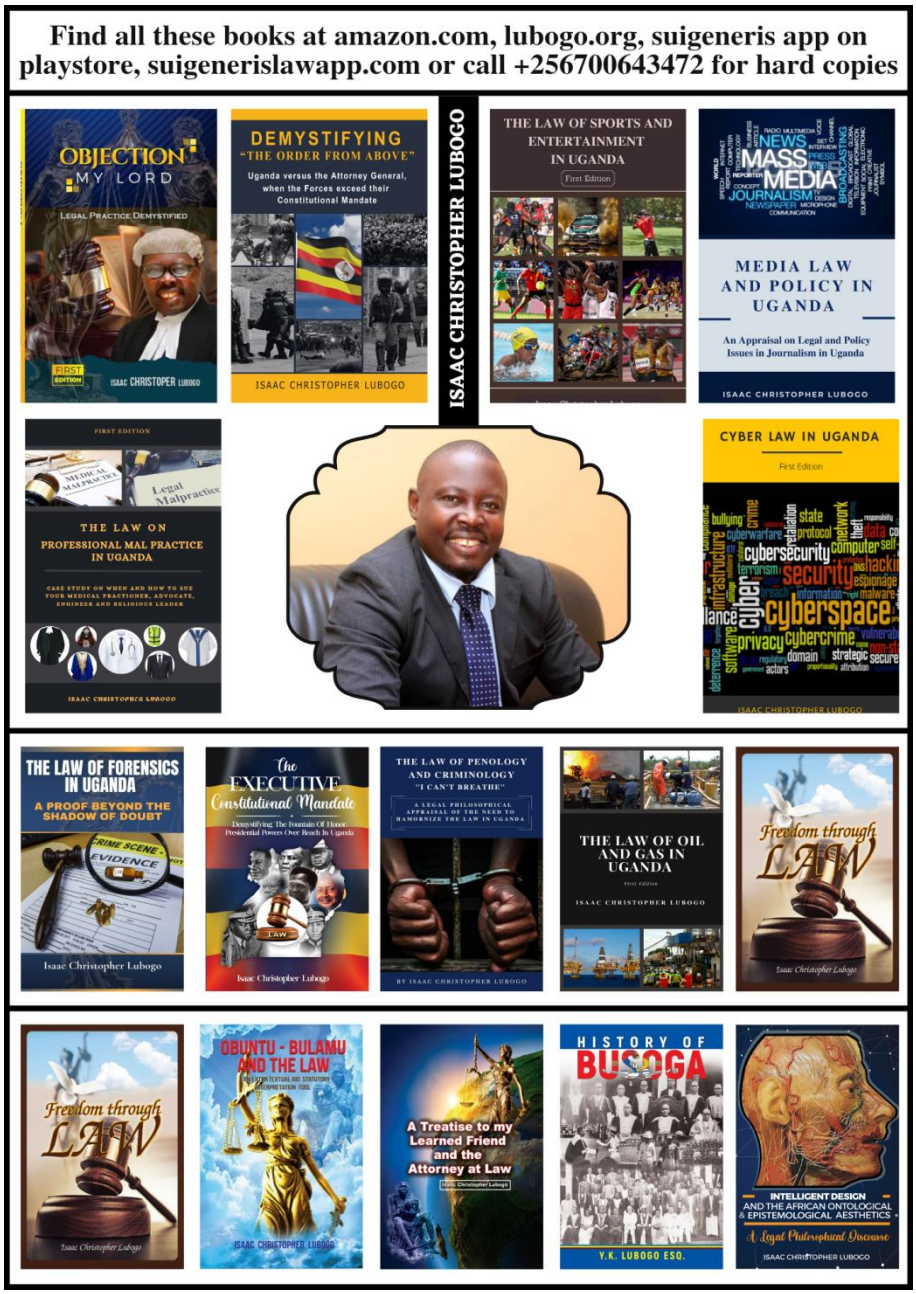
---

First Printed in the Uganda

**Find more books from this author at this website (https://www.lubogo.org)**

# TABLE OF CONTENTS

# DEDICATION


Find all these books at amazon.com, lubogo.org, suigeneris app on playstore, suigenerislawapp.com or call +256700643472 for hard copies
ISAAC CHRISTOPHER LUBOGO
OBJECTION MY LORD
LEGAL PRACTICE DEMYSTIFIED
ISAAC CHRISTOPER LUBOGO
DEMYSTIFYING "THE ORDER FROM ABOVE"
Uganda versus the Attorney General, when the Forces exceed their Constitutional Mandate
ISAAC CHRISTOPHER LUBOGO
THE LAW OF SPORTS AND ENTERTAINMENT IN UGANDA
First Edition
MASS MEDIA
JOURNALISM
MEDIA LAW AND POLICY IN UGANDA
An Appraisal on Legal and Policy Issues in Journalism in Uganda
ISAAC CHRISTOPHER LUBOGO
FIRST EDITION
Legal Malpractice
THE LAW ON PROFESSIONAL MAL PRACTICE IN UGANDA
CASE STUDY ON WHEN AND HOW TO SUE YOUR MEDICAL PRACTIONER, ADVOCATE, ENGINEER AND RELIGIOUS LEADER
ISAAC CHRISTOPHER LUBOGO
CYBER LAW IN UGANDA
First Edition
cybersecurity
cyberspace
cybercrime
privacy
ISAAC CHRISTOPHER LUBOGO
THE LAW OF FORENSICS IN UGANDA
A PROOF BEYOND THE SHADOW OF DOUBT
CRIME SCENE
EVIDENCE
Isaac Christopher Lubogo
The EXECUTIVE Constitutional Mandate
Isaac Christopher Lubogo
THE LAW OF PENOLOGY AND CRIMINOLOGY "I CAN'T BREATHE"
A LEGAL PHILOSOPHICAL APPRAISAL OF THE NEED TO HARMONIZE THE LAW IN UGANDA
BY ISAAC CHRISTOPHER LUBOGO
THE LAW OF OIL AND GAS IN UGANDA
ISAAC CHRISTOPHER LUBOGO
Freedom through LAW
Isaac Christopher Lubogo
Freedom through LAW
Isaac Christopher Lubogo
OBUNTU - BULAMU AND THE LAW
ISAAC CHRISTOPHER LUBOGO
A Treatise to my Learned Friend and the Attorney at Law
HISTORY OF BUSOGA
Y.K. LUBOGO ESQ.
INTELLIGENT DESIGN AND THE AFRICAN ONTOLOGICAL & EPISTEMOLOGICAL AESTHETICS
A Legal Philosophical Discourse
ISAAC CHRISTOPHER LUBOGO


10101
010

CHAPTER 01

# GENERAL INTRODUCTION TO ICT LAW / CYBER LAW

Cyber law is the law governing the internet and all digital transactions carried out thereon. Cyber law is indeed one of the novel areas of the legal system. This is because internet technology develops at such a rapid pace. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet. Cyber Law has also been referred to as the "law of the internet.[1]

Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law has been referred to as the Law of the Internet.

Information technology law provides the legal framework for collecting, storing, and disseminating electronic information in the global marketplace. Hence, Cyber law can be considered as a part of the overall legal system that deals with the Internet, E-commerce, digital contracts, electronic evidence, cyberspace, and

[1]https://www.upcounsel.com/cyber-law

their respective legal issues. Attorneys practicing in this area of the law represent individuals and businesses from all different industries. They help structure information technology transactions in a way that maximizes the client's economic benefit while ensuring regulatory compliance. A great deal of emphasis is also placed on anticipating potential sources of dispute between the parties to a transaction, and crafting agreements that address these concerns, thereby reducing the risk of litigation.

# ICT / CYBER LAW AREAS

The main coverage of ICT contracts relates to;

1. **Information** – (or data) in paper or electronic format.
2. **Communication** – in person or electronically (electronic communications), in writing or voice, telecommunications, and broadcasting.
3. **Information technology (IT)** – including software, hardware and electronics.
4. **Communications technology** – including protocols, software and hardware.

ICT law includes contentious and non-contentious matters [2] also civil and criminal matters. There is no single body of law which can be called ICT law. It is a distinct field of law that comprises elements of various branches of the law, originating under various acts or statutes of Parliament and the common law for instance; contract law, consumer protection law, criminal law, patent law, copyright law, trade mark law intellectual property law, banking law, privacy and data protection law, freedom of expression law, tax law, telecommunications law, work or labour law, the law of evidence

[2]https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286

# CYBER CRIME.

## *Categories of Cybercrime*

Categories of cybercrime are quite broad. Some of the examples can be explained as follow;[3]

**Fraud.**

With the prevalence of cyber technology, there is an increase in fraud and various acts that may constitute fraud. According to ***Kampala Bottlers v. Damanico***, fraud means actual fraud or some act of dishonesty. Constructive fraud may also arise through an unfortunate expression calculated towards misleading another for selfish gain. And one may opt to mislead, Consumers rely on cyber laws to protect them from online fraud. Laws exist to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face federal or state criminal charges. They might also face a civil action brought by a victim. Cyber lawyers work to both prosecute and defend against allegations of fraud using the internet.

**Copyright Infringement.**

According to ***Atal v. Kiruta t/a 97 Africa (CS 2004/967) [2009]***, a copyright is the exclusive right to do and to authorize others to do… certain acts in relation to literary, dramatic and musical works, in relation to artistic works and in relation to sound recordings, films, broadcasts, cable programs and published editions of works. The internet has made copyright violations easier. The early days of online communication made copyright violations as easy as clicking a button on a file-sharing website. Both individuals and companies need attorneys to bring actions to enforce copyright protections. Copyright infringement is an area of cyber law that defends the rights of individuals and companies to profit from their creative works. According to ***Sikuku V. Uganda Baati (HCCS (2012),*** the

[3]http://legalcareerpath.com/what-is-cyber-law/

main legislation under which a right arises over copyright infringement is in the Copyright and Neighboring Rights Act 2006.

**Defamation.**

As in ***Sembatya Kimbowa V. Editor, the Observer & 2 Ors,***the essence of defamation is *publication which excites others against the plaintiff to form adverse opinions or exposes him to hatred.*

Many people use the internet to speak their mind. When people use the internet to say things that are untrue, it can cross the line into defamation. Defamation laws are civil laws that protect individuals from untrue public statements that can hurt a business or someone's personal reputation. Defamation law is cyber law when people use the internet to make statements that violate civil laws.

**Harassment and Stalking.**

In domestic relations, to harass is legally defined as engaging in a certain pattern of conduct that induces fear of harm, annoyance and aggravation with the intention of inducing fear in a person[4]. Sometimes online statements can violate criminal laws that prohibit harassment and stalking. When a person makes repeated or threatening statements about someone else online, they may violate both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication. Any person who willfully, maliciously and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in a reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred twenty currency points *(shs.2,400,000)* or imprisonment not exceeding five years or both.

[4] Domestic Violence Act 2010 - section 2

**Freedom of Speech.**

An important area of cyber law is freedom of speech. Even though cyber laws prohibit certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. In addition, cyber lawyers may defend their clients when there's a debate about whether their actions constitute permissible free speech. Freedom of speech is guaranteed to Ugandans under **article 26 of the 1995 constitution**.

**Trade Secrets.**

Companies that do business online often rely on cyber law to protect their trade secrets. For example, Google and other online search engines spend a great deal of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber lawyers help their clients take legal action as necessary in order to protect their trade secrets.

**Contracts and Employment Law.**

Every time you click a button that says you agree to the terms and conditions of using a website, you've used cyber law. Contracts protect individuals and corporations as they use technology and do business online. For example, non-compete clauses in employment contracts used to impact only a small, local geographic area. As more business move online, the way lawyers draft these agreements and the way that courts enforce them may change. Lawyers must work to represent the best interests of their clients in areas of law that may still be unsettled.

Another area of cyber law may be domain disputes. When parties disagree about who owns or who should own a website, cyber lawyers may step in. Civil litigation may involve seeking monetary damages or an injunction to prevent.

# TRENDS OF CYBER LAW

Cyber law is increasing in importance every single year. This is because cybercrime is increasing. To fight these crimes, there have been recent trends in cyber law. These trends include the following'

New and more stringent regulations, Reinforcing current laws, Increased awareness of privacy issues, Cloud computing, How virtual currency might be vulnerable to crime, Usage of data analytics.

# SOURCES OF ICT LAW

Each country's legal system has its own sources of law, with greater weight placed on some sources than others. In developing an infrastructure project, it is important to identify which sources of law apply in the host country and their relative weighting. The following are the most common sources[5];

1. *Constitution*
2. *statutes*
3. *Judicial Decisions*
4. *Treaties*
5. *Other Source*

**Constitution**

In every country, the supreme law there is its constitution. A constitution can be described as a set of laws of a nation, state or social group that determine the powers and duties of government and guarantee certain rights to the people in it[6]. The Constitution may also set out basic principles, such as fundamental freedoms and rights. In Civil Law systems these rules are usually embodied in "Codes".

[5]https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/sources-of-law
[6] https://www.mariam

All but a very few countries have written constitutions where these fundamental rules can be easily identified (although their interpretation may be less straightforward). The remaining few have unwritten constitutions established by long-standing tradition.

A Constitution overrides any other source of law and it is usually highly difficult to amend. There may be a separate judicial court which considers constitutional issues, namely whether any law, regulation or administrative act is inconsistent with the Constitution and therefore void.

**Statutes**

Legislation is the second key source of law and usually takes priority over sources of law other than the Constitution. There may be more than one legislative body in a country - central, provincial or state and municipal authorities may each have separate power to legislate. Rules will determine the extent to which and in what areas one legislative body has priority over another.

Primary legislation may delegate powers to a particular ministry or regulator to prepare secondary legislation designed to supplement and develop the principles set out in the primary legislation. For example, tariff setting guidelines for a regulatory authority that is established by primary legislation may be set out in secondary legislation. Secondary legislation is usually not subject to full parliamentary scrutiny guidelines and so is faster to enact. However, it may be more difficult to identify than primary legislation as it may be recorded in subsidiary documents.

**Judicial Decisions**

In some countries including Uganda, judicial decisions are authoritative and develop into a source of law known as “case law”. Case law may extend the application of legislation and is deemed to form part of the law.

In other jurisdictions (mainly civil law jurisdictions) judicial decisions are formally only deemed to interpret the existing law and are not a binding source of law, although in practice they are often treated as authoritative.

**Treaties**

The host country may be subject (or may be about to become subject) to laws made by a regional or world grouping by becoming a signatory to a treaty. Examples are the laws of the European of Union, trade treaties, rules of the WTO and bilateral treaties. It is unlikely that a country could amend these rules easily.

An example of laws of a regional grouping is the body of regulations and directives of the European Union. Regulations have direct application in the respective member states legal systems and will take precedence over each member's national laws. Directives have to be adopted separately into law by each member state, but the member state must ensure consistency with the underlying EU directive. It is not just the current members that need to heed EU law. Countries seeking to accede to the EU (whether their accession has been formalized or not) need to take account of EU laws and the standards that they impose (particularly relevant to infrastructure).

Rules and guidelines may also be imported into law through treaty in relation to such matters as standards of engineering and health guidelines. For example, a country may adopt the World Health Organization's standards for drinking water.

**Other Sources**

There are a number of other sources of law that may be given greater or lesser weight in a particular country. These include;

1. writings of legal scholars - in civil law jurisdictions, academic writings interpreting the constitution or legislation have considerable influence on decisions of the courts;

2. edicts from a governor/ president

3. In the case of certain Islamic countries, "Sharia law" in the form of religious books and edicts from religious groupings.'

The Importance of Cyber Law

1. Just like any law, a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.[7]

2. Cyber law is vital because it touches almost all aspects of transactions and behavior on and concerning the Internet, the World Wide Web and Cyberspace. Primarily it may seem that Cyber laws is a very technical field and that it does not have any attitude to most activities in Cyberspace. But the actual fact is that nothing could be further than the truth. Whether we realize it or not, every work and every reaction in Cyberspace has some legal and Cyber legal perspectives.[8]

3. Companies are able to carry out electronic commerce using the legal infrastructure provided by the laws.

4. Digital signatures are given legal validity and sanction in the law.

5. The law, if specific throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

[7]https://www.computerhope.com/jargon/c/cyber-law.htm
[8]https://expertcyberlawyer.com/meaning-of-cyber-law-and-importance-of-cyber-law/ ; see also http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws

6. The law allows Government to issue notification on the web thus heralding e-governance.

7. The Act enables companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

8. The law also addresses the important issues of security, which are so critical to the success of electronic transactions. Thus far, the Electronic Signatures Act gives a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

9. The laws also provide for the possibility of corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the law is in the form of monetary damages.

CHAPTER 02

# THE EVOLUTION OF INTERNET AND THE LAW

In the **1960s**, during the Cold War, the US government saw the need for tracking all incoming flights into US airspace. They created 26 SAGE (Semi-Automatic Ground Environment) computer systems; these systems were distributed all over the USA and Canada. The SAGE computers were networked together and all aircraft could be tracked, no matter where they were in North America. Each SAGE computer was contained in a specialized building, which was the size of seven football fields.[14]

These networks had one crucial weakness: if one computer system was destroyed by enemy action, then the whole network would collapse and leave North America defenseless.

During this time, US defence agencies and universities were using different computer networks to store information. The idea was to join these computer networks together so that specialized information, about things like nuclear physics or the weather, could be stored in one university and the information could be shared with all the other linked organizations.

DARPA (Defence Advanced Research Projects Agency) were approached to find a solution to the problem of interconnecting networks, hence the phrase

Internet. This was termed the 'Internet Problem': how to get different computer networks, consisting of different hardware and software, and using different standards, all to talk to one another.

The resulting DARPA network was the ARPANET, the forerunner to all wide area networks (WAN).

Since the **1970s** the essence of the Internet has been against control and governance. It s very creators were working under the assumption that they were creating something that would exist outside of conventional control. Robert Kahn an Internet pioneer states that while he was working to develop his protocols for internet communication he was focusing on creating a system where individual networks could stand on their own, a system that was fault tolerant to the point that if a transmission or part of a transmission failed it would simply be resent from the source. He was trying to create a system that would have no global control (*Leiner et al., 2009)*. ARPANET was officially terminated in **1989** but by that time the Internet as we understand it today was just getting started (*Waldrop, nod.).* By the time the ARPANET died companies were incorporating TCP/IP into their products (*Leiner et al., 1997)*. As time passed computers, networks and the Internet have become more entangled in our everyday lives. Online shopping, gaming and communicating have become common place.

# DEFINITION OF THE INTERNET AND HOW IT WORKS

The Internet is a worldwide, publicly accessible network of interconnected computer networks that transmit data using the standard Internet Protocol (IP). It allows people to send and receive data wherever they are in the world if they have internet access. The internet is used for many different things such as:, Talking to friends-using programs and social media platforms such as msn and other social websites. Online shopping-buying items from the internet without leaving your home using online shopping sites, Watching Videos-using

websites, Research- using search engines, Downloading/listening to music. Internet Services

## *The World Wide Web*

The World Wide Web (WWW) is the most commonly used Internet service. Don't confuse the WWW with the Internet. The WWW is just one of the many services available on the Internet.

The WWW consists of millions of multimedia hyperlinked documents. Each multimedia document is called a web page. A website consists of a number of hyperlinked web pages, hosted on a web server. Web servers are capable of storing thousands of websites. The WWW allows the user to interact with a number of other web services. These include: business services, educational services, personal services.

**Business web services include;** e-commerce**,** e-banking**,** e-marketplace, business to business (B2B)**,** e-sale-government.

**Educational web services include:** edutainment, e-books, online courses, university research that student's use for studies and making research.

**Personal web services include;** computer games, news and weather**,** video on demand**,** web TV, webcast, music distribution, local services, search engines.

**Internet Governance** No one person, company, organization or government runs the Internet. It is a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body with each constituent network setting and enforcing its own policies. Its governance is conducted by a decentralized and international multi stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.[15]

Therefore, Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (the Information World Summit on the Information Society, 2005).

## DEVELOPMENT OF CORE INTERNET STANDARDS PLAYERS AND PROCESSES

Historically standards and governance act as a tool to aid in the development and advancement of systems and technology. A well-defined set of standards and a clear governance structure will help pave the way for new systems and technologies to be presented to the masses and be adopted which in turn will allow for more advancement and still more required governance. This system growth and governance is not limited to tangible goods and service. Telecommunications, networked computing and the Internet are not exceptions to this trend. Since the inception of networked computing governance and standardization have played a heavy role in the direction and development of what we now understand as the Internet. Since the early 1970's efforts have been made to provide governance to networked computing. In **1972 RFC 433** was published by Jon Postel pertaining to a unified process for the transmission of Registry Information (Socket Number Lists, 1972). Efforts of individuals like Jon helped spur the creation of numerous national, international, non-profit, for-profit, independent and government funded governing organizations specific to telecommunications and the Internet.

## INTERNATIONAL TELECOMMUNICATIONS UNION

The International Telecommunications Union (ITU) is the United Nations specialized agency for information and communication technologies ICTs.

The International Telecommunication Union (ITU) was founded in 1865 in Paris as the International Telegraph Union. The 1932 Madrid Plenipotentiary Conference decided the current name, which came into force on 1 January 1934. The ITU is an inter-governmental organization that brings together governments and industry to coordinate the establishment and operation of global telecommunication networks and services of the Union.

1. Extend international cooperation among Member States for the improvement and rational use of telecommunications of all kinds.

2. Promote and enhance participation of entities and organizations in the activities of the Union and foster cooperation and partnership between them and Member States.

3. Promote and offer technical assistance to developing countries in telecommunications.

4. Promote the development of technical facilities and their most efficient operation.

5. Promote the extension of the benefits of information and communication technologies to all the world's inhabitants.

6. Promote the use of telecommunication services with the aim of facilitating peaceful relations.

7. Harmonise the actions of Member States and promote cooperation and partnership between Member States and sector members.

8. Promote internationally a broader approach to telecommunications issues by cooperating with other inter-governmental organisations and those non-governmental organizations concerned with telecommunications.

The Union pursues its objectives by means of:

1. Promoting international cooperation in the delivery of technical assistance to developing countries.

2. Policy papers and reports designed to provide a focus on topics of current interest the regulators, policy-makers and the broader ITU membership.

3. Global coordination of radio frequency spectrum usage and orbital satellite positions, and the adoption of international regulations and treaties governing all uses of the frequency spectrum within which countries frame their national legislation.

4. Adopting technical standards that foster global inter-connectivity and inter-operability with as low rates as possible, consistent with efficient service.

5. Policy advice and technical assistance to developing countries.

6. Measures for ensuring the safety of life, particularly in the aftermath of natural disasters

7. Promoting preferential and favorable lines of credit for the development of social projects aimed at extending telecommunication services to the most isolated areas.

## *The Union's Current Areas of Focus*

1. Developing infrastructure for information and communication technologies (ICTs) to connect under-served and remote communities. Building cyber security and confidence in online transactions with a focus on protecting children online.

2. Promoting ICTs as an aid to combat climate change

3. Strengthening emergency telecommunications

4. Facilitating implementation of the outcomes of the World Summit on the Information Society.

It allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide.

ITU is committed to connecting all the world's people wherever they live and whatever their means. Through our work, we protect and support everyone's fundamental right to communicate.

# INTERNATIONAL ELECTRO TECHNICAL COMMISSION

The IEC was founded in **1906.** It is the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies. These are known collectively as "electro technology"

IEC provides a platform to companies, industries and governments for meeting, discussing and developing the International Standards they require.

All IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in IEC work. Every member country, no matter how large or small, has one vote and a say in what goes into an IEC International Standard.

The International Electro technical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

Close to 20 000 experts from industry, commerce, government, test and research labs, academia and consumer groups participate in IEC Standardization work.

# GLOBAL RELEVANCY

The IEC is one of three global sister organizations (IEC, ISO, ITU) that develop International Standards for the world.

When appropriate, IEC cooperates with ISO (International Organization for Standardization) or ITU (International Telecommunication Union) to ensure that International Standards fit together seamlessly and complement each other. Joint committees ensure that International Standards combine all relevant knowledge of experts working in related areas.

# THE INTERNATIONAL STANDARDS ORGANIZATION

The International Organization for Standardization (IOS) is a voluntary, non-treaty federation of standards setting bodies of 162 countries. Founded in 1946-47 in Geneva as a UN agency, it promotes development of standardization and related activities to facilitate international trade in goods and services, and cooperation on economic, intellectual, scientific, and technological aspects. ISO covers standardization in all fields including computers and data communications, but excluding electrical and electronic engineering (governed by the International Electro technical Commission or IEC) and telecommunications (governed by International Telecommunications Union's Telecommunications Standards Sector or ITU-TSS)

ISO explains its name by stating, “Because ‘International Organization for Standardization’ would have different acronyms in different languages (IOS in English, OIN in French for Organization internationale de normalisation), The founders decided to give it the short form ISO. ISO is derived from the Greek isos, meaning equal. Whatever the country, whatever the language, we are always ISO.” (ISO, Website: http://www.iso.org/iso/home/about.html)

ISO’s members are a network of national standards bodies for which there is one per country and the body represents ISO in its country. Individuals or companies cannot be members of ISO. Examples of national standards bodies include the American National Standards Institute (ANSI), the Standards Council of Canada

(SCC), and the British Standards Institute (BSI). ISO's members are involved in the operation of ISO through a once a year "General Assembly" which is managed by ISO's Secretary General and ISO's staff of more than 150 full time employees. Day to day operations are also managed from the Geneva office. Additionally ISO's members are active in the operations of ISO by serving on Technical Committees who are developing standards as well as on governance committees.

ISO International Standards provide specifications for products, services, systems and persons and are designed to ensure quality, safety and efficiency. By having standards, international trade is facilitated. When a standard is developed, an organization can choose to voluntarily use the standards or, in some cases, can choose to be certified as meeting the standard. Certification of products, services, systems and persons are conducted by certification bodies also known as conformity assessment bodies.

ISO has a conformity assessment committee (CASCO) that develops standards and addresses issues related to conformity assessment. Conformity assessment is a set of processes that demonstrate that a product, service or system meets the requirements of a standard. It is basically comparing the organization against the standard. ISO CASCO develops conformity assessment policy and publishes conformity assessment standards.

You can identify a conformity assessment standard because it starts with the number 17. ISO/IEC 17024 Conformity assessment General requirements for bodies operating certification of persons is an example of an ISO CASCO standard. ISO/IEC 17024 is a conformity assessment standard that contains requirements for Certification Bodies that certify the competence of people. Similarly ISO/IEC 17011 Conformity assessment General requirements for accreditation bodies accrediting conformity assessment bodies is a conformity assessment standard that contains requirements for bodies that accredit conformity assessment bodies. Examples of accrediting bodies are the ANSI, the SCC, and the United Kingdom Accreditation Services (UKAS).

ISO CASCO also has several policy committees including the;

1. Chairman's Policy and Coordination Group (CPC) which coordinates the technical work of CASCO and assists the CASCO Chair in identifying strategic conformity assessment issues.

2. Technical Interface Group (TIG) which liaises with other ISO technical committees (TCs) in order to ensure a consistent and harmonized approach to conformity assessment in those TCs, and

3. Strategic Alliance and Regulatory Group (STAR) which provides a forum for industry sectors and regulators to interact with CASCO.

The standards activities of ISO and ISO CASCO are designed to promote international standards to ensure that products and services are safe, reliable and of good quality. ISO standards reduce costs by minimizing waste and errors and increasing productivity. And ISO standards help companies to access new markets, level the playing field for developing countries and facilitate free and fair global trade.

Participation in International Standards provides opportunities for Personnel Certification Bodies to develop certification programs that meet international standards and facilitates their movement to other countries.

## INSTITUTE FOR ELECTRICAL AND ELECTRONICS ENGINEERS

The Institute of Electrical and Electronics Engineers, Inc (IEEE) is the world's largest technical professional association with more than 423,000 members in 160 countries.[24] It is a non-profit organization that is dedicated to advancing the theory and application of electrical and electronics engineering and computer science. Through its members, the IEEE is a leading authority on areas ranging from aerospace, computers, and telecommunications to biomedicine, electric power, and consumer electronics.

The IEEE has served electrical and electronics engineers and scientists since 1884, when a group of inventors and entrepreneurs including Thomas Edison

and Alexander Graham Bell founded the American Institute of Electrical Engineers (AIEE). In **1912** radio technology practitioners formed a separate international society, the Institute of Radio Engineers (IRE). In **1963** the AIEE and IRE merged to form the IEEE.

Today, the IEEE produces nearly 30 percent of the world's literature in the electrical, electronics, and computer engineering fields, and sponsors or cosponsors more than 300 technical conferences each year. It also has produced 900 active industry standards, more than one third of which influence the information technology and computer industries.

The IEEE consists of 300 local sections and 1,200 student chapters as well as 40 societies and councils that cover a wide range of technical interest areas. The largest of the institute's societies is the IEEE Computer Society.

## THE IEEE COMPUTER SOCIETY

Tracing its origins back to **1946**, the Computer Society is the leading provider of technical information and services to the world's computing professionals. The society's mission is to advance computer and information processing science and technology; promote professional interaction; and keep members up-to-date on the latest developments.

The Institute of Electrical and Electronics Engineers, Inc. (IEEE) is the world's largest technical professional association with more than 350,000 members in 150 countries. It is a non-profit organization that is dedicated to advancing the theory and application of electrical and electronics engineering and computer science. Through its members, the IEEE is a leading authority on areas ranging from aerospace, computers, and telecommunications to biomedicine, electric power, and consumer electronics.

The IEEE has served electrical and electronics engineers and scientists since 1884, when a group of inventors and entrepreneurs including Thomas Edison and Alexander Graham Bell founded the American Institute of Electrical Engineers (AIEE). In 1912 radio technology practitioners formed a separate

international society, the Institute of Radio Engineers (IRE). In 1963 the AIEE and IRE merged to form the IEEE.

Today, the IEEE produces nearly 30 percent of the world's literature in the electrical, electronics, and computer engineering fields, and sponsors or cosponsors more than 300 technical conferences each year. It also has produced 900 active industry standards, more than one third of which influence the information technology and computer industries.

The IEEE consists of 300 local sections and 1,200 student chapters as well as 40 societies and councils that cover a wide range of technical interest areas. The largest of the institute's societies is the IEEE Computer Society.

## REPORT ADVERTISEMENT.

The growth of the IEEE Computer Society mirrors the growth of the computing profession. Society membership has expanded from less than 10,000 in the **1950s t**o more than 100,000 in 2002. About 60 percent of these members work in industry, with the rest in government and academia. They include computer scientists, computer engineers, electrical engineers, information scientists, software engineers, information technology managers, and practitioners in emerging classifications. Students comprise about 10 percent of the membership. With 41 percent of its constituents living outside of the United States, the society is truly a global organization.

To serve the profession, the Computer Society supports a variety of activities. It publishes a wide array of magazines and archival transactions and delivers more than 15,000 editorial pages in 20 titles every year. The society also is a leading publisher of conference proceedings, which contain peer-reviewed papers containing the latest technical information. These proceedings stem from the many technical workshops, symposia, and conferences the society sponsors or cosponsors each year. Additionally, more than 30 technical committees in specialty areas organize meetings, produce newsletters, and provide networking opportunities for Computer Society members.

# SOCIETY FUNCTIONS

The society is a leader in developing standards for the computing industry, supporting more than 200 standards development groups in twelve major technical areas. Among these standards are wireless networking, web page engineering, and software engineering. IEEE standards are widely adopted by industry to assure consistent operability and functionality. One example is the IEEE 1012 Software Verification and Validation standard, which, among other uses, helps to ensure airplane and nuclear power plant safety and provide consistent performance of cell phones, beepers, and video games.

In addition to these activities, the society develops curriculum recommendations for programs in computer science and engineering and related disciplines. The society has supported the major computer science accreditation board in the United States and has participated in international accreditation efforts.

# INTERNET ARCHITECTURE BOARD

The origin of today's IAB lies in the Internet Configuration Control Board (ICCB), which was created in **1979 by Vint Cerf**, at that time program manager at DARPA, to advise him on technical issues. The ICCB was chaired by David Clark, MIT.[26] The Internet Architecture Board (IAB) serves as a committee of the Internet Engineering Task Force (IETF) and as an advisory body of the Internet Society. IAB provides architectural oversight of IETF activities, oversight and appeal for the Internet Standards Process, as well as management for the IETF protocol parameter registries.

The IAB was originally called the Internet Activities Board, and it was set up in 1983, chaired by Dave Clark, back in the days when the Internet was still largely a research activity of the US Government. The early history of the IAB is hard to trace in detail from the public record, for a reason expressed clearly in the minutes of its meeting in **January 1990:** "The IAB decided that IAB meeting minutes will be published to the Internet community." The earlier minutes are not on the public record. A good snapshot of the IAB in 1990, and a short

history, are given in **RFC 1160**, written by Vint Cerf who was the second IAB Chair. He was followed in this post by Lyman Chapin and Christian Huitema. In any case, the **1980s a**re pre-history as far as the Internet is concerned, and this article concentrates on the present.

Today, the IAB consists of thirteen members. Of these, six are nominated each year by a nominating committee drawn from the Internet Engineering Task Force (IETF) for a two year term. This process is described in RFC 2727. The slate of nominees is then approved by the Board of Trustees of the Internet Society. The thirteenth member of the IAB is the IETF Chair. The Internet Research Task Force (IRTF) chair serves as an ex-officio member but cannot vote. Finally, the IAB has a volunteer Executive Director.

In addition, IAB meetings are attended by a representative of the Internet Society (ISOC) and of the RFC Editor, and by a liaison with the Internet Engineering Steering Group (IESG). The IAB elects its own Chair from among its twelve IETF-nominated members.

## MEETINGS OF IAB

Currently, the IAB holds two 90-minute business meetings via telephone conference each month. These meetings are the first and third Wednesday of each month, in the morning on the US West Coast. In addition, the IAB has a monthly two-hour technical chat at a similar time on the fourth Wednesday of the month. The time slots are periodically adjusted to be as convenient as possible for IAB members in the face of varying schedules and time zones.

In addition to conference calls, the IAB meets in person at the thrice-yearly IETF meetings. Typically, the IAB will meet Sunday from lunch through the afternoon and then Monday through Friday each morning for breakfast. Finally, the IAB holds a plenary session, at each IETF meeting, either alone or jointly with the IESG. During the plenary, any member of the IETF can address the IAB.

To understand what the IAB really does in its meetings, it is necessary to know that the detailed work of driving the Internet standards process is done by the IESG. Not only must individual members of the IESG, known as IETF Area Directors, oversee the work of all the working groups in their area, but the IESG as a group must approve all formal standards actions. This means approving the conversion of Internet Drafts into Proposed Standards, and subsequent steps towards full standardization. Since the last set of reforms of IETF process, in 1992-93, the IAB itself does not have to approve individual standards actions.

The IESG consists of a set of specialists in various technical areas, and IESG positions are filled from the IETF by looking for specialists. In contrast, the IAB members are not appointed as specialists, but rather as generalists with a good understanding all aspects of the Internet architecture. In a typical meeting, apart from routine business such as reviewing the IAB action list, we will try to discuss one or two strategic issues in some depth. The intention is to reach conclusions that can be passed on as guidance to the IESG, or turned into published statements, or simply passed directly to the relevant IETF working group.

## FUNCTIONS OF IAB

**The IAB is responsible for:**

1. Providing architectural oversight of Internet protocols and procedures
2. Liaising with other organizations on behalf of the Internet Engineering Task Force (IETF)
3. Reviewing appeals of the Internet standards process
4. Managing Internet standards documents (the RFC series) and protocol parameter value assignment
5. Confirming the Chair of the IETF and the IETF Area Directors
6. Selecting the Internet Research Task Force (IRTF) Chair

7. Acting as a source of advice and guidance to the Internet Society.

**In its work, the IAB strives to:**

1. Ensure that the Internet is a trusted medium of communication that provides a solid technical foundation for privacy and security, especially in light of pervasive surveillance,

2. Establish the technical direction for an Internet that will enable billions more people to connect, support the vision for an Internet of Things, and allow mobile networks to flourish, while keeping the core capabilities that have been a foundation of the Internet's success, and

3. Promote the technical evolution of an open Internet without special controls, especially those which hinder trust in the network.

# DOMAIN NAME AND ICCAN DOMAIN NAME

Each internet page has a unique address referred to as uniform resource locator. Protocol exists on the various parts of each uniform resource locator. Domain name is an identification string that defines a realm of administrative autonomy, authority or control within the internet. Domain names are centrally organized and registered and must be unique.

It is pertinent to note that the first commercial internet domain name was registered in 1985 in the name symbolic .com by symbolic inc. a computer systems firms in Cambridge Massachusetts.

Domain names are used in various networking contexts and for application of specific naming and addressing purposes. Therefore in general, domain name identifies a network it represents on internet protocol.

Internet protocol services such as personnel computer hosting a web site or any other service communicated via the internet. Domain names are formed by the rules and procedures of the Domain name system. Any name registered in the

Domain Name System is a domain name. The names are organized in subordinate levels. That is; the sub domains of the Domain name system.

## PURPOSE OF DOMAIN NAMES

Domain names serve to identify internet resources such as complete networks and services with a text based label that is easier to memorize than the numerical addresses used in the internet protocol. Domain names may represent entire collections of such resources or individual instances.

Domain names are also used as a simple identification label to indicate ownership or control of resource. That is the realm identifies used in the session initiation protocol the domain keys used to verify the domain name system domains in e-mail systems and in many other uniform resource identifiers.

Domain names establish unique identity. Organizations can choose a domain name that corresponds to their names thus helping internet users. .

## THE ROLE OF THE INTERNATIONAL CORPORATION FOR ASSIGNED NAMES AND NUMBERS / ICANN

The International Corporation for Assigned Names and Numbers ICANN is an international corporation responsible for coordinating the domain name system the internet protocol, generic top level domain names and also publishes the complete list of Top level Domain registrars.

**Overview**

The DNS is made up of many servers and databases which, through a series of lookups in various caches, configure Domain Names into IP Addresses. The Domain Name System is a distributed database arranged hierarchically; its purpose is to provide a layer of abstraction between Internet services (web, email, etc.) and the numeric addresses (IP addresses) used to uniquely identify any given machine on the Internet. The DNS associates a variety of information with the domain names assigned and, most importantly, translates the domain

names meaningful to humans into the numerical identifiers that locate the desired destination.

**How the DNS Works.**

The DNS makes it possible to assign domain names in a meaningful way to Internet resources as well as to users, regardless of the entity's location. As a result, the WWW hyperlinks remain consistent, even for mobile devices. A domain name is an easy way to remember an address, but that needs to be converted to its numerical, IP format.

Coordination across the Internet is maintained by means of a complex authoritative root system known as the Top Level Domain (TLD), as well as the DNS and other smaller name servers responsible for hosting individual domain information.

DNS includes three types of top-level domains: generic (gTLD), country code (ccTLD), and sponsored (sTLD). gTLDs include domains that could be obtained by anyone (.com, .info, .net, and .org). Since 2014 many other gTLDs have been added like .pub, .ngo, .sucks. sTLDs are limited to a specific group e.g .aero (for air-transport industry). For each domain, the DNS spreads the responsibility by mapping the domain names and assigning them into IP addresses, and vice-versa. This is accomplished through authoritative name servers which have been designated for each domain. Each authoritative name server is responsible for its own particular domain, but it has the authority to assign new authoritative name servers to any of its sub-domains. The DNS is able to store many types of information, even the mail server lists for a specific domain. The DNS is a core element which ensures the functionality of the Internet through its distributed keyword-based redirection service.

However, the DNS does not include security extensions, which was instead developed as DNSSEC.

**The Structure of a DNS**

The Domain Name System presents the following structure:

1. Domain space name: represented by tree of domain names with nodes and leaves
2. Domain name syntax: rules include in standards like RFC 1035, RFC 1123, and RFC 2181
3. Name server
4. Domain names Internationalized
5. DNS resolver: initiates the queries will finally lead to the complete translation (resolution) of the information.

## THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

ICANN was formed in **1998.** It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

**What is the domain name system?**

The domain name system, or DNS, is a system designed to make the Internet accessible to human beings. The main way computers that make up the Internet find one another is through a series of numbers, with each number (called an "IP address") correlating to a different device. However it is difficult for the human

mind to remember long lists of numbers so the DNS uses letters rather than numbers, and then links a precise series of letters with a precise series of numbers.

The end result is that ICANN's website can be found at "icann.org" rather than "192.0.32.7" – which is how computers on the network know it. One advantage to this system apart from making the network much easier to use for people is that a particular domain name does not have to be tied to one particular computer because the link between a particular domain and a particular IP address can be changed quickly and easily. This change will then be recognised by the entire Internet within 48 hours thanks to the constantly updating DNS infrastructure. The result is an extremely flexible system.

A domain name itself comprises two elements: before and after "the dot". The part to the right of the dot, such as "com", "net", "org" and so on, is known as a "top-level domain" or TLD. One company in each case (called a registry), is in charge of all domains ending with that particular TLD and has access to a full list of domains directly under that name, as well as the IP addresses with which those names are associated. The part before the dot is the domain name that you register and which is then used to provide online systems such as websites, email and so on. These domains are sold by a large number of "registrars", free to charge whatever they wish, although in each case they pay a set per- domain fee to the particular registry under whose name the domain is being registered.

ICANN draws up contracts with each registry*. It also runs an accreditation system for registrars. It is these contracts that provide a consistent and stable environment for the domain name system, and hence the Internet.

In summary then, the DNS provides an addressing system for the Internet so people can find particular websites. It is also the basis for email and many other online uses.

**What is ICANN's Role?**

As mentioned earlier, ICANN's role is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.

This is commonly termed "universal resolvability" and means that wherever you are on the network and hence the world – that you receive the same predictable results when you access the network. Without this, you could end up with an Internet that worked entirely differently depending on your location on the globe.

**How does ICANN make decisions?**

When it comes to making technical changes to the Internet, here is a simplified rundown of the process:

Any issue of concern or suggested changes to the existing network is typically raised within one of the supporting organizations (often following a report by one of the advisory committees), where it is discussed and a report produced which is then put out for public review. If the suggested changes impact on any other group within ICANN's system, that group also reviews the suggested changes and makes its views known. The result is then put out for public review a second time. At the end of that process, the ICANN Board is provided with a report outlining all the previous discussions and with a list of recommendations. The Board then discusses the matter and either approves the changes, approves some and rejects others, rejects all of them, or sends the issue back down to one of the supporting organisations to review, often with an explanation as to what the problems are that need to be resolved before it can be approved. The process is then rerun until all the different parts of ICANN can agree a compromise or the Board of Directors make a decision on a report it is presented with.

**How ICANN is held accountable?**

ICANN has external as well as internal accountabilities.

1. Externally, ICANN is an organization incorporated under the law of the State of California in the United States. That means ICANN must abide

by the laws of the United States and can be called to account by the judicial system i.e. ICANN can be taken to court.

2. ICANN is also a non-profit public benefit corporation and its directors are legally responsible for upholding their duties under corporation law.

Internally, ICANN is accountable to the community through:

1. Its bylaws
2. The representative composition of the ICANN Board from across the globe
3. An independent Nominating Committee that selects a majority of the voting Board members
4. Senior staff who must be elected annually by the Board
5. Three different dispute resolution procedures (Board reconsideration committee; Independent Review Panel; Ombudsman)

# INTERNET ASSIGNED NUMBERS AUTHORITY

The Internet Assigned Numbers Authority (IANA) is responsible for maintaining a collection of registries that are critical in ensuring global coordination of the DNS root zone, IP addressing, and other Internet protocol resources. Since 1997, this role has been performed by ICANN, under a contract awarded by the National Telecommunications and Information Administration (NTIA), an agency in the U.S. Department of Commerce.[38]

Hence IANA is an acronym for the Internet Assigned Numbers Authority, one of the Internet's oldest institutions. IANA is responsible for managing the root zone of the Domain Name System (DNS), coordinating global Internet Protocol (IP) address allocation, and managing IP numbering systems. Basically, they take care of maintaining and managing the technical functions that keep the Internet

running smoothly. The IANA registries fall into three categories, each of which relate to a specific function in the Internet infrastructure:

**IP Addresses**

The IANA includes the global registry for IPv4 and IPv6 addresses and Autonomous System Numbers (ASNs). These lists contain entries for all the IP address ranges and ASN blocks that are allocated for use on the Internet, as well as the Regional Internet Registry (RIR) to whom responsibility for these resources has been delegated. For instance, the entry for 185.0.0.0/8 points to the RIPE NCC as the responsible registry.

The IANA will make changes to the global IP address registries (such as allocating a block of IP address space to an RIR) according to policies developed and agreed on by the global community.

# POLICY-MAKING AND IANA

## DNS ROOT ZONE

The Domain Name System (DNS) is a hierarchical distributed database that links domain names such as www.ripe.net to an IP address, which is then used to send data between computers. This can be compared to a phone book.

IANA maintains the top level of this hierarchy, the DNS root zone, which contains pointers to where information about second level domains, such as .com, .net and .nl can be found.

## PROTOCOL PARAMETER

In order to make sure computers understand each other when communicating, certain numbers used in networking protocols need to have a globally unique meaning. These protocol parameters are defined as part of the technical protocol

standards produced by the IETF. The IANA maintains and publishes these registries, which can then be used by software makers to ensure stable and predictable communications.

Domain Name Dispute Resolution – UDRP, Trademarks and Beyond Abuse of Domain Names and the online dispute resolution

The highest institution responsible for the general management of the domain name system is the Internet Corporation for assigned Names and Numbers (ICANN).

## *Registration of the domain name*

The registration of these domain names is usually administered by the domain name registrars who sell their services to the public. A Fully qualified domain name that is completely specified with all labels in the hierarchy of the domain name system having no parts omitted. Traditionally, a fully qualified domain name ends in a dot (.) to denote the top of the domain name system tree.

Labels in the domain name system are case insensitive; that is they can be written in upper or lower case. But most usually they are in lower case. The registry is responsible for maintaining the data base of names registered within the top level domain it administers. The registry receives registration information from each domain name registrar authorized to assign names in the corresponding top level domain and publishes the information using a special service that is; the who is protocol.

Who is an internet protocol for users to find details of the owner of a domain name, an internet protocol address or an autonomous system number on the internet. It is a policy of ICANN and other domain name administrators to provide and maintain registers of domain name registrars and licensees.

Registries and registers usually charge an annual fees for the service of delegating a domain name to a user and providing a default set of name servers. Often this transaction is termed as sale or lease of the domain name and the

registration may sometimes be called an owner but no such legal relationship is actually associated with the transaction only the exclusive right to use the domain name. Interestingly to note is that once registered, each domain name is unique and so there can never be an identical domain name even in a different country.

# ABUSE OF DOMAIN NAME / DOMAIN NAME DISPUTE

Domain name disputes arise for a number of reasons but most especially due to the interests in each unique domain name. The common forms of abuse are majorly **cyber squatting, cyber piracy** and **typo squatting.**

## *Cyber squatting*

The term cyber squatting comes from a word squatting which means the physical taking over of tenements and refusing to move which leads to establishment of a possessory title. With regard to cyber law, squatting means Cyber squatting means registering a domain name identical to another well-known name with the purpose of getting an exorbitant fee for transfer.

Cyber squatting is therefore illegal and improper dishonesty action that can be accidental as observed in ***Pitman Training limited V Nominet***[9] or deliberate as seen in the case of ***Panavision International V Toeppen***[10]where the squatters / knowledgeable internet users made a grab for well-known word based corporation marks , symbols and logos due to ignorance about the domain name and significance of domain names. However, court held that both parties had a right to use pittman in their domain names. Cyber squatting take various forms

[9] 1997(EWHC) 367
[10] District California case 1997 EWHC Ch 367

and these include stealing a name, misspelling the name well aware that almost a similar domain name exists.[11]

**Cause of action.**

In bringing a cause of action, the plaintiff must prove that he had a distinctive registered domain name, and that the defendant has also obtained a name that is identical or similar with that of the plaintiff with intention of making profits.

### *Typo squatting.*

Typo squatting was defined in the case of ***Mantra Group Property v Tailly Property limited***[12]as the process into which some one mistypes a domain name into an internet browser such as internet explorer to attract the internet search engine that are programmed to pick up such misspellings. Such an act as observed in***Sydney Markets limited V Sydney Flower Market Property limited***[13]mislead the public.

**Cause of action.**

In bringing a cause of action, the plaintiff must prove that he had a distinctive registered domain name, and that the defendant has also obtained a name that is identical or similar with that of the plaintiff with intention of making profits.

## REMEDIES AVAILABLE TO THE COMPLAINT FOR ABUSE OF A DOMAIN NAME

The law did not have obvious remedy for abuse of domain name but currently courts have considered trademark infringement, misrepresentation, fraud, and the tort of passing in handling domain name disputes.

[11]Allan Davidson, Social media and electronic commerce law, 2012, Cambridge University Press page 294
[12] 2010) FCA 291
[13] 2002 FCA 124

# DISPUTE RESOLUTION

By 1990, ICANN was in need of a solution for the raising dispute resolution because even in court, it was expensive. Consequently in 1999 ICANN issued the **Uniform Domain Name Dispute Resolution Policy** as an alternative to legal proceedings before courts. Surprisingly the **Uniform Domain Name Dispute Resolution Policy** has become an international standard for resolving domain name disputes. The policy is intended to discourage abusive registrations.

Dispute proceedings on abuse of domain names are initiated by parties claiming trade mark or service mark rights. In lodging a cause of action, the complainant is required to demonstrate that the dispute domain name is identical or confusingly similar to theirs. The complainant must also prove that the registrant does not have a right or legitimate interest in the domain name and that the registrant has registered the domain name in bad faith.

When the matter is brought up before for abuse of domain name, the registrar will cancel, suspend or transfer the domain name. ICANN provides that domain name disputes must be resolved by agreement court action or arbitration.

# REGISTRATION AND USE IN BAD FAITH.

The UDRP rules provide for the meaning registration and use of a domain name in bad faith to include registering the name with the aim of selling, renting and transferring the domain name registration of the complainant , or registering the domain name to prevent the owner of the trademark from reflecting the mark in a corresponding domain name It also includes instances where the registrant has registered the domain name primarily to disrupting the business of the complainant and also instances where by using the domain name, enables the registrant to attract Internet users to his web site or other on-line location for commercial gains by creating a likelihood of confusion with the complainant's trade mark

In ***Mary Lynn Mondich and American Vintage Wine Biscuits Inc. V Big Daddy's Antiques*[14]*,*** the panel held that merely offering to sell the domain name to the owner of a trade mark is sufficient evidence of use and registration of the name in bad faith especially where the registrant claimed smore than any underlying costs. In the case of ***City Utilities V Ed Davidson,*** [15]and similarly in the case of ***Blue Cross And Blue Shield Association And Trigon Insurance Company V. Interactive Communications Inc***[16] it was held that where the complainant initiated transfer discussions and the registrant has no prior plans to sell the dominant name, the panel could not term that as bad faith. In the case of ***Telstra Corporation Limited V. Nuclear Marshmallows,***[17]it was held that It is bad faith where the registrant concealed its identity by operating under a false name.

# EVIDENCE OF LEGITIMATE INTERESTS

It is compulsory for the complainant of domain name abuse to prove that the registrant has no rights and interests in the domain name. Paragraph 4 of the UDRP sets out specific circumstances to assist the registrant in demonstrating legitimate rights and interests in the domain name. The title to the paragraph is clearly suggests that how to demonstrate your rights to and legitimate interests in the Domain name in responding to a complaint.

Under this, it provides circumstances under which the complainant can demonstrate his rights or legitimate interests. This is by proving that before the dispute, you used the domain name in good faith offering the good or services or that your organization or business is commonly known to have that business name and that you have trade mark or service mark rights to this effect. You must also prove that you are making a legitimate noncommercial gain to misleadingly divert consumers or tarnish trademarks or service marks at issue.

[14] WIPO Case No D2000-0004
[15]City utilities v ed davidson, wipo case no d2000-0004,
[16]Blue cross and blue shield association and trigon insurance company v interactive communications inc wipo case no d2000- 0788
[17]Telstra corporation limited v nuclear marshmallows , wipo case no d2000 -0003,[17]

In ***Libro Ag v NA Global Link***[18]**,**the registrant argued that the complainant's trade mark 'libro' is a common Spanish and Italian name for books. The registrant had actually registered it and obtained a domain name to establish online virtual book store and in fact that even the customers were redirected to restaurant. Com. It was held that mere assertion of making preparations to use the domain name for the bona-fide offering of goods is insufficient to demonstrate rights or legitimate interests.

In ***Bruce Springsteen V Jeff Burgar and Bruce Springsteen Club***[19]**,** both the complainant and the registrant had interest in the domain name. the registrant was Bruce Springteen club with Jeffer Burger at the point of contact. The panel described *Bruce Springteen* as the famous almost legendry recording artist and composer and that his name alone is recognized in almost all parts of the globe.

The panel in regard to the meaning of "commonly and known by " found that the use of the name Bruce Springteen Club would not give rise to the impression in the minds of internet users that the proprietor was effectively known as 'Bruce springteen "commonly recognized in that fashion. In regards to the meaning of commercial and fair use, it observed that Bruce Springteen when imputed into a search engine would yield thousand of his hits which would be apparent to the users that even the sites would be official and authorized and it is hard to infer from the conduct of the registrant was for commercial gain or misleadingly divert customers. The panel found that there was fair use since the conduct did not tarnish the common law rights of Bruce Springteen with the celebrity 1000.com websites.

# REMEDIES AVAILABLE TO THE COMPLAINT FOR ABUSE OF A DOMAIN NAME

The law did not have obvious remedy for abuse of domain name but currently courts have considered trademark infringement, misrepresentation, fraud, and

[18] WIPO Case No. D 2000-0186
[19] WIPO Case No. 2000-1532

the tort of passing off. However the law is now clear. It provides for cancellation of the domain name, or transfer of the domain name to the complainant.

UDRP decision is not final. The dissatisfied party has a right to redress in the competent court of any jurisdiction after or before the UDRP decision.

The decision Of UDRP can only be implemented after ICANN receiving satisfactory evidence of a resolution between the parties or evidence that trial was conducted.

## THE WIPO APPROACH

Following WIPO's recommendations, **ICANN** adopted the **Uniform Domain Name Dispute Resolution Policy on August 26, 1999. The UDRP** provides holders of trademark rights with an administrative mechanism for the efficient resolution of disputes arising out of bad faith registration and use by third parties of domain names corresponding to those trademark rights.

Under the **UDRP**, trademark owners may submit disputes arising from alleged abusive registration of domain names to a mandatory expedited administrative proceeding, by filing a complaint with an approved dispute resolution service provider (provider). For GTLDs these providers are accredited by ICANN, and for those CCTLDs that have voluntarily adopted the UDRP, the providers are accredited by the registration authority of the CCTLD in question.

## APPLICABLE TO ALL GTLDS AND CERTAIN CCTLDS

Pursuant to their accreditation agreement with ICANN, all **GTL**D registrars agree to abide by and implement the UDRP. Accordingly, the UDRP is applicable to the **GTLD**s .com, .net, .org, and to all more recently introduced **GTLDs.**

The UDRP is incorporated into the standard dispute resolution clause of all GTLD domain name registration agreements. On this basis, the registrant of a GTLD domain name must submit to any proceeding that is brought under the UDRP, regardless of whether the domain name registration was effected before the entry into force of the **UDRP.**

Apart from the GTLDs, certain CCTLDs have also adopted the UDRP on a voluntary basis.

## GLOBAL SCOPE

The UDRP is international in scope, in that it provides a single mechanism for resolving a domain name dispute regardless of where the registrar, the domain name registrant, or the complaining trademark owner is located.

## TIME AND COST EFFECTIVE

Compared to court litigation, the UDRP procedure is highly time and cost effective, especially in an international context. A domain name case filed with the WIPO Center is normally concluded within two months, involving one round of limited pleadings and using mostly online procedures. WIPO fees are fixed and moderate

## ENFORCEABLE DECISIONS

A key advantage of the UDRP procedure is the mandatory implementation of the resulting decisions. There are no international enforcement issues, as registrars are obliged to take the necessary steps to enforce any UDRP transfer decisions, subject to the losing party's right to file court proceedings and suspend the implementation of the decision.

**Transparent**

The UDRP process is transparent. The WIPO Center posts all disputed domain names, case status, case statistics and full-text of decisions on its web site. In addition, the WIPO Center's online Index of WIPO UDRP Panel Decisions, and its jurisprudential overview of key issues offer free and easy access to the jurisprudence developed under the UDRP.

**Without Prejudice to Court Adjudication**

Once a complainant initiates a UDRP proceeding, the registrant of a domain name must submit to the process. However, in line with its administrative character, the UDRP does not preclude the domain name registrant or the trademark holder from submitting the dispute to a court for independent resolution; either party may commence a lawsuit in court before, during, or after a UDRP proceeding. Paragraph 4(k) of the UDRP also allows a losing domain name registrant to challenge the administrative panel's decision by filing a lawsuit in a competent court and thereby suspend the implementation of the panel decision. Although parties retain this court option, in practice this is a rare occurrence. The WIPO Center maintains a selection of court orders and decisions in relation to the UDRP or specific UDRP cases at its web site.

**Who are the Parties in the UDRP Complainant?**

The complainant is any person or entity, claiming trademark or service mark rights, who initiates a complaint concerning a domain name registration in accordance with the UDRP The WIPO Center processes complaints from a wide array of complainants from around the world, ranging from large multinational corporations (e.g., BMW, Gucci, Tata, Microsoft, and Sony) to small- and medium- size enterprises and to individuals (e.g., Isabelle Adjani, Venus and Serena Williams, Isabel Preysler, Julia Roberts, and Michael Crichton).

**Respondent**

The respondent is the holder of the domain name registration against which a complaint is Under the terms of the domain name registration agreement, which the respondent entered into with the registrar, the respondent must participate in the UDRP proceeding. The UDRP Rules provide a twenty-day period for the respondent to file a response to a complaint brought against it under the UDRP. As with complainants in cases filed with the WIPO Center, respondents come from around the world.

**UDRP Procedure**

The UDRP as a Policy is given effect by the Rules for Uniform Domain Name Dispute Resolution Policy (UDRP Rules) and by the dispute resolution service provider's supplemental rules. The WIPO Center has developed the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (WIPO Supplemental Rules) which complement the UDRP and the UDRP Rules on a number of procedural issues.

**The Three UDRP Criteria**

The UDRP procedure is designed for domain name disputes that meet the following cumulative criteria (UDRP, paragraph 4(a)):

1. the domain name registered by the domain name registrar is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

2. the domain name registrant has no rights or legitimate interests in respect of the domain name in question; and

3. the domain name has been registered and is being used in bad faith.

**Paragraph 4(b) of the UDRP** provides non-exhaustive illustrations (e.g., the domain name has been registered primarily for the purpose of selling it to the trademark owner) which, if found to be present, should be considered as evidence of the registration and use of a domain name in bad faith. Similarly, **paragraph 4(c) of the UDRP** provides non- exhaustive illustrations of

circumstances (e.g., the domain name is used in connection with a bona fide offering of goods) which, if found to be present, should be considered as evidence of the respondent having rights or legitimate interests in the disputed domain name.

A search of the online Index of WIPO UDRP Panel Decisions allows parties and panelists to search decisions of previous panels to examine the facts and circumstances of the case in light of prior WIPO decisions. WIPO also makes available a jurisprudential overview of key issues.

# WORLD SUMMIT ON INFORMATION SOCIETY

The World Summit on Information Society (WSIS) is a unique two-phase United Nations (UN) summit that was initiated in order to create an evolving multi- stakeholder platform aimed at addressing the issues raised by information and communication technologies (ICTs) through a structured and inclusive approach at the national, regional and international levels. The goal of WSIS is to achieve a common vision, desire and commitment to build a people-centric, inclusive and development-oriented Information Society where everyone can create, access, utilize and share information. **The UN General Assembly Resolution 56/183 (21 December 2001**) endorsed the holding of the **World Summit on the Information Society (WSIS)** in two phases. The first phase took place in **Geneva** from **10 to 12 December 2003** and the second phase took place in Tunis, from **16 to 18 November** 2005. In 2003, the number of participants was 11,000 representing 175 countries and in 2005 the number of participants was more than 19,000 representing **174 countries**.

The Overall Review of the Implementation of the Implementation of the Outcomes of the World Summit on the Information Society was held by **UN General Assembly in 2015** that adopted Resolution A/70/125 calling for close alignment between the WSIS process and the **2030 Agenda for Sustainable Developmen**t, highlighting the crosscutting contribution of information and communications technology (ICT) to the Sustainable Development Goals (SDGs) and poverty eradication, and noting that access to information and

communications technologies has also become a development indicator and aspiration in and of itself.

# WSIS FORUM

Since 2005, and following **Para 109 and Para 110 of the Tunis Agenda for the Information Society a cluster of WSIS-**related events was held on an annual basis in Geneva. In **2009,** the cluster of WSIS- related events was re-branded as WSIS Forum. With time WSIS Forum has proven to be an efficient mechanism for multi-stakeholder implementation of WSIS Action Lines and cross-cutting commitments on gender equality, information exchange, knowledge creation, the sharing of best practices and continues to provide assistance in developing multi-stakeholder and public/private partnerships to achieve the sustainable development goals.

WSIS Forums are organized each year, hosted by the ITU, co-organized by ITU, UNESCO, UNCTAD and UNDP in close collaboration with all WSIS Action Line Facilitators/Co-Facilitators (UNDESA, FAO, UNEP, WHO, UN Women, WIPO, WFP, ILO, WMO, UN, ITC, UPU, UNODC, and UN Regional Commissions). In **2015, the UN General Assembly** Overall Review resolved to hold the WSIS Forum on the annual basis till **2025.** UNGA also called for close alignment between WSIS and SDG process.

Moreover on the occasion of the UNGA review heads of the UN Agencies decided that beyond 2015 WSIS Forum can serve as a key forum for discussing the role of ICTs as a means of implementation of the Sustainable Development Goals and targets, with due regard to the global mechanism for follow-up and review of the implementation of the **2030 Agenda for Sustainable Development**, as set out in General **Assembly resolution A/70/1.**

The WSIS-SDG Matrix developed by UN WSIS Action Line Facilitators serves as the mechanism to map, analyse and coordinate the implementation of WSIS Action Lines, and more specifically, ICTs as enablers and accelerators of the SDGs.

# INTERNET GOVERNANCE FORUM

The Internet Governance Forum (IGF) was established by **WSIS in 2005**; with the first global IGF held in Athens in **2006.** The IGF has no decision making powers and is intended to serve as a discussion space that gives developing countries the same opportunity as wealthier nations to engage in the debate on Internet governance. Its purpose is to provide a platform where new and ongoing issues of Internet governance can be frankly debated by stakeholders from civil society, the business and technical sectors, governments, and academia. Participation in the IGF is open to all interested participants and accreditation is free. Ultimately, the involvement of all stakeholders, from developed as well as developing countries, is necessary for the future development of the Internet. It brings about 1500-2200 participants from various stakeholder groups to discuss policy issues relating to the Internet such as understanding how to maximize Internet opportunities, identify emerging trends and address risks and challenges that arise. The IGF works closely with the Dynamic Coalition on Public Access in Libraries.

The global IGF is held annually, usually in the final quarter of the year. In 2015 the IGF took place in João Pessoa, Brazil. In 2016 IGF took place in Guadalajara, Mexico, December 6-9.

CHAPTER 03

# DEVELOPMENT OF ICT IN UGANDA

## HISTORICAL BACKGROUND

The history of ICTs in Uganda is a short but intense one. Uganda started embracing ICTs as part of its economic development strategy when the first mobile phone service came onto the Ugandan scene in December 1994. The telecom company Celtel, using the GSM 900 technology mainly targeted high end users like business people and the diplomatic community. The cost of owning and maintaining a mobile phone was so high that that having a car was estimated to be a cheaper undertaking. Owning a mobile phone was a status symbol.

Things began to change however, with the entry into the market, of the South African giant Mobile Telecommunications Network (MTN) in 1998. Calls became cheaper, and the network was extended to rural areas, going beyond Kampala as the hub for the mobile telephone industry. More players like Airtel, Warid and Zain entered the marked with more diversified products making communication even cheaper. More internet providers also came on the scene and the cost, while still one of the most expensive in the world, became much cheaper than before.

Since then, the ICT sector has grown rapidly. The industry Grew by 30.3% in the 2009/10 financial year accounting for 3.3% of the GDP. Over 50% of the population are subscribed to mobile phone service provider and the number of internet users increased from 2,475,812 in 2008 to 4,178,085 in 2010 (168% of growth). Millions own smart phones, a fact driving digital penetration even in the rural countryside. Internet users are estimated at 6.5million as of 2012, accounting for 18.5 percent of the country's population of 35 million. The increase in internet usage has been further fueled by the country's youth bulge. Uganda has the world's youngest population, with over 78% below 30 years. These are more embracing of ICTs than their older, and inevitably old school, parents.

The liberalization of the communication industry also led to an increase in FM radio stations which now number in hundreds and as a result up to 80 percent of all households especially in the countryside now rely on radio for news and information. The "Ebimeeza" (people's parliaments) call-in talk shows were popularized and people began to freely debate the most important political and social issues of the day. There also dozens of TV stations and a couple of daily newspapers serving different audiences in the country.

The explosion in ICTs was aided by friendly ICT policies which created an enabling environment for ICT entrepreneurs to blossom. The **National Information And Communication Technology Policy of 2003** was intended to help the government implement more successful long term national development programmes like the Poverty Eradication Action Plan (PEAP), the Plan for Modernization of Agriculture (PMA), and others, by ensuring that timely and relevant information is available at all levels of implementation.

The Ministry of Information and Communications was established in **June 2006** with a mandate of "providing strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy for the ICT sector".

Developments in ICTs have dramatically changed the way information is collected, stored, processed, disseminated and used, thus making it a powerful tool for modernization and development.

# BACKLASH

Inevitably however, the growth in ICTs also culminated into social, political and economic situations that were not equally desirable for all the stakeholders

The free discussions by ordinary people of social-political issues on several radio stations did not augur well for some in the government who decided to start clamping down on these discussions. *Ebimeeza* were banned by the Broadcasting Council in September 2009.

Radio and TV stations as well as newspapers that were deemed to "spread inflammatory material" were threatened and some were closed which forced others into self-censorship

Then came the explosion in Social Media growth. Millions of Ugandans are signed up on face book, twitter and many young elite activists are endlessly sharing their opinions on blogs across the internet. Social media today has continued expanding to see new platforms such as Instagram, snapchat, tik tok among others and Ugandans too have adopted the technology to develop their own social media apps. This is aided by the increasing ownership of smart phones that are replacing old, 'call-only' handsets that are now scorned as belonging to 'stone age'. Face book and Twitter were blocked by the government during the **2016 presidential election** over fears that people might announce premature results. similary today, face book remains under an indefinite ban by the president during the **2020 elections** due to the unwarranted closure of certain face book accounts belonging to top government figures, a thing which caused ***H.E. Yoweri K.Museveni*** to put a ban on face book for the whole nation.

Cybercrime is also increasing in Uganda. The country's Tax collecting body, The Uganda Revenue Authority (URA)'s systems were hacked into in **2013**

leading to an estimated sh2billion ($700,000) tax loss in vehicle registrations. The telecom giant MTN also lost sh15 billion (US$5.7million) in Mobile Money fraud, a scam made possible by insider collaboration. Many companies desist from reporting such crimes for fear of scaring away potential clients so it's possible the problem is more widespread than reported. Such crimes are complex and difficult to prosecute by a justice system to which they are a completely new development.

This has created a dilemma for the government; how to protect information users while not appearing to clamp down on freedom of information and expression the country's laws unabashedly support.

The government has so far failed to walk this fine line. Sweeping legislations have been put in place that are threatening the rights of individuals' constitutional rights to privacy and self-expression

The regulations put in place and their enforcement sometimes go beyond their mandate. In March 2012, the Government of Uganda tabled the Communications Regulatory Authority Bill, a major piece of legislation 'intended to consolidate and harmonise existing and overlapping laws'

Citing what it calls 'security ramifications of online activity that have begun to permeate the national consciousness' Government under the Ministry of Information and Communications Technology developed a National Information Security Strategy (2011) which aims at addressing security challenges that are envisaged in this era of technological advances.

Other laws that came before or at the heels of this strategy include: the Regulation of Interception of Communications (RIC), 2010, which parliament hurriedly passed in the aftermath of the July 2010 bomb attacks, and allows for interception of communications and possible intrusion into personal communications. It also requires telecom companies to collect customers' information, including name, address and identity number, and to take other measures to enable interception. A registration of all SIM card owners in Uganda exercise concluded on May 31, 2013, which made the monitoring easier.

As a matter of fact, an explosive report by the BBC last year stated that Uganda's government had been spying on the opposition and the media for years, using spying equipment supplied by a UK technology firm.

The **Anti-Terrorism Act No.14 of 2002** gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance. The scope of the interception and surveillance includes letters and postal packages, telephone calls, faxes, emails and other communications, as well monitoring meetings of any group of persons. Others powers include the surveillance (including electronic) of individual's movements and activities, and access to their bank accounts.

Older laws such as the **Anti-Terrorism Act (2002); Press and Journalist Act of 2000** and the **Regulation of the Interception of Communications Act of 2010** remain on the books to negate these freedoms. Since **2010,** a number of other restrictive laws have also been drafted such as the **Public Order Management Act(2013**) which seeks to regulate the conduct of public meetings as well as discussion of issues at such meetings and the **2010 Press and Journalists Amendment Bill** intended to enforce annual registration and licensing of newspapers by the statutory Media Council.

Even those laws exclusively focused on fighting cybercrime are suspiciously viewed by some due to the dubious language in which they are crafted:

The **Computer Misuse Act of 2010** is intended to "ensure the safety and security of electronic transactions and information systems and other related matters. The **Electronic Transaction Act 2011** is "to provide for the use, security, facilitation and regulation of electronic communications and transactions and to provide for related matters. The **Electronic Signatures Act, 2011** aims "to make provision for and to regulate the use of electronic signatures and to provide for other related matters"

It is those "other related matters" that analysts believe may in the end make these laws go beyond the limits of their jurisdiction, and negate some of the freedoms

enshrined in other government laws that guarantee peoples' freedoms to use and benefit from the country's ICTs revolution

Government therefore needs some self-restraint to avoid overzealousness in controlling people's enjoyment of the information age. The ICT industry in Uganda has a number of stakeholders who play different complementary roles. These include the Government that plays regulatory role, private sector that invests in technology and establishes ICT businesses, the donor community that supports the sector financially and technically, civil society and the media, while citizens consume and use the proceeds from the industry. A framework needs to be worked out to protect the stakeholder roles and promote positive interrelationships in the ICT ecosystem and thus increase the positive impact of ICTs in Uganda without harming the interests of any stakeholder.

# COMPUTER HARDWARE AND SOFTWARE

Every computer is made up of the hardware and the software component. In this part, we discuss the various components of a computer hardware and software. The hardware needed for Internet access is divided into two i.e. the client side and the server side.

## *Client side*

Strictly speaking, the client is the connection that links you to the network. However, most people think of themselves, or their computer, as the client. It is what you need to get online and 'surf the Net such as a *computer, a modem, a telephone line, Browser software, An Internet service provider.*

## *Computer*

The computer is needed to allow you to run the browser software and interact with the Internet. Accordingly, Computer Law relates to and crosses over with a

number of legal areas affecting the design and use of computers and software, and the transmission of data via physical media or across data networks.[20]

## *Modem*

A modem is a device, which converts the computer's digital code so that it can be sent along the telephone line. Standard telephone lines cannot send digital information. Instead, they send information by varying, or modulating, electrical voltages.

When information is received, the modem converts the voltage into digital code. Most modern computers have internal modems, which can be configured to run at different speeds. Modems modulate digital information and demodulate analogue information. Hence the name *modem*. Modems are a combination of digital-to-analogue converters and analogue-to-digital converters. Note that even broadband requires a modem.

## *Telephone line*

The telephone line links you to an Internet service provider (ISP). You might use a cable service at home, instead of a telephone line. The principle is much the same. Network Internet access generally uses dedicated cabling and/or wireless transmissions.

## *Internet service provider/ ISP*

An Internet Service Provider is an organization/company that will link you to the Internet. You will pay your ISP for this access. Some of the examples of ISPs

[20]https://www.hg.org/compute.html

include, **Datanet, MTN Uganda Ltd,Uganda Telecom Ltd Infocom, AFSAT Communications Uganda Ltd**

CHAPTER 04

# THE SOURCES OF CYBER LAWS IN UGANDA

The existence of cyber law is a necessary hindrance to one's freedom of speech and expression and has molded the digital discipline of Ugandans who have now had to melt their excitement over the digital era. Currently, actions that threaten the enjoyment of online freedoms and rights in Uganda are stemming from the existing cyber legal framework.[21] The Ugandan cyber legislation gives government and its agencies unlimited powers with regard to procuring surveillance equipment[22] and criminalizing gadgets (computers) as well as Internet content. Their powers range from illegally ordering Internet service providers to block certain social platforms[23] to signing secret memorandum of understanding among government agencies to share information about Internet

[21] See http://www.refworld.org/pdfid/549026360.pdf for an overview over the state of Internet freedom of Uganda in 2014.

[22] https://unwantedwitness.or.ug/the-unwanted-witness-uw-news-brief-state-house-is-procuringsurveillance-equipment/.

[23] See e.g. http://www.reuters.com/article/2011/04/19/us-uganda-unrest-media-Idustre73i3lp20110419 and http://www.article19.org/data/files/pdfs/reports/world-press-freedomday-no-frontiers-new-barriers.pdf.

users and published content in order to enforce the Ugandan cyber legislation.[24] Harassment of online activists by police has also been reported[25]

These developments prove the urgent need to contiguously analyze the regulation of the Internet in order for citizens to be able to exercise fundamental freedoms, to be empowered and able to change their lives through the Internet. Many citizens view the Internet as one of the remaining independent platforms where a decent and sound debate can take place and where ideas can be shared without political interference. According to the Uganda Communication Commission the number of Internet users is growing steadily. The number of Internet users was estimated to be more than 8.5 million in June 2014.

Against this background, surely analyzing the Ugandan cyber legal framework from a human rights perspective is an important undertaking. The principal purpose is to assess whether these provisions are compatible with international human rights standards on the freedom of expression and right to privacy. The second purpose is to support advocacy concerning Uganda's Internet freedoms.

The disposition of the analysis is the following: first the relevant international human rights standards regarding freedom of expression and right to privacy will be discussed Thereafter, relevant Ugandan cyber laws will be analyzed in the light of international human rights law. The laws will be analyzed in chronological order so that changes over time are made apparent. This approach will also allow for a contextual understanding of the challenges that Uganda faces today regarding freedom on the Internet. In the final chapter the most important findings of the analysis will be discussed and summarized. Recommendations will be put forward as to how Ugandan cyber laws can be made better compatible with the international human rights standards on freedom of expression and right to privacy in the digital environment.

[24]https://unwantedwitness.or.ug/uganda-police-signs-a-secret-mou-with-uganda-communicationcommission/.
[25]https://unwantedwitness.or.ug/police-is-harassing-an-online-activist-in-mid-western-uganda/ and

Securing access to the Internet for as many people as possible constitute an important part of Internet freedoms. The report will not deal with that particular question in detail. Instead it will focus on the analysis of legal restrictions that affect online freedoms of those who already have access to Internet.

Furthermore, the analysis will only focus on the provisions that are relevant to freedoms on the Internet. Other provisions that violate basic human rights but lack a direct connection to freedom on Internet are therefore not discussed in this report.

Provisions protecting freedom of expression and the right to privacy can be found in the majority of international human rights instruments. There are also international human rights standards that directly take aim at the protection of these rights in the digital environment. Not all of these standards are legally binding but can rather be seen as recommendations and soft law. Free speech and privacy guarantees in the international human rights instruments will be discussed in this chapter. Focus will primarily be on United Nations instruments of international scope. Thereafter relevant regional human rights instruments will be discussed. The legally nonbinding recommendations and guidelines with regard to Internet freedoms will also be discussed.

As regards the protection of an individual's private life, a difference can be made between the right to privacy and data protection rights. It is also important to keep in mind that there is not one universally recognized definition of these rights. Although privacy and data protection overlap to a great extent, there is for example a specific provision for data protection in the **European Union Charter of Fundamental Rights** alongside a provision protecting the respect for private and family life. Comprehensively defining "*privacy"* is a difficult, even close to an impossible, task. According to one definition, privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive

unsolicited intervention by other uninvited individuals.[26] When it comes to data protection rights, in the **Data Protection Directive of the EU (Directive 95/46/EC)** personal data is defined to mean any information relating to an identified or identifiable natural person. One of the key differences between these two rights lies in that not all information relating to an identified or identifiable person need to fall within the scope of privacy. This makes the scope of data protection broader than the scope of privacy.[27][28]

# THE LEGAL FRAMEWORK IN UGANDA

In this chapter, Ugandan cyber law provisions will be analyzed against the framework of international human rights law as described above. According to international law all restrictions of freedom of expression and right to privacy on the Internet must conform to the following three part test:

Restrictions must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and

Restrictions must pursue one of the purposes set out in **Article 19(3) of the Covenantion on Civil and political Rights**, namely **(i)** to protect the rights or reputations of others, or **(ii)** to protect national security or of public order, or of public health or morals (principle of legitimacy); and Restrictions must be necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).[29]

The provisions analyzed in the following are those, which can be seen to restrict the Internet freedom of Ugandan citizens by posing threats to freedom of expression and right to privacy in the digital environment.

---

[26] SR A/HRC/23/40 (22).

[27] See Kokott, J, & Sobotta, C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, 2013, Vol. 3, No. 4, p.

[28] . This article provides an interesting and more comprehensive discussion on the topic on the European leve.

[29] As summarised by the UN Special Rapporteur on Freedom of Expression (SR) in A/ HRC/17/27 (24).

In addition to the international human rights framework freedom of expression, freedom of information and right to privacy are also guaranteed in the **Constitution of the Republic of Uganda, 1995**. According to **Article 27 of the constitution**, no person shall be subjected to unlawful search of the person, home or other property of that person, or unlawful entry by others of the premises of that person.

Furthermore, no person shall be subjected to interference with the privacy of his or her home, correspondence, communication or other property. Freedom of expression is protected by **Article 29** where it is stated that every person shall have the right to freedom of speech and expression, which shall include freedom of the press and other media. As regards freedom of information, it is stipulated by **Article 41** that every citizen has a right of access to information in the possession of the State or any other organ or agency of the State except where the release of the information can put the security or sovereignty of the State at risk, or interfere with the right to the privacy of any other person. It is therefore important to bear in mind that these rights are not only protected through international human rights instruments but also within the framework of the Ugandan constitution. Thus their continued derogation is contrary to Uganda`s international human rights commitments.

## *The Anti-Terrorism Act, 2002*

The Anti-Terrorism Act (ATA) was adopted in **2002** and includes provisions that provide for obtaining information in respect of acts of terrorism. This includes the authorizing of the interception of the correspondence and the surveillance of persons suspected to be planning or to be involved in acts of terrorism.

**Section 9(1)** states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism or training or mobilizing any group of persons or recruiting persons for carrying out terrorism or mobilizing funds for the purpose of terrorism commits an offence and shall be liable on conviction, to

suffer death. It is further laid down in **Section 9(2) of the Anti Terrorism Act** that any person who, without establishing or running an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death.

It is asserted by the **UN Special Rapporteur** that states are required under international law to prohibit incitement to terrorism in national criminal law, but such provisions must comply with the requirements of prescription by unambiguous law; pursuance of a legitimate purpose; and respect for the principles of necessity and proportionality.[30] Furthermore, the Special Report has emphasized that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless it can be demonstrated that:

(a) The expression is intended to incite imminent violence;

(b) It is likely to incite such violence; and

(c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

What is exactly meant by promoting terrorism under **Anti Terrorism Act** is not defined in the law and there is hence a risk of the provision getting a too wide and arbitrary scope of application. It is also difficult for media and individuals to know which type of material is seen as promoting terrorism. It can thus be argued that the requirements under international law of unambiguous, predictable and transparent law are not fulfilled.

Publishing and disseminating material promoting terrorism can also result in an individual being convicted to the death penalty. According to the HRC, under no circumstances can an attack on a person, because of the exercise of his or her freedom of opinion or expression, including such forms of attack as arbitrary arrest, torture, threats to life and killing, be compatible with **Article 19.** It is

[30] SR, A/66/290 (81).

clear those disproportionate penalties on publishing and disseminating information of a type that is not clearly defined threatens the freedom of expression on Internet. That death penalty at all is applied in this context can in itself be seen as a serious infringement of the international human rights law.

Furthermore, the **Special Rapporteur** underlines that arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to that very right. This is due to it not only creating a "chilling effect", but also leading to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman or degrading treatment or punishment.

The interception of communications and surveillance within the framework of **Anti Terrorism Act is** regulated in its part IIV. The responsible minister may designate an authorized officer who has the right to intercept communications and otherwise conduct surveillance in respect of a person or a group or category of persons suspected of committing any offence under ATA. Interception of e-mails and electronic surveillance fall under the scope of surveillance allowed according to ATA. The purposes for which interception or surveillance may be conducted are: safeguarding the public interest, prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism, preventing or detecting the commission of any offence under ATA and safeguarding the national economy from terrorism (**Sections 18-19**). Obstructing an authorized officer can result in a prison sentence of maximum two years **(Section 20**). None of these grounds is defined within the framework of ATA, which opens up for considerable abuse of the interception and surveillance powers as these can be based on loose and vague grounds. There is no requirement of authorization, external control or review by an impartial and independent judge of any kind. Also these provisions of ATA can thus be seen to contravene the principles of international human rights law.

ATA has been criticized by **Amnesty International** in its report Stifling Dissent - **Restrictions on the Rights of Freedom of Expression and Peaceful**

**Assembly in Uganda.**[31]The overly board definitions of "terrorism", "aiding and abetting" to terrorism and the fact that "promoting terrorism" is not defined under ATA are seen to be able to inhibit media work and criminalize legitimate media coverage. Even the interception powers of the authorized officers are criticized as they could make it possible to intercept communications between journalists and their sources.[32]

ATA consequently contains both provisions that constitute a violation of right to privacy on the Internet by providing for interception of digital communications and provisions that threaten the freedom of expression on the Internet.

## *The National Information Technology Authority, Uganda Act, 2009*

This law establishes the **National Information Technology Authority in Uganda (NITA-U)**. It is a government agency under the general supervision of the minister responsible for information technology **(Section 3 (3) and Section 2**). The goals of the NITA-U listed in Section 4 include diverse ways to promote information technology in Uganda and most of these aims are commendable. The functions of the NITA-U listed in Section 5 are many (18) and rather broadly formulated. **Section 5 (18**) extends the functions of the authority to undertake any other activity necessary for the implementation of the objects of the authority.

**Functions of NITA.**

**Section 5 (3) of NITA act provides that NITA is** to co-ordinate, supervise and monitor the utilization of information technology in the public and private sectors,

[31] Stifling Dissent - Restrictions on the Rights of Freedom of Expression and Peaceful Assembly in Uganda, Amnesty International, November 2011, https://www.amnesty.org/en/documents/ AFR59/016/2011/en/.
[32] Ibid., p. 14.

**Section 5 (4);** - to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals

However a clear analysis of this provision opens up for the NITA-U to stipulate standards for hardware and software in public computers that can restrict freedom of expression and privacy. It could for example be interpreted to allow for regulations requiring installation of filters, blocking mechanisms or spyware in public computers.

**Section 5 (5) of the act provides that NITA is** to create and manage the national databank,

Analysis; its inputs and outputs what is meant by the national databank is not defined within the framework of the law and it is neither made clear what type of data it consists of. Nor is it explained what is the origin of the data stored in the data bank. It is thus unclear what type of data is collected in the national databank, who gathers the data, and who has the access to the data in the databank. This can mean both collecting and processing of personal data in a way that breaches the right to privacy. As the exact nature of the databank is not defined in the law and the character and origin of its data are unclear, there is a risk for personal data being processed in conflict with data protection principles. This could for example include collecting data based on individuals' behavior on the Internet or making personal data digitally searchable in a way that infringes the right to privacy.

**Section 5 (6) mandates NITA** to set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organization, sustenance, disposal, risk management, data protection, security and contingency planning

However, this provision grants the **NITA-U an** extensive power to set standards with regard to different aspects of utilization of information technology. Most of the issues can be seen to be related above all to the information technology infrastructure and access to Internet instead of the actual content. However,

above all the possibility to regulate data protection and security related to information technology can open up for restrictions on the Internet content.

**Part V of the NITA-**U regulates the information technology surveys and powers of the authority. With information technology survey is understood an operation in which enumerations, inspections, studies, examinations, reviews, inquiries or analyses are carried out to collect or gather information and data on matters related to information technology (**Section 2). Section 19 (1**) stipulates that the minister may, on the recommendation of the board[33] direct, by a statutory order, that an information technology survey be taken by the authority on both public and private sectors. In carrying out such a survey the authority has the power to collect information and data regarding information technology for the sector specified in the order. It may use summons and search warrants to facilitate the enforcement of such collections of data and information **(Section 19 (3) a-b).**

**Section 20 (1)** stipulates that where data or information on information technology is being collected in accordance with **Section 19,** the Executive Director, an officer of the Authority, or an authorized officer, may require any person to supply him or her with any particulars as may be prescribed, or any particulars as the Executive Director may consider necessary or desirable in relation to the collection of the information. Furthermore, a person who is required to give information under subsection (1), shall, to the best of his or her knowledge and belief provide all the necessary information, in the manner and within the time specified by the Executive Director **(Section 20(2)).** The powers of the authority are further expanded in Section 21, where it is stipulated that the staff of the Authority or an authorized officer may at all reasonable times enter and inspect any building or place and make such inquiries as may be necessary for the collection of information and data for a survey being carried out under **Section 19.** The right to enter a dwelling house is limited to the purposes of collecting information relating to information technology matters and for the exercise of functions under this Act.

[33] The Board of Directors appointed under Section 7 (Section 2). The Chairperson and the members of the Board are appointed by the Minister, with the approval of Cabinet (Section 7 (2).

It is further laid down in **Section 38(4)** that a person who for example hinders or obstructs the Executive Director, an officer of the Authority or an authorized officer in the lawful performance of any duties or in lawful exercise of any power imposed or conferred on him or her under NITA-U commits an offence. The same goes for a person who for example refuses or neglects to complete and supply, within the time specified for the purpose, the particulars required by the Authority in any return, form or other document, to answer any question or inquiries put to or made of him or her, under this Act. A person who commits such an offence is liable, on conviction, to a fine not exceeding twelve currency points or imprisonment not exceeding six months, or both.

**Analysis;** the scope of different purposes for which information technology surveys can be conducted is not clearly defined. It is however, expressly stated that they cover both the public and private sector. This combined with the far-reaching powers of entry and inspections means that it is difficult for individuals to foresee what kind of information might be of interest for the NITA-U and can thus end up as objects for inspection. This legislative framework can be seen to constitute a violation of privacy that is incompatible with the international human rights law as regards the requirement of predictable and transparent legal provisions.

**Section 22** stipulates that confidentiality is the main rule as regards for example data set or part of data stored in a computer or any other electronic media. However, this does not affect the fact that the NITA-U as a public authority has a possibility to get access to personal data concerning individuals.

According **to Section 34,** the Minister may, after consultation with the Executive Director and the Board, give NITA-U directions of a general nature. Such directions shall be in writing and relate to policy matters in the exercise of the functions of NITA-U. NITA-U shall comply with any direction given by the Minister. The particulars of any directions given by the Minister shall be included in the annual report of the Authority, together with the extent to which the directions were complied with. It is stipulated in Section 36 that The Board shall cause to be prepared and shall submit to the Minister within three months

after the end of each financial year, an annual report on the activities and operations of the Authority for that financial year. According to Section 37 The Minister shall in each financial year, submit to Parliament as soon as possible after receiving them, the Auditor General's report and the annual report of the Authority. This can be seen as the only means of external control in relation the Minister's actions in relation to the NITA-U. **Section 39** gives the Minister the power to, in consultation with the Board, make regulations generally for giving effect to the provisions of the act by statutory instrument. These regulations may prescribe, in contravention with the regulations, a prison sentence up to two years; three years in case of second of subsequent offence.

Analysis; These provisions can be seen to give the responsible minister wide powers, which also bring with itself a risk of misuse, as regards the functions of the authority. Although there is a certain parliamentary control involved in the form of annual report, the Minister still has possibility to for example stipulate offences resulting in prison sentence.

## *The Regulation of Interception of Communications Act, 2010./ RICA*

The **Regulations of Interception of Communications Act (RICA**) is probably the most problematic law when it comes to guaranteeing the Internet freedom of Ugandan citizens. **Section 3 of RICA** provides for the establishment of a Monitoring Centre for the interception of communications under the act. The minister responsible for security is mainly responsible for establishing and running the centre.

An application for the lawful interception of any communication may be made by the Chief of Defence Forces, the Director General of the External Security Organization, the Director General of the Internal Security Organization, the Inspector General of Police or their nominees (**Section 4 (1)),** also referred to as authorized persons **(Section 1).** A warrant to intercept communications shall be issued by a designated judge, by which is understood a judge designated by the

Chief Justice to perform the functions of a designated judge for purposes of **RICA (Section 1).**

**Section 5** lists the grounds on which the designated judge may issue a warrant to an authorized person. Although the interests that allow for issuing of a warrant can generally be seen as legitimate, the level of evidence the authorized persons are required to show is not higher than reasonable grounds for the designated judge to believe that a legitimate interest it at hand. It is thus a very low level of evidence that is required for a designated judge to be able issue a warrant under RICA. This naturally opens up for abuse of both the power to apply for and to issue warrants. Neither are there any more specific requirements of impartiality, independence or competence stipulated when designating the responsible judge, the decision is thus completely left to the discretion of the Chief Justice. When it comes to the actual grounds that make it legitimate to issue a warrant to intercept communications, it is the gathering information for any actual or potential threat concerning any national economic interest **(Section 5 (c-d)**) that is the most problematic provision. What is meant by a national economic interest is not defined within the framework of RICA and it can thus be loosely interpreted to mean many different things. It can therefore be seen to conflict with the requirement of transparency and unambiguous legislation in international human rights law. Combined with the low requirement of evidence and the lack of requirements of objectivity and impartiality with regard to the designated judge, this point can above all render possible the abuse of the power to intercept communications. The lack of requirement of objectivity and impartiality as regards the designated judges can above all constitute a threat by making judges economically corruptible.

When it comes to service providers, they are required under **Section 8 to** ensure that they have installed relevant equipment with capability to enable the interception of communications. A failure to do this can result in a prison sentence up to five years. This can be seen to threaten both privacy and freedom of expression on the Internet as service providers are with the threat of criminal sanctions forced to take into account the state's interests, not the individuals' interest to be able to enjoy their human rights. The balancing of interests made

my legislator is thus clearly tipped in favour of the national interests instead of the individual rights. Combined with the vague grounds for interception and the discretion of the judges, can this balance of interests on the whole be seen to constitute a disproportionate infringement of an individual's privacy.

Telecommunications service providers also have a duty to ensure that subscribers register their SIM-cards and provide service provides with comprehensive information about e.g. their identity and address (**Section 9).** This requirement of SIM-card registration can be seen to gravely undermine the Internet freedom of those who choose to use their mobile phones to surf on the web, as it is possible to directly connect their online activities to their identities. There are consequently provisions requiring service providers to enable the interception of communications in the state's interest while provision protecting the privacy and personal data of the affected individuals is considerably weaker. On top of these concerns, service providers (telecom companies) have embedded terms and conditions on the SIM card registration forms that can endanger people's privacy. These include handing over people's collected data to government upon request with or without the owner's permission or consent. There are also concerns by service providers making disclaimers at registration of SIM cards to be able to provide user identification to authorities when requested.

**Section 10** concerns notice on disclosure of protected information. By protected information is understood information that is encrypted by means of a key as per **Section 1 of the Act**. It is asserted in **Section 10** that an authorized person may by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information. This can be done when the authorized person believes on reasonable grounds that a key to any protected information is in the possession of any person. It is also possible to impose a disclosure requirement if the authorized person believes that the imposition of a disclosure requirement in respect of the protected information is necessary with regard to one of the interests and purposes that legitimate the issuing of warrants. Again, the low requirement of evidence "reasonable

grounds" appears, and the "interest of economic well-being of Uganda" is listed as one of the grounds that give right to impose a disclosure requirement. Thus, the possibilities to impose on an individual a requirement to disclose protected information are not combined with sufficient legal safeguards as required under international law. A person who fails to make the disclosure required by a notice can be sentenced to a prison sentence of up to five years (**Section 10 (6**)). This penalty can be seen as disproportionate and, combined with the loose grounds that enable requiring the disclosure, to contravene the international law.

**Amnesty International and the Special Report** have also expressed their worries concerning several provisions of RICA. Amnesty called for more precise definitions regarding the grounds for and the purposes of the interceptions of communications and surveillance. They also demand a clearer procedure as regards the appointment and operation of the designated judge as well as independent oversight over both ministerial powers over the workings of the monitoring centre and the actual operations of it. Amnesty also calls for an explicit provisions requiring judicial authorization for disclosure of protected information.[34] The Special Rapporteur has criticized the low threshold, which requires law enforcement authorities to only demonstrate that "reasonable" grounds exist to allow for the interception.

According to the Special Rapporteur the burden of proof to establish the necessity for surveillance is extremely low given the potential for surveillance to result in investigation, discrimination or violations of human rights.[35]

## *The Electronic Signatures Act, 2011*

The **Electronic Signatures Act (ESA**) regulates the use of electronic signatures in Uganda. While promoting the use of electronic signatures can generally be regarded as a positive development, there are some aspects of ESA that can be seen as creating risks in relation to individuals' right to privacy and freedom of

[34] Amnesty International Memorandum on Regulation of Interception of Communications Act, 14 December 2010. See under "Conclusion" for a comprehensive list of recommendations by Amnesty International with regard to RICA.
[35] SR, A/HRC/23/40, (56).

expression. ESA for example includes provisions on advanced electronic signature that are uniquely linked to signatory, reliably capable of identifying the signatory and linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable **(Section 2).** In case the security of these types of signatory systems is not adequate, the anonymity of a person's online behavior can be threatened due to the possibility to identify the individual through his or her signature.

ESA also contains provisions concerning the public key infrastructure (PKI) that is controlled by the NITA-U, who are also responsible for licensing certification service provides (Part IV). The NITA-U is responsible for monitoring and overseeing activities of certification service providers (**Section 22).** NITA-U further has far-reaching search powers as regards the activities of service provides. These include e.g. an unlimited access to computerized data **(Section 88)** and the right to inspect, examine and copy computerized data kept by licensed certifications service provides **(Section 91). The** NITA-Us control over the public key infrastructure and far-reaching investigative powers combined with the fact that individuals' identities within the PKI are connected to a certificate can be seen to open up for abuse as regards the anonymity and privacy of the individuals whose identities are connected to a certificate.

## *The Computer Misuse Act, 2011*

**The Computer Misuse Act (CMA**) prescribes liability for offences related to computers. For example child pornography, cyber harassment, offensive communications, and cyber stalking are penalized under CMA. The maximum penalties for these offences range from one to five years of prison, with the exception of child pornography, which can generate the maximum prison sentence of 15 years. The conditions required for these offences to be at hand are, however, often rather vaguely defined. This both contravenes the requirement of unambiguous and foreseeable provisions in international law and can have a hampering effect on freedom of expression.

CMA also penalizes unauthorized access to computer programs and data, unauthorized modification of computer material, unauthorized use of interception of computer service. The maximum penalties for these offences are between 1015 years. Such heavy penalties can have a chilling effect on individual's use of computers in order to access to information and in order to use their freedom of expression. **Section 18** further penalizes unauthorized disclosure of information with a maximum prison sentence of 15 years. It is stipulated that a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access. Such a vaguely formulated provision restricting the right to disseminate lawfully obtained information can constitute a serious threat to freedom of expression online.

It is stipulated in **Section 9** that an investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification. This data includes traffic data and subscriber information. This provision can be seen to infringe on the right to privacy, and indirectly on the freedom of expression. Even though it is a court that decides over the preservation order, the grounds for issuing it are very vague. According to **Section 9 (3)** the preservation order shall remain in force until such time as may reasonable be required for the investigation of an offence or, where prosecution is instituted, until the final determination of the case until such time as the court deems fit. There is, however, no express requirements as to the level of evidence required when applying for a preservation order. It is enough that there are reasonable grounds to believe that the data is vulnerable to loss or modification, while nothing is said as regards any suspected offence. This can lead to preservation orders being issued without the level suspicion being proportionate to the infringement of privacy the preservation of computer data can result in. This provision can thus be seen to open up for abuse of the preservation orders and thus limit individuals' freedom on the Internet as it

creates a risk that e.g. information about their online traffic is preserved. It is not defined in the provision who can be targeted by a preservation order. It can thus be interpreted to impose the responsibility to preserve data to service providers as well as private individuals.

The investigative officer may also, for the purpose of a criminal investigation or the prosecution of an offence, apply to a court of law for an order for the disclosure of all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data or sufficient data to identify the service providers and the path through which the data was transmitted, or electronic key enabling access to or the interpretation of data (**Section 10). It is** further stipulated that where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling any person to submit specified data in that person's possession or control, which is stored in a computer system and any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control (**Section 11).** The investigative officers have thus far-reaching powers to get access to information through a court order. It is not specified which type of offences make it possible for investigative officers to apply for a court order. It is neither specified which level of suspicion is required for a court order to be issued. The provisions can thus be interpreted to open up for issuing a court order when the violation of privacy caused by the disclosure and submission of the data is not proportionate in relation to the seriousness of the offence. In the same way, a court order could be issued when the level of suspicion is not strong enough to render the disclosure of data proportionate as regards the ensuing violation of privacy. These provisions can consequently be seen to lack adequate privacy guarantees when it comes to the rights of authorities to access computer data, either through service providers or private individuals. Apart from breaching privacy, these provisions can also indirectly have a chilling effect on freedom of expression as it is possible for authorities to get access to individuals' Internet communications on unclear and unforeseeable grounds.

Police officers further have far-reaching powers of search and seizure if they suspect an offence under **Computer Misuse Act.** It is asserted in **Section 28** that where a Magistrate is satisfied by information given by the police that there are reasonable grounds for believing that an offence under Computer Misuse Act has been or is about to be committed in any premises and that evidence that such an offence has been or is about to be committed is in those premises the Magistrate may issue a warrant authorizing a police officer to enter and search the premises, using reasonable force as is necessary. An authorized officer may seize any computer system or take any samples or copies of applications or data that are on reasonable grounds believed to be concerned or may afford evidence in the commission or suspected commission of an offence or are intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence. In order for these extensive search powers to be triggered, the level of evidence required is low: only amounting to the reasonable grounds.

These far-reaching powers of search and seizure combined with the low threshold of evidence required constitute a threat to privacy and freedom of expression. The police have broad powers to get access to people's computer data, which creates risk for violating privacy. In addition, the awareness of these extensive powers can have chilling effect on the use of freedom of expression in the digital environment as people can be afraid of risking a police search on loose grounds.

## *The Electronic Transactions Act, 2011*

**The Electronic Transactions Act (ETA**) provides for the use, security, facilitation and regulation of electronic communications and transactions. As regards possible threats to Internet freedom, ETA contains above all pertinent provisions concerning the liability of Internet service providers.

It is stipulated in **Section 29** that a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is

founded on the making, publication, dissemination or distribution of the material or a statement made in the material or the infringement of any rights subsisting in or in relation to the material. This shall, however, not affect a contractual obligation, the obligation of a network service provider under a licensing or regulatory framework which is established by law or an obligation which is imposed by law or a court to remove, block or deny access to any material. According to **Section 30**, a service provider is not liable for damage incurred by a user for referring or linking users to a data message containing an infringing data message or infringing activity if it ;

a) Does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;
b) Is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
c) Does not receive a financial benefit directly attributable to the infringing activity; or
d) Removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

**Section 31 further** prescribes that a person who complains that a data message or an activity relating to the data message is unlawful shall notify the service provider in writing.

Although the service providers are not as a main rule responsible for third party content, ETA makes it possible for Internet service providers to take down a data message if a person informs them that it is unlawful. There seems thus to be no requirement of court order in order for the service providers to be responsible to take down material that can be deemed unlawful. This can have a chilling effect on free speech as service providers can after a request from individuals to choose to take down material that an individual deems unlawful without the question being tried by a court.

It is further stated **in Section 32** that service providers are not obliged to monitor the data which the service provider transmits or stores or actively seek for facts or circumstances indicating an unlawful activity. The Minister in consultation with the NITA-U may, however, by statutory instrument prescribe the procedure for service providers to inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service and communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority. It can be seen as problematic that a minister and the NITA-U have the power to prescribe responsibilities for Internet service providers to inform the public authorities of illegal activities and help with the identification of Internet users. There is no requirement that such statutory instruments would take necessary notice of the individual rights that can be infringed by imposing Internet service providers the responsibility to give authorities information and thus violate the privacy of individuals.

## *The Uganda Communications Act, 2013*

The Uganda Communications Act (UCA) regulates the Ugandan communications services. **Section** 4 provides for the establishment of the Ugandan Communications Commission (UCC) . Functions of the UCC include e.g. to monitor, inspect, licence, supervise, control and regulate communications services (b), to receive, investigate and arbitrate complaints relating to communications services and take necessary action (j) and establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators (u) and to set standards, monitor and enforce compliance relating to content (x) (Section 5). According to Section 8, the UCC shall exercise its functions independently while **according to Section 7.** the Minister may, in writing, give policy guidelines to the Commission regarding the performance of its functions and it shall comply with these guidelines **(Section 7).**

The functions of the UCC open up for extensive possibilities to supervise and control the communications falling under the scope of UCA. This also makes it

possible for it to act in a way that infringes both privacy and freedom of expression. Section 5(u) has for example been used to establish the Social Media monitoring centre and the interception of Communication monitoring centre under RICA to conduct communication surveillance of individuals' communications for example on the Internet.[36] Government has also recently threatened to completely block the usage of social media platforms such as Fac ebook and WhatsApp. The effect of these types of actions on the Internet freedom of citizens with regard to both freedom of expression and privacy is obviously extremely hampering.

## *The Anti-Pornography Act, 2014*

The Anti-Pornography Act (APA) was adopted in **2014 and** criminalizes all forms of pornography. According **to Section 13(1),** a person shall not produce, traffic in, broadcast, procure, import, export, sell or abet any form of pornography. An offence under this paragraph can result in a prison sentence of maximum ten years (Section 13 (2)). **Section 14(1**) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years. The realization of APA is overseen by the Pornography Control Committee established in Part II.

Pornography is defined within the framework of APA to mean any presentation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or stimulated explicit sexual activities or any representation of the sexual parts of the person primarily for sexual excitement.

Anti pornography Act prohibits all forms of pornography and covers also pornographic presentations through information technology. The definition of pornography is not exact enough to enable media and individuals to know for

[36] Unwanted Witness -report "The Internet: They are coming for it too!" January,2014,https://www.unwantedwitness.or.ug/wpcontent/uploads/2014/01/internet-they-are-coming-for-it-too.pdf. 42https://unwantedwitness.or.ug/uw-news-brief-ucc-threatens-to-shut-down-social-mediaplatforms/.

certain which presentations fall within the scope of Anti Pornography Act. According to the Special Rapporteur, the only form of pornography that the states are allowed to prohibit is child pornography.[37] States are even required to do so under international law.[38] In Ugandan law the sentences in cases of both pornography and child pornography are very heavy. As mentioned above, arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to freedom of expression. Prohibition of all forms of pornography can accordingly be seen to both limit the right to freedom of expression on the Internet and contravene the international human rights standards.

Moreover, the right to privacy is threatened within the framework of APA. **Section 24** stipulates that a register of pornography offenders containing the name of every person convicted of an offence under APA shall be maintained. The creation of this type of register can be seen to contravene both the privacy standards in international human rights law and the data protection principles.

It is laid down in **Section 15 (1)** that where information is brought to the attention of court that there exists in premises, an object or material containing pornography or an act of event of a pornographic nature, the court shall issue a warrant for the seizure of the object or material and for the arrest of the person promoting the material or object. An authorized person[39] in possession of a search warrant issued by the court may enter any premises and inspect any object or material including any computer, and seize the object, material or gadget for the purpose of giving effect to Anti Pornography Act . Consequently, if someone makes it known to the court that someone is in possession of pornographic material, the court shall issue a warrant that makes it possible to enter the suspect's home and inspect and size the individual's computer. The level of evidence required for the court to issue a warrant is not specified more closely, which means that the provision can make it possible for authorized

[37] SR, A/HRC/17/27, (25), (32).
[38] SR, A/66/290, (18), (81).
[39] According to Art. 1, by "authorized person" is understood a member of the Pornography Control Committee or a police officer.

officers to get access to an individual's computers without there being any real evidence of the existence of pornographic material. It is also asserted in **Section 24 (3**) that anyone who obstructs authorized officers commits and offence and can suffer the maximum sentence of five years. With regard to the fact that the universal criminalization of pornography can be seen to contravene international human rights principles and that the definition of pornography is vague, Section 15 can be seen to constitute a disproportionate violation of privacy.

**Section 17 of APA** also stipulates responsibility for Internet service providers. It is laid down that an Internet service provider who, by not using or enforcing the means recommended by the Committee to control pornography, permits to be uploaded or downloaded through its service any content of pornographic nature, commits an offence which can result in a prison sentence of maximum of five years (1). Section 17 (2) also makes it possible for the court to for a subsequent offence to suspend the business of Internet service providers who commit an offence under (1) In JDFEI it is emphasized that no one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so. Within the framework of APA the individuals behind Internet service providers risk a prison sentence of maximum five years for allowing individuals to upload and download pornographic material. It is also the Committees recommendations, not a court order, which lay as the basis for the Internet service providers' obligations. Such a long-going intermediary liability that is not based on a court order and has as an aim to prevent in many case legitimate expression cannot be considered to be compatible with international human rights standards.

The Ugandan cyber laws analyzed above contain many deficiencies as regards their compatibility with international human rights standards. Criminalization of certain forms of expression (e.g. the all curtailment of access to social media under the pretext of national security as witnessed during the 2016 general

elections), can in itself be seen to contravene international human rights law. At the same time the more legitimate criminalization of certain forms of expression (terrorism, child pornography) is based on vague, loose definitions, formulations and can result in disproportionate penalties.

The right to privacy is threatened under the Ugandan cyber laws as various provisions enable both targeted and mass surveillance of individuals' communications, as well as search and seizure of private mobile electronic gadgets and computers. This position is not only legitimized under the RICA, as has been analyzed above, but also several of the other analyzed laws contain provisions which make it possible to intercept individual's communications and search private property. The level of evidence required for a warrant to be issued is as a rule extremely low and the judicial involvement in the process of issuing warrants is either unclearly defined or lacking totally. independent oversight is both lacking in want and has no technical capacity. The laws lack more long-going guarantees for the protection of the right to privacy and protection of personal data in the wake of recent revelations by civil society groups under the Funga Macho report.[40]

The problematic provisions of the laws discussed above should be modified in order to become more transparent and unambiguous as regards the grounds on which freedom of expression and right to privacy can be limited in the digital environment. Interventions that seek to strengthen adherence to the rule of law by both individual officers and especially security institutions should be prioritized.

There should also be express guarantees as regards the need to assess the proportionality of the interference. This should take into consideration repealing or making necessary amendments to such laws that affect the full enjoyment of the rights and freedoms discussed above. Specifically the government should consider enacting the Privacy and Data Protection Law that has been shelved since **2014** to guarantee the full realization of the right to privacy in the wake of continued targeted surveillance by security agencies.

[40] https://www.privacyinternational.org/node/656

Establish independent oversight bodies and procedures over such actions that have the capability of negatively impacting fundamental rights and freedoms. The powers of the ministers as regards the infringements of rights should also be limited in favor of a system of independent and impartial judges or oversight commissions.

Related to the above, there is also a need to strengthen data protection. The long overdue privacy and data protection law should be enacted to give effect to **Article 27 of the 1995 Constitution**. The mass enrollment exercises, together with the compulsory SIM card registration are likely to expose many citizens data to third parties in the absence of data protection mechanisms.[41]

[41] The draft of the proposed bill can be found at http://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20PrivacyBill%20-%20Revised%20PDF.pdf

CHAPTER 05

# THE INTERNATIONAL SOURCES OF CYBER LAW

Cyber law has been developed in the many states to guarantee rights such as freedom of speech and expression. It has also been developed internationally to handle issues of jurisdictional challenges since cyber crime is not limited to space. Various international law treaties, declaration have recognized Cyber law and the rights under cyber laws.

## THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the General Assembly of the United Nations in 1966 and ratified by Uganda in 1995. The right to privacy is guaranteed in **Article 17 and freedom of expression in Article 19. para. 2.** It is stated in Article 17 that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" (para. 1) and that "everyone has the right to the protection of the law against such interference or attacks." (para. 2). As regards freedom of expression, according to **Article 19 para**. 2 "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive

and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

In the **General Comment No. 34 to Art. 19**[42] the Human Rights Committee (HRC), the body overseeing the implementation of the ICCPR, has asserted that it covers electronic and internet-based modes of expression. It has also stated that states should take into account the extent to which developments in information and communications technologies, such as the Internet, have substantially changed the communications practices around the world.

This is due to there being a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. It is asserted that state parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals to them. The free speech guarantees in ICCPR are thus applicable also on the Internet and states must guarantee the enjoyment of these rights in the digital environment.

In the same **General Comment the HRC** also stated that **Article 19 para. 2** includes the right to access to information held by public bodies. Such information includes records held by a public body, regardless of the form in which the information is stored, its source, and the date of production.

All restrictions of freedom of expression must be provided by law and be necessary for; the respect of the rights or reputations of others, the protection of national security or public order, or the protection of public health or morals (**Art. 19 para.** 3). The restrictions must also be proportionate.[43] The HRC has further emphasized that not under any circumstance, can an attack on a person, because of the exercise of his or her freedom of opinion or expression, be

[42] General Comment No. 34 to the Art. 19, Human Rights Committee, 102nd session, Geneva, 1129 July 2011. 10 Ibid. (12).
[43] Ibid. (34).

compatible with Article. This includes arbitrary arrest, torture, threats to life and killing. [44]

The HRC has also asserted that a norm, in order to be characterized as a law, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. It must also be made accessible to the public. It is further affirmed that a law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Moreover, laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.[45]

Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, must also be compatible with **Art. 19 para. 3.** Regarding counter-terrorism measures, the HRC has asserted that states parties should ensure that such measures are compatible with para. 3. This means that offences such as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. The HRC has also emphasized that excessive restrictions on access to information must be avoided. As media plays a crucial role in informing the public about acts of terrorism, its capacity to operate should not be unduly restricted and journalists should not be penalized for carrying out their legitimate activities.

**The General Comment No. 16 to Art. 17** was adopted in **1988, before** the proper arrival of the digital era, and provides less up-to-date guidance as regards Internet freedoms than **General Comment No. 34.** It was, however, asserted already at that point in time that surveillance, whether electronic or otherwise,

[44] Ibid. (23).
[45] Ibid. (25).

interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited under **Art. 17.**[46]

It was further stated that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Furthermore, effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive process or use it and that it is never used for purposes incompatible with the ICCPR. Moreover, in order to have the most effective protection of one's private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes.

Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control his or her files. If such files contain incorrect personal data or if data have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[47]

# THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

The Universal Declaration of Human Rights (UDHR) was adopted by the General Assembly of the United Nations in 1948 and it contains guarantees for both right to privacy and freedom of expression.

The right to privacy is protected by **Article 12 of the Declaration**, which states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

[46] General Comment No. 16 to the Art. 17, Human Rights Committee, Thirty second session, 8th of April 1988,(8).
[47] Ibid. (10).
http://www.ohchr.org/EN/ISSUES/FREEDOMOPINION/Pages/OpinionIndex.aspx for more information about the role of the Special Rapporteur.

Everyone has the right to the protection of the law against such interference or attacks.

**Article 19** provides guarantees for freedom of expression by asserting that everyone has the right to freedom of opinion and expression; including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

# THE EUROPEAN CONVENTION ON HUMAN RIGHTS

The **European Convention on Human Rights (ECHR)** is the most important human rights instrument at the European level. It conforms to the standards set by the ICCPR. The right to respect for private and family life, home, and correspondence is guaranteed in **Article 8. Article 10** provide protection for freedom of expression.

According to **Article8 (1)** everyone has the right to respect for his private and family life, his home and his correspondence**. Article 10** recognizes that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

These two rights may only be restricted in accordance with the law and each restriction must be necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others and in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. In order for the interference to be necessary in a democratic society, there must

exist a pressing social need and it must be proportionate to the legitimate aim pursued.[48]

# THE EU CHARTER ON FUNDAMENTAL RIGHTS

**The EU Charter on Fundamental Rights (EUCFR**) is the principal human rights instrument of the European Union.[49] It conforms in a great extent to the ICCPR and the ECHR but includes more far-reaching provisions on data protection than the other international human rights instruments. As regards the relationship between the EUCFR and ECHR, it is laid down in **article 52(3) EUCFR** that whenever the rights contained in the EUCFR correspond to those in the ECHR, the meaning and the scope of these rights will be the same. This does not, however, prevent the EU from providing more extensive protection for these rights. The accession of the European Union to the ECHR has also been planned for a long time but remains yet to be completed.[50]

**Article 7** of the Charter provides protection for the right to respect for private and family life, home and communications. **Article 8 further** guarantees protection for personal data concerning an individual. It is further stated in **Article 8** that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law and that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (para. 2). The compliance with these data protection rules shall also be subject to control by an independent authority (para. 3). In **2014 the European Court of Justice (ECJ)** declared the EUs. **Data Retention Directive (Directive No. 2006/24/EC)** to be invalid as it entailed a wide-ranging and particularly serious interference

[48] See e.g. case of Dubská and Krejzová v. the Czech Republic, 11/12/2014 and case of gough v. the United kingdom 28/10/2014 .

[49] the eucfr was first solemnly proclaimed by the council of ministers, the European Commission, and the European Parliament in 2000 and acquired full legal effect when the Lisbon Treaty came in force in 2009.

[50] See e.g. Chalmers et al., European Union Law, 2014, p. 288 f. The draft agreement on the accession of the EU to the ECHR was reached in 2013 and has been critically commented by the Court of Justice of the European Union, see http://curia.europa.eu/jcms/upload/docs/application/ pdf/2014-12/cp140180en.pdf.

with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. According to the ECJ, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality.[51]

Freedom of expression is protected by **Article 11**, which asserts that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (para. 1). It is further stated that the freedom and pluralism of the media shall be respected (para. 2).

It is further stated in **Article 52** that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

# THE AMERICAN CONVENTION ON HUMAN RIGHTS

**The American Convention on Human Rights (ACHR**) includes provisions protecting both right to privacy **(Article 11**) and freedom of expression **(Art. 13).Art. 11** stipulates that no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation and that everyone has the right to the protection of the law against such interference or attacks.

As regards freedom of expression, it is asserted in **Article 13 para. 1** that everyone has the right to freedom of thought and expression, This includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. This right shall not be subject to

[51] The joined cases C-293/12 and C-594/12.

prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure respect for the rights or reputations of others or the protection of national security, public order, or public health or morals (para. 2). Neither may the right of expression to be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions (para. 3).

## THE AFRICAN CHARTER ON HUMAN AND PEOPLE'S RIGHTS

The African Charter on Human and People's Rights (ACHPR) is an inter-African human rights instrument which Uganda ratified in 1986. While there is no provision providing protection for the right to privacy, freedom of expression is protected by **Article 9 of the Charter**. This includes right to receive information (para. 1) and right to express and disseminate opinions within law. This free speech provision can be seen to be more restrictive than the corresponding provisions in ICCPR, ECHR and ACHR as it stipulates a right to express and disseminate opinions within law without imposing any limitations on lawmakers as regards restricting freedom of expression in law.[52] Combined with the lack of the provision protecting the right to privacy, this makes the protection provided by the ACHPR for these two rights considerably weaker compared with the other international human rights instruments.

[52] Compare e.g. with Art. 11 in ACHPR protecting freedom of assembly where it is stated that "the exercise of this right shall be subject only to necessary restrictions provided for by law, in particular those enacted in the interest of national security, the safety, health, ethics and rights and freedoms of others."

# INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE (NECESSARY AND PROPORTIONATE)

The so called Necessary and Proportionate -principles are the result of a global consultation with civil society groups, industry, and international experts in Communications Surveillance law, policy, and technology. They attempt to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques. It is asserted that states must comply with each of the principles in order to actually meet their international human rights obligations in relation to Communications Surveillance. The principles in themselves are, however, not legally binding.[53]

The fundamental principles of legality, legitimate aim, proportionality, necessity, as well as the principle of adequacy, are the starting point for Necessary and Proportionate- principles. Adequacy signifies that any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

When it comes to proportionality, it is stated that decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires states, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and there is a high degree of

[53] https://en.necessaryandproportionate.org/text.

probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged;

and any excess information collected will not be retained, but instead will be promptly destroyed or returned; And information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given; That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms; To make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and have adequate resources in exercising the functions assigned to them.

Other relevant principles included in the Necessary and Proportionate- principles are the requirements of due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation and safeguards against illegitimate access and right to effective remedy.

# JOINT DECLARATION ON FREEDOM OF EXPRESSION AND THE INTERNET

Joint Declaration on Freedom of Expression and the Internet declaration (JCFEI) was adopted in 2011 by the Special Rapporteurs for Freedom of Expression of the Americas, Europe, Africa, and the United Nations.[54] The four rapporteurs

[54] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, Frank LaRue; the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) of the Organization of American States (OAS), Catalina Botero Marino; the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, Dunja Mijatoviæ; and the African Commission on Human and Peoples' Rights (ACHPR)

discussed the issues together with the assistance of **Article 19,** Global Campaign for Free Expression and the Centre for Law and Democracy. JCFEI establishes guidelines in order to protect freedom of expression on the Internet.[55] The declaration is not legally binding but it specifies many of the principles found on the legally binding instruments as regards the enjoyment of freedom of expression online.

The first of the principles states that freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards. These include the restrictions being provided for by law and necessary to protect an interest which is recognised under international law (the 'three-part' test)

**Article 1 (a)** It is also asserted that when assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests.

Further, with regard to intermediary liability, it is stated that no one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle') **I**ntermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied)

As regards filtering and blocking, it is laid down that mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as

---

Special Rapporteur on Freedom of Expression, Faith Pansy Tlakula. 28 http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848.

[55] Ibid.

social networking) is an extreme measure – analogous to banning a newspaper or broadcaster which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse. (Art. 3 a). It is further stated that Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression (Art. 3 b).

# THE AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS/ ADRIRF

The African Declaration on Internet Rights and Freedoms (ADIRF) is another document setting out principles that aim to strengthen freedom on the Internet.[56] Just like the Necessary and Proportionate - principles and JCFEI, it is not legally binding. It was launched in 2014 after more than twenty organizations having participated in the drafting process.

The development of the African Declaration on Internet Rights and Freedoms is a Pan-African initiative to promote human rights standards and principles of openness in the Internet policy formulation and implementation on the continent. The intention with ADIRF is to elaborate on the principles which are necessary to uphold human and people's rights on the Internet, and to cultivate an Internet environment that can best meet Africa's social and economic development needs and goals.[57]

AIDRF provides protection for freedom of expression, right to information and right to privacy. It also states that the right to freedom of expression on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards (3 para. 2).

[56] africaninternetrights.org/declaration/.
[57] http://africaninternetrights.org/about/.

As regards freedom of information, it is asserted that all information, including scientific and social research, produced with the support of public funds should be freely available to all (4). With regard to freedom of expression, it is further stated that no one should be held liable for content on the Internet of which they are not the author and that state should not use or force intermediaries to undertake censorship on its behalf and intermediaries should not be required to prevent, hide or block content or disclose information about Internet users, or to remove access to user-generated content, including those that infringe copyright laws, unless they are required to do so by an order of a court.

What makes ADIRF particularly relevant in the African context is that it stipulates for protection of privacy and personal data as neither or these rights are included in the ACHPR. It is stated that everyone has the right to privacy online including the right to control how their personal data is collected, used, disclosed, retained and disposed of. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication (8 para. 1).

It is further affirmed, just as in case of freedom of expression, that the right to privacy on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards (8 para. 2). Collecting personal data is only allowed when it complies with well-established data protection principles. First, personal data or information must be processed fairly and lawfully; secondly, personal data or information must be obtained only for one or more specified and lawful purposes; thirdly, personal data or information must not be excessive in relation to the purpose or purposes for which they are processed; fourthly, personal data or information must be deleted when no longer necessary for the purposes for which they were collected.

When it comes to surveillance, it is stated that mass surveillance should be prohibited by law and that the collection, interception and retention of communications data amounts to an interference with the right to privacy

whether or not those data are subsequently examined or used. It is also asserted that in order to meet the requirements of international human rights law, lawful surveillance of online communications must be governed by clear and transparent laws that, at a minimum, comply with the following basic principles:

First, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime; Secondly, communications surveillance must be judicially authorized and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation. Thirdly, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

**Conclusion.** As the survey above has shown, both freedom of expression and right to privacy are universally protected in the majority of the international human rights instruments. Limiting these two rights requires as a rule that the restrictions are laid down in law and that a due notice is taken of the principles of necessity and proportionality. There is a broad consensus that freedom of expression and right to privacy should be guaranteed the same protection also in the digital environment. Besides the traditional free speech and privacy guarantees getting a new interpretation in the digital era, there are also several legally non-binding declarations that specifically take aim on guaranteeing these rights on the Internet.

CHAPTER 06

# TERRITORIAL SOVEREIGNITY AND JURISDICTIONAL CHALLENGES IN CYBER LAW

The greatest challenge with cyber law is cross jurisdictional challenges. Cyber law and cyber crime are not limited space and so present jurisdictional challenges. A Person in Uganda can commit a cyber crime that affects another country such as Tanzania. Jurisdiction is the question of what court has authority to hear the case. Where a person makes a statement in one jurisdiction and a person reads or hears it in another, it creates a question of where to bring litigation. When crimes occur, it may be hard to even figure out where a defendant committed a crime. There may even be difficulties working between states or countries to bring litigation. Cyber lawyers must navigate all of these challenges to effectively pursue their case on behalf of the public or the client.

It is pertinent to note that there is no international treaty governing internet jurisdiction. This means countries must exercise their territorial sovereignity making courts apply traditional principles to virtual space.

**Territorial sovereignity refers** to the state's complete and exclusive exercise of authority and power over its geographical territory. Territorial sovereignity can be violated when third parties gain unauthorized access to ICT in foreign

countries without knowledge and permission of the host country and or its law enforcement agents. This violation happens when even pursuant to an investigation of a cyber crime committed in a different country in an effort by that country to locate or stop the cyber crime.

Jurisdiction is defined in the case of **Koboko District Local Government V Okujjo Swali**[58] in which the court defined jurisdiction to mean the authority conferred by law upon the court to decide or adjudicate any dispute between parties or pass judgement or order. Jurisdiction in line with state sovereignity is to the effect that states have power and authority to determine, define and preserve the duties and rights of people within its territory to enforce laws and provide penalty for their violations. Territorial sovereignity can be applied to cyber space particularly to state's information and Communication Strategy.

Cyber Crime jurisdiction is determined by several factors and these include nationality of the offender, principle of nationality, active personality principle and the impact of the Cyber crimes on the interests and security of the state.[protective principles].

A genuine connection between the cyber crime and a state's laws are important in determining jurisdiction of the state. In the **case of R V Sheppards and another** [2010**]** the court upheld the application of Britain's **Public Order Act of 1986** to racially inflammatory Material posted on a website hosted by the United State's Server , and the Conviction of two British residents for posting this material.

Different countries and regional groupings have enacted the different laws to handle prosecution of cyber crimes. Jurisdiction is usually primarily determined by location of the offenders, victims, and Impacts of Cyber crime.

In the League of Arab countries, they have enacted the **Arab Convention on Combating Information Technology Offences of2010. Article 40 of this Convention** provides that every state party shall commit itself, subject to its own

[58] Koboko District local Government V Okujjo 2016

statutes or constitutional principles to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignity of States and non interference in the International affairs of other states.

In Europe, **article 21, of the Convention on Cyber crimes 2005**, states that each party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence included in its territory.

It is worth noting that National Cyber laws establish cyber crime jurisdiction. In **Malaysia, the Computer Crimes Act 1997**established the state's jurisdiction over Cyber crime. **Article 9** of this article holds that the provisions of this Act shall in relation to any person, whatever his nationality or citizenship have effect outside as well as within Malaysia and where an offence is committed by any person outside Malaysia he or she may be dealt with in respect of such offence as if it was committed at any place in Malaysia.

According to **Section 30 of the Cyber Crimes Act 2015** Cyber Crimes Act law in Tanzania, Tanzania claims jurisdiction over Cyber crime when an act or omission constituting an offence wholly or in part within Tanzania on a ship or aircraft registered within the United Republic Of Tanzania who resides outside Tanzania if the act or omission would equally constitute an offence under a law of that country or by any person irrespective of his nationality or citizenship or location, when the offence is committed using a computer system , device or data located within Tanzania.

In **Kenya,** section **66**of the **Computer Misuse and Cyber Crimes Act of TWENTY EIGHTEEN** provides that an act or omission committed outside Kenya which could have been have been an offence under this Act if committed in Kenya if the person committing the act or omission is a citizen of Kenya or ordinarily a resident in Kenya and the act or omission against property belongiong to the Government of Kenya outside Kenya or to compel the government of Kenya to do or refrain from doing any act … the person who commits the act or omission present in Kenya. Territorial Jurisdiction

In Uganda, the criminal trial process is governed by legal principles such as the burden of proof, principle of legality and presumption of innocence.

**Section 32 of the Electronic Transactions Act Subject to subsection (2),** this Act envisages territorial jurisdiction. It is to the effect, that any person, whatever his or her nationality or citizenship and whether he or she is outside or within Uganda.

**Section 30(3)(b)** also provides that for this section to apply, the computer, program, or data must have been in Uganda at that material time.

Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

In the case of **Doctor Stella Nyanzi V Uganda**[59]**,** Doctor Stella Nyanzi was charged with two counts. Count One was the offence of cyber harassment contrary to section 24(1)(2)(a) of the Computer Misuse Act 2011. During the lower court trial, the appellant pleaded not guilty to both charges.

She appealed to the High court after being dissatisfied and grieved by the judgement and orders of the lower court. She contended that the trial judge erred in law and fact when she entertained the suit and yet the appellant court had no jurisdiction. She also sought a revision in the lower court to enable it determine its correctness, legality and propriety of the trial of the findings. However, the revision was dismissed.

However she succeeded on appeal because the state failed to provide evidence that the gadgets she used at the time of committing the said acts were in Uganda.

In **Fred Muwema V Facebook Ireland Limited**[60]the background of the case was that the plainfiff was a facebook user and was subjected to various allegations against him on his page. He sought court orders majorly to identify

[59] Uganda V Doctor Stella Nyanzi Ncriminal;Appeal NUMBER 79 OF 2009 Arising from Criminal Case AL –CR –CO-11115 of 2018

[60](2016)

the persons behind the said acts, to take down the alleged defamatory posts and to prevent similar posts from being reposted. Court held that the details collected by facebook relating to the identities and location of persons operating under the name Tom Voltaire Okwalinga could be secured from facebook to prove the residency of the device used in making an alleged offensive posting and the identity of the person doing so when legally sought through this particular case, the court declined to grant the order for facebook to release the information for security of the person who allegedly posted the information.

In **Uganda V Ssebuwafu Mohammed**[61] and seven others, the witness exhibited the phones of four of the accused person as well as the telephone printouts which showed the location of the accused persons as having been within or around the area of the crime scene. The court held that such evidence was capable of proving a proposition within the accuracy of mathematics.

# TYPES OF JURISDICTION

**Personal Jurisdiction**

This is the geographical restriction on where a plaintiff may elect to a sue a defendant for a particular claim**.** The restriction is intended to prevent a plaintiff from suing a defendant in a jurisdiction foreign to the defendant unless that defendant has established some relationship with that forum that would lead him to reasonably anticipate being sued there.

In Personal Jurisdiction, the issue is whether court has authority to decide a case involving a specific defendant. The plaintiff must demonstrate that defendants have sufficient minimum contacts with the forum such that finding personal jurisdiction will not offend 'traditional notions of fair play and substancial justice. By minimum contact, it means that as long as a person or a group of people natural or corporate are found, then the courts have jurisdiction to hear the suit.

[61] Uganda v Ssebuwufu Mohammed and 7 others (2016)

In **International Shoe V Washington**[62]**,**the International Shoe company had branches over so many countries and about 13 of its stuff was in Washington D.C . When they were being sued, the company averred that the court had no jurisdiction to try them because the head offices of the company were not in Washington DC. It was held that the court had jurisdiction to entertain the suit because it was exercising personal jurisdiction in which only minimum contact is necessary to grant jurisdiction to the court. It was further held that the plaintiff has a burden of proving that the defendant has minimum contacts with the forum .

To establish Personal Jurisdiction over a non resident, court must engage in a two part inquiry. That is the court must first establish whether jurisdiction is applicable under the state's law and whether a finding of jurisdiction satisfies the constitutional requirement of due process.

**General Jurisdiction.**

General Jurisdiction refers to authority of a court to hear any cause of action involving a defendant even those unrelated to the defendants contacts with the forum state. The defendant must have continuous and systematic contacts with the forum state in order for a court to assert jurisdiction general jurisdiction.

In **Helicopteros V Nacionales de Columbia** , [63] the Supreme court found that mere purchases were insufficient to assert jurisdiction over a Colombian Corporation in a claim arising out of a Peruvian Helicopter crash was neither 'continous and systematic.' The court held that general jurisdiction did not exist when the Colombian defendant negotiated a contract in Texas, accepted checks from Texas and sent employees to purchase helicopters and attend training sessions in Texas.

If minimum contacts are sufficient to establish general jurisdiction, the out of state defendant may be sued in the form in the forum state for any cause of action arising in any place. The threshold for general jurisdiction is high, the

[62] International shoe V Washington, (1945)US 326
[63] Helicopteros V Nicionales de Columbia {1984}

contacts must be sufficiently extensive and pervasive to be the functional equivalent of physical presence. With general jurisdiction, the defendant's contacts are so extensive in the foreign forum that the defendant becomes functionally present.

In **Good year Dunlop Tires Operations, SA V Brown**[64] it was held that a corporation is subject to general jurisdiction only in a home state defined as the state of incorporation and principal place of business. The court further emphasized that the threshold for a finding of general jurisdiction is extremely high.

In ***Gator. Com Corporation V LL Bean Incorporation***[65], Court found that general jurisdiction based on L.L Beans millions of dollars of Sales to California consumers. The L.L.Bean court noted that direct e-mail solicitations and millions of catalog sales spurred this revenue stream. The facts of the case is that Gator.com Corp filed this suit against the outdoor outfitter in a California federal Court seeking a declaratory judgement that its pop-up ads did not infringe L.L Bean's trademarks or constitute an unfair business practice. L.L Bean is a Maine corporation with its principal place of business in Maine. Because L.L. Bean had neither property nor employees in California the district granted L.L Bean's motion to dismiss for lack of personal jurisdiction.

On appeal, the decision was reversed. Court held that there is a basis for general jurisdiction over the Maine outfitter. The basis for this holding was that the company had done extensive marketing and sales targeting California vendors in addition to creating a website.

Basing on the above, it is right to say that general jurisdiction is a process through which a court can assert personal jurisdiction over a non resident.

[64] Good year Dunlop Tires Operation SA V Brown [2011]
[65] Gator. Com Corporation V LL Bean Incorporation (2005)

**Specific Jurisdiction**

Courts use a three part test to evaluate whether there is a basis for specific jurisdiction or case linked jurisdiction in a particular case to prevent the defendant from being subject to personal jurisdiction solely because of random fortious or attenuated contacts or the unilateral activity of another third party. that is; the defendant must have either purposefully direct its activities at the forum or purposefully avail itself of the privilege of doing business there, the claim must arise from the defendants forum activities, the exercise of jurisdiction must be reasonable.

**Purposeful availment**

The purposeful availment test seeks to determine whether the defendant purposefully avails itself of the privilege of conducting activities within a state through systematic and continuous contacts. In the case of *International Shoe V Washington*[66], the court coined a new term purposeful availment to serve as a litmus test for specific jurisdiction.

In the case of *Good year Dunlop Tires Operations, SA V Brown*[67] it was observed that Specific jurisdiction depends on an affliation between the forum and the underlying controversy principally, activity, or an occurance that takes place in the forum state and is therefore subject to the states regulation.

In *Burger King Corp V Rudzewicz (1985)* it was emphasized that contacts must proximately result from actions by the defendant himself that create a substantial connection with the forum state.

**Purposeful direction**

This is to the effect that where a defendant targets a particular forum, he may be called to answer his or her forum (effects principle)**. In Calder V Jones,** the courts exercised jurisdiction on the principal that her actions would lead be

[66] International shoe V Washington, (1945)US 326
[67] Good year Dunlop Tires Operation SA V Brown [2011]

injurious to the plaintiff, then she must reasonably anticipate being sued into the court where the injury occurred.

**In Keeton V Hustler Magazine** [68]the case dealt with allegedly libelous statements made in Hustler magazine. The plaintiff brought the action in New Hampshire, despite not being a resident of New Hampshire.

**Passive Jurisdiction**

This is jurisdiction based on interactivity of the websites. With Passive jurisdiction, there is no interaction with visiters, courts find no personal jurisdiction at the end of the spectrum. Interactive websites often give rise to a finding of personal jurisdiction 'gray area, middle ground cases, the courts will assess the level of interactivity in order to determine whether changes are commercial or not.

**In Cyber incorporation V Cyber sell Incorporation,** [69]court found that Cybersell's operation of a passive website did not purportedly vail itself the priviledge of doing business in Arizona thus his contacts were insufficient to establish personal jurisdiction. However, the court noted that the operation of an interactive commercial websites often is sufficient to warrant personal jurisdiction.

**In Rem Jurisdiction**

In Rem Jurisdiction relates to the determination of title to, or the status of property located within the court's territorial limits. A quasi in rem judgement affects the interests of a particular persons in designated property**.**

**Conclusion,** Internet presence automatically creates an international presence triggering the potential for cross border litigation. Cyber law and cyber crimes are not limited to a defined space. However, there is no single treaty establishing rules for cyber space and yet internet law requires harmonized jurisdictional rules.

[68]Keeton V Hustler Magazine 1984
[69]Cyber incorporation V Cyber sell Incorporation,

CHAPTER 07

# CHALLENGES OF IMPLEMENTING CYBER LAWS IN UGANDA

Government of Uganda passed three critical laws, namely (i) **Computer Misuse Act, 2011, Electronic Transactions Act, 2011, Electronic Signatures Act, 2011**. Taken together, they are referred to the Uganda Cyber Laws.

According to **Computer Misuse Act long title (preamble**) it provides for the safety of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters."

Cyber laws are important in so far as Tackling cyber crimes is concerned, addressing intellectual property rights and copyrights protection, promoting e-commerce and facilitate trade and Regulate the use of electronic signatures to ensure security (confidentiality, integrity and availability) of communication and non-repudiation.

**Computer Misuse** refers to unauthorized access to private computers and network systems, deliberate corruption or destruction of other people's data, disrupting the network or systems, introduction of viruses or disrupting the work of others; the creation and forwarding of defamatory material, infringement of

copyright, as well as the transmission of unsolicited advertising or other material to outside organizations. It includes all the activities that undermine computer security affect the integrity, confidentiality and availability of computer systems.

**A digital signature** is an electronic signature used to confirm the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate (reject) it later.

A digital signature is NOT a scanned copy of your physical signature. An electronic signature on the other hand, "is a typed name or a digitized image of a handwritten signature. Consequently, electronic signatures (signatures) are very problematic with regards to maintaining integrity and security, as nothing prevents one individual from typing another individual's name. Due to this reality, an electronic signature that does not incorporate additional measures of security (the way digital signatures do, as described above) is considered an insecure way of signing documentation." The **Electronic Signature Act, 2011** laws of Uganda is intended to address the challenges associated with electronic signatures by providing for the use of digital signatures in commercial transactions.

Electronic Transaction means a transaction of either commercial or non-commercial nature communicated electronically by means of data messages and includes the provision of information and e-government services.

Makes provision for the use, security, facilitation and regulation of electronic communications and transactions;

Encourages the use of e-Government service, and provides for related matters.

**The Electronic Transaction Act addresses the following issues, among others;**

Enforceability and form requirements for electronic contracts, Regulation of domain names which are a new form of digital property, Privacy protection for consumers and users of electronic media, Establishment of a regulatory framework that is compliant with the rapid technological changes, Determining the levels of responsibility in tort and contract attached to enhanced abilities of machines, Classification of trade in information products especially where the relationship between the producer and ultimate consumer is remote.

## STATUS OF IMPLEMENTATION OF CYBER LAWS IN UGANDA

The Ministry of Information and Communications Technology (MoICT) of Uganda has been at the forefront in the implementation of cyber laws. A lot has been achieved since 2011, when the cyber laws were enacted.

## THE CHALLENGES IN IMPLEMENTING CYBER LAWS IN UGANDA

Lack of skills and tools in to investigate computer crimes, Cyber law is relatively a new the right development in Uganda. Most Ugandan Lawyers and members of the bench have little knowledge on how to prosecute cyber crimes or information on cyber law.

There are missing mechanisms of control and there are anonymous communications e.g. anonymous cloud emails involved in crime e.g. use of internet cafes, wireless networks, dynamic IPs internet access and too make matters worse most users use encryption which encryption technology make it difficult to investigate

Low understanding of cyber laws among key stakeholders. Even the key stake holder's lack knowledge about cyber law such as the ministry of justice and the ministry of Information technology

Very few cyber crime training experts local capacity is not being developed and empowered to help government. This makes prosecution and investigation very hard.

High levels of public ignorance, People are ignorant of cyber law and even if told that they are committing cyber crimes, they are reluctant to change. The rate of hooliganism in Uganda is very high.

Lack of harmonization of laws, The laws on Cyber seem to be conflicting with the constitution. For example the laws seem to limit freedom of speech and expression that are guaranteed under article of the constitution.

Cyber law is wide evolving and complex. Cyber initiatives are implemented by a single vendor, with single experts. There is need to get more experts. Approach is lacking. old people being trained instead of young graduates

In regard to procuring surveillance equipment and criminalizing gadgets (computers) as well as Internet content. Their powers range from illegally ordering Internet service providers to block certain social platforms to signing secret memorandum of understanding among government agencies to share information about Internet users and published content in order to enforce the Ugandan cyber legislation. Harassment of online activists by police has also been reported.

There is no statutory framework governing the transactions. The mobile network operators have no obligations to report or disclose info on mobile money services to Bank of Uganda (BOU) as a regulator. All these are gaps that are clearly visible in the Ugandan legal framework on cyber crime.

There is a general lack of capacity among the police and other law enforcement agencies to detect, investigate and assist in prosecution under the Computer Misuse Act 2011. This has been a challenge in the prosecution of some high

profile cases in the country like **Uganda Vs Kato Kajubi and Uganda Vs Dr. Aggrey Kiyingi cases** that relied on electronic evidence. In Kato Kajubi following a retrial, the accused was convicted. Following the terrorist attack on Kampala on 1Ith July 2010, the police with the help of the FBI were able to uncover emails linking the bombings to the suspects.

There is lack of capacity and funding to enable special skills training required to counter the ever evolving and increasing cyber crime nationally and globally. Uganda does not have adequate data protection laws. Across the East African sub region and the African continent, there is a lack of a harmonized legislative regime to tackle cybercrime. Finally, there is insufficient knowledge about the law and inadequate sensitization of the public and other potential victims of cybercrime.

Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

On enforcement and implementation of laws, there is no centralized budget for cyber security. Every Ministry allocates its budget separately and depends on previous experience and future plans to allocate budget for cyber security. In agreement, an advocate interviewed said there is limited capacity by the law enforcement agencies to investigate computer-related crimes, in-line with known global best practices. This has been attributed largely due to lack of sufficient technical expertise in digital forensic in Cybercrime cases."

A key informant said that the National Information Security Strategy (NISS) does not provide specific actionable directives that relate to cyber security. He added "Risks may exist but the strategies are not aligned with national goals; at the moment every Agency has their own list of incidents and have different priorities. Different institutions place different levels of importance to technology, depending on their priorities."

Uganda does not have an official list of Critical National Infrastructure (CNI) sectors in Uganda. This is mainly attributed to the lack of clear understanding of what constitutes a CNI sector list and the difficulty in recognizing what needs to be protected. Experts believe they generally have the ability to recognize what is important for Uganda and will take the appropriate & necessary measures to protect Uganda's CNI. Thé National Information Security (NIS) Policy defines the concept of critical information infrastructure (Cll), but does not clear address the CNI issue in detail. According to the National Information Security policy "the information and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services". This is an areas that needs to be developed further.

Overall, cyber security capacity in Uganda lies between an initial and formative stage of maturity. This expresses a state of maturity where some features have begun to grow and be formulated, but may be ad-hoc, while these can be clearly evidenced.

CHAPTER 08

# ELECTRONIC CONTRACTS AND ELECTRONIC TRANSACTIONS / ELECTRONIC COMMERCE

## INTRODUCTION

The customer pays his money and gets a ticket. He cannot refuse it. He cannot get his money back. He may protest to the machine, even swear at it. But it will remain unmoved. He is committed beyond recall. He was committed at the very moment when he put his money into the machine." Lord Denning, in **Thornton V. Shoe Lane Parking (1971) 2 QB 163 at 169**

Over the last several years the Internet has emerged as an important tool to facilitate the conduct of business for consumers and businesses alike. Conducting business in the off-line world requires that the parties engaging in commerce each understand and agree to the legal rules that will govern their business relationship. In order to ensure certainty, parties engaging in electronic commerce need to ensure that transactions conducted by electronic means over the Internet are legally binding and enforceable to the same extent as traditional paper - based transactions.

The struggle of contract law to keep pace with technological change is not new; past technological advancements such as the telegraph and facsimile machine also introduced hurdles in the application of traditional contract law principles that the common law had to overcome. However, the Internet has revolutionized the ease at which businesses and individuals can engage in commercial activity and arguably has required contract law to adapt at a much faster pace. The Internet has introduced some uncertainty into many aspects of commercial transactions conducted via electronic means, such as in the areas of the formation of enforceable electronic contracts, jurisdiction, and statutory issues relating to evidence and signature requirements. Slowly, through the combination of common law developments and legislative reform, the legal rules relating the creation of enforceable electronic contracts are becoming increasingly more certain.

Electronic commerce is the buying and selling is the buying and selling of goods and services or transmitting of funds or data over an electronic network, primarily the internet. It is a type of e-business that features online sale transactions made using mobile devices, such as smart phones, and tablets. The term e- commerce and e-business are often used interchangeably. It includes mobile shopping, mobile banking, and mobile payments.

Electronic transactions is defined under section 2 of the Electronic Transactions Act to mean exchange of information, or data ,the sale and purchase of goods and services between businesses, households, individuals, governments and other public or private organizations conducted over computer mediated networks.

The use of modern means of communication, including electronic means such as email, in conducting business is on the increase. This can partly be attributed to increase in technological developments in the area of information and communication technology and increased access to the internet.

For instance, many transactions are now effected electronically. For example, by the use of automated teller machines (ATMs or cash point dispensers outside banks) and electronic fund transfers (EFTs) transactions are made between

financial institutions and at the point of sale. More so, many organisations now exchange data electronically. For example, a large manufacturing company may order components automatically and electronically from its suppliers when stock levels reach a predetermined lower limit.

## HISTORY OF E- COMMERCE

The beginning of E- commerce can be traced to the 1960s when business started using EDI to share business documents with each other companies. In 1979, the American National Standards Institute developed ASCX12 as a universal standard for businesses to share documents through electronic networks

After the number of individual users sharing electronic documents with each other grew in the 1980s, the rise of the e Bay and Amazon in 1990s revolutionalized the e-commerce industry. Consumers can now purchase endless amounts of items online, from e-tailers, typical brick and mortor stores with e-commerce capabilities.

The legal regime in Uganda governing electronic contracts is the; The Electronic Transactions Act, No. 8 of 2011, the Electronic Transactions Regulations, the Electronic Signatures Act, No.7 of 2011, the Electronic Signatures Regulations ,The Contracts Act, 2010.

## TYPES OF E-COMMERCE

**Business to business**. This refers to the electronic exchange of products, services, or information between businesses rather than between business and consumers. Examples include online directories and product and supply exchange websites that allow businesses to search for products, services and information to initiate transactions through e-procurement interfaces.

**Business to consumer**. This is the retail part of e-commerce on the internet. It is when businesses sell products, services, or information directly to consumers.

Examples include Jumia online shopping and adverts on various social media platforms .

**Consumer to business**. This is a type of e- business in which consumers make their products and services available online for companies to bid on and purchase. This is the opposite of the traditional commerce model of Business to consumer

An example of a consumer to business platform is a market that sells royalty free photographs, images, media, and design elements.

**Business to administration**. This refers to transactions conducted online between companies and public administration or government bodies. Many branches of government are dependent on e-services or products in one way or another, especially when it comes to legal documents , registers , social security, fiscals and employment. Businesses can supply these electronically . Business to administration services have grown considerably in recent years as investments have been made in e- government capabilities.

**Consumer to administration.** This refers to transactions conducted between individual consumers and public administration or government bodies. The government rarely buys products or services from citizens but individuals frequently use electronic means in the following areas.

- Education by disseminating information , distance learning or on line lectures through various online learning platforms .
- Social security by distributing information and payments.
- Taxes by filing tax returns, and making payments.
- Health. By making appointments, providing information about illness and making health service payments.

There are however certain hindrances which may be faced in using information and communication technology in business transactions including, skepticism

from consumers, questions on security of information and uncertainty of legal validity of such transactions.

Examples of the legal consequences associated with electronic trading include the fact that:

- The law requires that some contracts are in a particular form – for example, by deed or in writing. (This is now covered under the Contracts Act, which defines written contracts to include data message)
- There may be doubts as to when the contract was made and, if the parties are in different countries, which country's law will apply to the contract.
- The evidential weight of electronic documents must be considered and assessed.

# EVIDENTIAL STATUS OF ELECTRONIC DOCUMENTS AND ELECTRONIC TRANSACTIONS

**Article 9 of the UNCITRAL Model Law on Electronic Commerce** 1996, amended 1998, states that nothing in the application of the rules of evidence shall apply to prevent the admissibility of a data message in evidence on the sole ground that it is a data message or, if it is the best evidence the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. (See meaning of data message ETA)

Originally, the best evidence rule insisted that only an original document could be admitted as evidence and copies were not allowed. However, this could cause significant hardship if the original had been lost or destroyed. The best evidence rule has all but disappeared but remnants of it still remain. The courts have recognised that a rigid adherence to the best evidence rule is inappropriate in the context of the accuracy with which copies of originals may now be made. LordJustice Lloyd said in **R v Governor of Pentonville Prison, ex parte Osman [1989] 3 All ER 701:** We accept that it [the best evidence rule] served

an important purpose in the days of parchment and quill pens. But, since the invention of carbon paper and, still more, the photocopier and telefacsimile machine, that purpose has largely gone.

**Sections 7 of the Act** provides for authenticity of electronic information or a data message which must ordinarily clothe it with evidential value. It provides that where a law requires information to be presented or retained in its original form, the requirement is fulfilled by a data message if:

a) The integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
b) That information is capable of being displayed or produced to the person to whom it is to be presented. **Section 7(2) of the Act** provides for the following criteria for assessing the authenticity of a data message:
c) by considering whether the information has remained complete and unaltered, except for the addition of an endorsement and any change which arises in the normal course of communication, storage or display;
d) in light of the purpose for which the information was generated; and
e) having regard to all other relevant circumstances.

**Section 63 of the Evidence Act, Cap. 6 of the Laws of Uganda requires proof of documents by primary evidence (Primary evidence** is defined **under s. 61 of the Act** as meaning the document itself produced for the inspection of the court) except in the cases where secondary evidence may be admissible (Secondary evidence **under s. 62 means** and includes: certified copies given under the provisions hereafter contained; copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with those copies; copies made from or compared with the original; counterparts of documents as against the parties who did not execute them; oral accounts of the contents of a document given by some person who has himself or herself seen it).

In light of this existing strict rule of evidence, the Electronic Transactions Act, 2011 forestalls any possible hurdles by providing under section 8 that the rules

of evidence shall not be applied in legal proceedings so as to deny the admissibility of a data message or an electronic record because:

a) merely on the ground that it is constituted by a data message or an electronic record;
b) if it is the best evidence that the person adducing the evidence could reasonably be expected to obtain; or
c) merely on the ground that it is not in its original form.

Nonetheless, subsection (2) places on a person seeking to introduce a data message or an electronic record in legal proceeding the burden to prove its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

In **Kalungi Robert v. Uganda, High Court of Uganda (Anti-Corruption Division) Criminal Appeal No. 41 of 2015** the court confirmed the admission in evidence of a compact disc that had been submitted by the prosecution after it was satisfied that the disc's authenticity is all that the prosecution had to demonstrate upon presenting it as an electronic record. The court held as follows with regard to the rules of evidence and authentication.

**Section 8 of the Electronic Transactions Act** waives the application of rules of evidence to deny admissibility of data message or electronic record in legal proceedings. The section however requires the court to establish the integrity of the means with which that electronic record was generated, stored, and communicated. The same provisions are found in section **29 of the Computer Misuse Act.**

The following rules are applied by a court in assessing the evidential weight of a data message or an electronic record:

a) the reliability of the manner in which the data message was generated, stored or communicated;
b) the reliability of the manner in which the authenticity of the data message was maintained;

c) the manner in which the originator of the data message or electronic record was identified; and
d) any other relevant factor.

Thus, in **Dian Gf International Ltd v. Damco Logistics Uganda Limited, High Court (Commercial Division) Civil Suit No. 161 of 2010** the defendant submitted evidence of an email which he sought to rely on. This was objected to by the plaintiff on the ground of its authentication which, it was submitted, could not be verified when it was sent and whether it was received. In its response, the defendant submitted that the law relied on to attack the email it sought to rely upon was a statutory rule under American Federal law and would not apply unless there was as statute in pari materia in Uganda.

Upholding the objection to the email, the court cited the **Electronic Transactions Act, 2011** and held as follows: I do not agree that the case law is irrelevant because the **Electronic Transactions Act 2011, Act 8 of 2011** applies modern practices in this case at the point of admissibility of evidence as far as requirements for authentication is concerned. Secondly the principles upon which email evidence may be admissible are analogous to the traditional grounds under the **Evidence Act cap. 6 Laws of Uganda** for the admissibility of documentary evidence

The Court of Appeal of Uganda also lent credence to the **Electronic Transactions Act, 2011 in Sematimba Peter Simon and National Council for Higher Education v. Sekigozi Stephen Court of Appeal Election Petition Appeal Nos 8 and 10 of 2016**where it upheld electronic information obtained from the internet, holding as follows:

"We have perused **Kabakubya Bashir's** Supplementary Affidavit in support of the Petition and noted that most of the annexures thereto were obtained from the internet and he acknowledges the source of the information. We agree with the trial Judge's reliance on the **Electronic Transactions Act, 2011** to admit the annexures on the affidavit. As rightly quoted by the trial Judge, **section 8(1)(a) and (b)** provide for the admissibility and the evidential weight of a data message or an electronic record … "

An aspect intrinsically related to the use of primary evidence is its storage in the original form. It is conceived that certain regulated sectors have a requirement for storage of information in its original form. For instance, **section 6(b) of the Press and Journalists Act** requires a proprietor and an editor of a mass media organisation to retain a copy of each newspaper published by the organisation and a copy of each supplement to it for not less than ten years.

Similarly, Financial Institutions are required under section **46 of the Financial Institutions Act, 2004 Act No. 2 of 2004** to keep financial ledgers and other financial records which show a complete, true and fair state of their affairs and which explain their transactions and financial position to enable the Central Bank to determine whether the institutions have complied and continue to comply with the Act.

The financial records envisaged include any book, computer record, report, statement or document relating to the business affairs, transactions, and property of a financial institution.

The records must be kept for a period of not less than ten years.

In line with the above statutory requirements, **section 9 of the Electronic Transactions Act, 2011** provides that where a law requires that a document, record or information be retained, the requirement is fulfilled by retaining the document, record or information in electronic form if:

a) the information contained in the electronic record remains accessible and can be used for subsequent reference;
b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to accurately represent the information originally generated, sent or received;
c) the information which is retained enables the identifification of the origin and destination of an electronic record and the date and time when it was sent or received; and

d) the consent of the department or ministry of the government, or the statutory corporation, which has supervision over the requirement for retaining the record, has been obtained.

# PROTECTING THE INTEGRITY OF ELECTRONIC TRANSACTIONS

Information technology is quite prone to manipulation and abuse by its users. Where there are electronic transactions which mostly involve money, the propensity of abuse naturally increases.

To nip the vice in the bud, one of the three earlier mentioned key cyber laws specifically provides mechanisms for this. The **Computer Misuse Act was enacted alongside the Electronic Transaction Act and the Electronic Signatures Act in 2011**.

Its long title carries its key purpose where it is provided that it is an Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

Key terms with specific definitions under **section 2 of the Act** include:

a) A computer which means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices.
b) Information system which means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system.

c) Access which means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective.
d) Damage which means any impairment to a computer or the integrity or availability of data, program, system or information that:

1) causes any loss;
2) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;
3) causes or threatens physical injury or death to any person; or
4) threatens public health or public safety;

The manner of regulation under the Act is the creation of offences for different kinds of infractions in respect to the use of computers. The starting point, however, is that every person may ordinarily have authorized access to a computer.

This is in two instances which are: where the person is entitled to control access to the program or data in question; or the person has consent to access that program or data from any person who is charged with giving that consent.

With access to a computer, a person's action is likely to result into modification of its contents. Content under **section 2 of the Act** includes components of computer hardware and software. Thus, modification of the contents of a computer is deemed to take place if, by the operation of any function of the computer concerned or any other computer connected to it result into:

a) a program, data or data message held in the computer concerned being altered or erased; or
b) a program, data or data message being added to its contents.

So far as directly relates to electronic transactions, the following infractions amount to offences:

a) Intentional access or interception of any program or data without authority or permission.

b) Interference with data in a manner that causes a program or data to be modifified, damaged, destroyed or rendered ineffective.
c) Unlawful production, selling, offering to sell, procuring for use, designing, adapting for use, distributing or possessing any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performing any of the foregoing acts with regard to a password, access code or any other similar kind of data.
d) Utilising any device or computer program in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data.
e) Accessing any information system so as to constitute a denial including a partial denial of service to legitimate users.
f) Causing an unauthorised modifification of the contents of any computer.
g) Securing access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service.
h) Intercepting or causing to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device whether similar or not.
i) Electronic fraud which is defined under **section 19 of the Act** to mean deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

Upon conviction, the penalties for the offences listed above include fines and custodial sentences or both. The custodial sentences are up to fififteen years imprisonment. Section 27 of the Act further provides that where a person is convicted under the Act, the court must in addition to the fine or custodial sentence or both order the convict to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the

In **High Court (Anti-Corruption Division) Criminal Session Case No. 123 of 2012, Uganda v. Sentongo and 4 Others,** accused 1 was found guilty of committing Electronic Fraud contrary to s. 19 of the Computer Misuse Act, 2011 and was accordingly convicted. To reach the conviction, the court stated that to constitute electronic fraud, there must be proof of deception deliberately performed by the accused with the intention of securing an unfair or unlawful gain through a computer network. Accused 1 was found to have been very deceptive when he created electronic ghosts gave them pseudo names and obscene rights to do anything without authorisation.

Although It is also hard to establish the court's jurisdiction. In **Uganda v. Stella Nyanzi** in which the accused was tried and convicted of the offence of cyber harassment which is provided for under section 24 of the Computer Misuse highlights the intent of the government of Uganda on implementing the provisions of Uganda's cyber laws.

Uganda has a number of legislations in place, which address electronic commerce such as the , the **Contracts Act, Computer Misuse Act,[70] the Electronic Signatures Act, The Electronic Transactions Act[71], Anti-pornography Act [72] and Electronic Misuse Act.**

In addition to the legal frame work, there are principal institutions whose work and efforts towards electronic transactions cannot be underestimated. The principal player agencies include, **Uganda Registration services Bureau, Uganda National Bureau of Standards**, **the Ministry of Information Communication Technology, the Uganda Communications Commission, the National Information Technology Act-Uganda (NITA-U), the Uganda Police Force and the judiciary.** Uganda has gone further to set up a **Computer Emergency Response Team (CERT**) with all the aforementioned Government agencies being represented on the committee. The Uganda Communications

[70] 2010
[71] 2011
[72] 2014

Commission (UCC) has set up its own CERT to compliment the national team and this was set up on the 6th of June 2013.

## *1995 constitution of the republic of Uganda*

The **Constitution of the Republic of Uganda, 1995**[73] the supreme law of the nation. According to **Article 1 of the constitution**, the people shall be governed according to their norms and aspirations. To this effect, Freedom of expression is protected by **Article 29** where it is stated that every person shall have the right to freedom of speech and expression, which shall include freedom of the press and other media. As regards freedom of information, it is stipulated by **Article 41** that every citizen has a right of access to information in the possession of the State or any other organ or agency of the State except where the release of the information can put the security or sovereignty of the State at risk, or interfere with the right to the privacy of any other person. This means that sellers and consumers have a right to freely express themselves concerning electronic transactions and other related aspects. **Article 40 of the Constitution** recognizes economic rights. To be specific**, article 40(2)** recognizes a right of practice or carry out any lawful trade or business.

Therefore the buyers and sellers are cautioned against engaging in illegal transactions to this effect.

It is important to note that the constitution is the supreme law of the land and any other law inconsistent with the constitution is null and void to the extent of its inconsistency. The human rights are to be enjoyed by all people regardless of age, health, race, tribe, religion and Human rights are inherent and not granted by the state.

[73] As amended.

## *The Contracts Act 2010*

The Contract Act is the major law concerning commercial transactions in Uganda. It gives the essential elements of a contract under section 10. Section 10 defines a contract as an agreement made with free consent of parties for a lawful consideration and with a lawful object with intentions of being legally bound. Concerning the mode the Act still recognizes that contracts can be in any form including written form and that a written form can be inform of a data message. **Section 2 of the Electronic Transactions Act** defines a data message as message generated and received by computer means.

## *The Anti-Pornography Act, 2014*

**The Anti-Pornography Act** was adopted in 2014 and criminalizes all forms of pornography. Pornography is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc."

**Section 13** prohibits pornography by restraining people from producing, publishing, broadcasting, procuring, importing, exporting, selling or abetting any form of pornography.

A person who produces or participates in the production of, or traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography contrary to subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding ten years or both. Child Pornography is provided for by section **23** of the **Computer Misuse Act, 2011** and the **Anti-Pornography Act, 2014, Section 14.**

**Section 23 of the Computer Misuse Act, 2011** provides that a person who produces child pornography for purposes of distribution, or avails and distributes pornography to a child commits an offence. The penalty for a person who commits an offence under this section is liable on conviction to a fine not

exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

A child under **section 2 of the Computer Misuse Act, 2011** refers to a person under the age of eighteen years;

However one of the challenges is that the definitions in the act itself are ambiguous. The use of terminologies such as 'sexual excitement' creates an offence that is overbroad, vague, and subjective in character and in contravention of the principle of legality under the constitution and criminal law. The principle of Legality is to the effect that no one can be punished unless the offence is clearly defined. It is expressed in a latin maxim '*nulla poene sine lege'.*

Child pornography is also difficult to define and quantify because it changes with place, location and time. With the ever changing and evolving digital age, understanding what can and cannot get you in legal hot water is critical. Child pornography is just about any image or depiction of a minor in a sexual explicit way. This includes computer-generated images, photos, videos and cell phone pictures. In the digital age, we're seeing more and more child pornography charges involving computers and the internet. Downloading child pornography is illegal.

## *The Computer Misuse Act of 2010*

**The Computer Misuse Act**[74] is intended to "ensure the safety and security of electronic transactions and information systems and information systems to prevent unlawful access or misuse of information systems to prevent unlawful access, abuse or misuse of information systems.

The Computer Misuse Act prescribes liability for offences related to computers and in regard to electronic transactions to be specific, the act criminalizes child pornography and electronic fraud. The maximum penalties for these offences

[74]The long title of the Computer Misuse Act of 201O

range from one to five years of prison, with the exception of child pornography, which can generate the maximum prison sentence of 15 years. The conditions required for these offences to be at hand are, however, often rather vaguely defined. This both contravenes the requirement of unambiguous and foreseeable provisions in international law and can have a hampering effect on freedom of expression.

Computer Misuse Offences are defined in **Section 12 (1) of the Computer Misuse Act.** According to **Section 12 (1) of the Computer Misuse A**ct[75] person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence. Access is defined by section two of the act as gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Electronic fraud is prohibited under **section 19 of the same Act**. S**ection 19 of the Computer Misuse Act defines electronic fraud** to mean deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

The custodial sentences is fifteen years imprisonment. According to **Section 27 of the Act** after conviction, the court must in addition to the fine or custodial sentence or both order the convict to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered.

The punishment itself is deterrent enough to scare away potential criminals. Heavy punishment imprisonment of fifteen years is enough to make one reform.

[75] The Computer Misuse Act 2010

In ***Uganda v. Sentongo and 4 Others***,[76] accused 1 was found guilty of committing Electronic Fraud contrary to **section 19 of the Computer Misuse Act, 2011** and was accordingly convicted. The court stated that to constitute electronic fraud, there must be proof of deception deliberately performed by the accused with the intention of securing an unfair or unlawful gain through a computer network. Accused 1 was found to have been very deceptive when he created electronic ghosts gave them pseudo names and obscene rights to do anything without authorization.

The challenge with this act is that **section 24 and 25**curtail the freedom of expression under **article 29 (1) and 43 (2)(3) of the constitution** limiting freedom of speech.

## *Electronic Transactions Act, 2011*

**Section 2 of the Electronic Transactions Act**[77] defines Electronic transactions is to mean information exchanged or conducted over computer mediated networks concerning the purchase and sale of goods and services between businesses, households, individuals, governments and other public or private organizations. The act recognizes important concepts in line with electronic Transactions and these among others include dispatch and receipt of a data message under **section 15 of the Electronic Transactions Act**[78], receipt of a data message is also recognized under **section 16 of the Electronic Transactions Act** and conclusion of the contract.

**The Electronic Transactions Act, 2011** provides for the use, security, facilitation and regulation of electronic transactions and communications. The Electronic Transactions Act, 2011 forestalls any possible hurdles by providing under **section 8** that the rules of evidence shall not be applied in legal proceedings so as to deny the admissibility of a data message or an electronic record because:

[76] Uganda V Sentogo and four others .High Court (Anti-Corruption Division) Criminal Session Case No. 123 of 2012,
[77] 2011
[78] 2011

a) merely on the ground that it is constituted by a data message or an electronic record;
b) if it is the best evidence that the person adducing the evidence could reasonably be expected to obtain; or
c) merely on the ground that it is not in its original form.

**Subsection (2)** places on a person seeking to introduce a data message or an electronic record in legal proceeding the burden to prove its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

**Section 8 of the Electronic Transactions Act** recognizes the admissibility of data message or electronic record in legal proceedings. The same provisions are found in **section 29 of the Computer Misuse Act.**

In **Dian Gf International Ltd v. Damco Logistics Uganda Limited[79], High Court** the court held that the **Electronic Transactions Act, 2011** recognizes the admissibility of electronic

**Sections 7 of the Act** provides for authenticity of electronic information or a data message.

Electronic commerce or e-commerce, is now part of our daily lives. If consumers and businesses did not believe that the commerce they were transacting was enforceable, they would not enter the digital market place provided by the internet. The internet gives business access to a vast number of consumers and gives businesses access to each other. The first large scale consumer and business use that was made of the World Wide Web was the erection of websites for marketing and advertising purposes.

These sights promoted companies and products. Initially, they did not offer the possibility of selling products and services. Sales took place in parallel through more traditional means of communication. A majority of websites now offer

[79]Dian Gf International Ltd v. Damco Logistics Uganda LimitedHigh Court (Commercial Division) Civil Suit No. 161 of 2010

international and cost effective opportunities for selling goods and services to consumers.

An online marketplace is a method of conducting e-commerce transactions, which connects buyers and sellers. The marketplace itself does not undertake the activity of buying and selling - the sale transactions happen between the actual third party buyers and sellers. Though there exists no standard definition for the term e-commerce, it is generally used in the sense of denoting a method of conducting business through electronic means rather than through conventional physical means. Such electronic means include 'click and buy' methods using computers as well as 'm-commerce' or mobile commerce. This term takes into account not just the act of purchasing goods and/or availing services through an online platform but also all other activities which are associated with any transaction such as:

1. Delivery
2. Payment facilitation
3. Supply chain and service management

The more significant feature of this communication network is that individuals have been empowered to access the widening knowledge repository anytime, anywhere by a click of the mouse. This access is at an inexpensive cost when compared to other current technologies. Some of the day to day activities that consumers indulge in be it buying and selling of various products, availing various services are now facilitated with the growth of e-commerce through platforms like Google, Amazon, Flipkart, Big Basket, Ola, Uber, OLX, etc.

Contracts have become so common in daily life that most of the time we do not even realize that we have entered into one. Right from hiring a taxi to buying airline tickets online, innumerable things in our daily lives are governed by contracts. **The Indian Contract Act, 1872** governs the manner in which contracts are made and executed in India. It governs the way in which the

provisions in a contract are implemented and codifies the effect of a breach of contractual provisions.

## ELEMENTS OF A VALID CONTRACT

The elements a valid contract can be derived from the Contracts Act 2010. They include:

1. Offer and acceptance
2. Intention of parties to form legal relationship
3. Lawful consideration
4. Lawful object
5. Competency of parties
6. Agreements not declared void
7. Impossibility of performance

While the rules on formation of contracts are well established in the offline world, there are significant issues that call for enunciation of legal position in the electronic world.

Electronic contracts are not paper based but rather in electronic form just like trading shares online by holding a Demat Account, which are born out of need for speed, convenience and efficiency. Imagine a contract that an Indian exporter and an American importer wish to enter into. One option would be that one party first draws up two copies of the contract, signs them and couriers them to the other, who in turn signs both the copies and couriers one copy back. The other option is that the two parties meet somewhere and sign the contract. By using e-commerce the whole transaction can be completed in a couple of seconds with both the parties simply affixing their digital signatures to an electronic copy of

the contract. There is no need for delayed couriers and additional travelling costs in such a scenario.

# E-CONTRACTING

One of the key issues of e-contracting is When is a message considered sent or received when it is transmitted through a different mechanism such as emails?' A message is said to be received by a designated mail box when it enters the system. If there is no designation it is also deemed received when the message enters the system of the recipient. If the message is sent to the mail box other than the one designated, it is received when the receiver retrieves the message.[130]

**In e-commerce transactions there are four possible ways to convey acceptance that is;**

1. By sending an email message acceptance.
2. By delivery of an online electronic digital product.
3. By delivery of an online electronic digital service.
4. By delivery of the physical products. Or by any other act or conduct indicating acceptance of the offer.

**Section 4 of the Contracts Act, 2010** provides that the communication of a proposal is complete when it comes to the knowledge of the person to whom it is made. The communication of an acceptance is complete when is it put in course of transmission to him as against the acceptor. In **Entores Ltd V Miles Far East Corporation (1955) 2 QB 327**, the offeree had sent his acceptance from Amsterdam by telex to the offeror in London. Lord Denning held that telex is a virtually instantaneous form of communication which when used makes acceptance through mail box inapplicable. The above view was accepted by the Supreme Court of India in **Bhagwan Das V Girdharilal and Co. (1966) 1 SCR 656.**

The issue as to when a message is deemed to be received poses few questions, example: when the messages will be deemed to be received, when the message is received in A's designated inbox at a remote server or when A actually logs on to his inbox and retrieves the mail. In Germany, jurisdiction practise has established that a message sent by an email id is deemed to be received when it reaches the host computer of the addressee, if the addressee has published the email address on his letter or otherwise makes it publicly known.

In **P.R. Transport Agency V Union of India &Ors AIR 2006 All 23 , Bharat Cooking Coal Lt**d. held an e- auction for coal in different lots. P.R. Transport Agency's bid was accepted for 4000 metric tons of coal from Dobari Colliery. The acceptance letter was issued on 19 July 2005 by PRTA's e-mail address. Acting upon this acceptance PRTA deposited the full amount of Rs. 81.12 Lakhs through a cheque in favour of BCC. This cheque was accepted and encashed by BCC. BCC did not deliver coal to PRTA; instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reason." The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its program or feeding of data the higher bid had not been considered earlier. This communication was challenged by PRTA in the Allahabad High Court. The court held that the acceptance was received by PRTA at Chandauli/ Varanasi. The contract became complete by receipt of such acceptance. Both these places were within the territorial jurisdiction of the High Court. Therefore, a part of the cause of action had arisen in U.P. and the court had territorial jurisdiction.

In another case of **J.K. Enterprise V. State of M.P AIR 1997 MP 68**, according to the plaintiff, he made an offer to the defendant, for the purchase of tendu leaves. It was the stand of the plaintiff that he was never informed that his offer had been accepted. He made the offer on 11.1.1993 and when he did not get the acceptance till 3.3.1993 and thus by a fax message sent on 3.3.1993, he withdrew his offer. In the return filed on behalf of defendant it has been stated that the offer of the plaintiff dated 11.1.1993 was accepted and communicated

under registered cover on the address disclosed by the plaintiff itself and was sent by the letter dated 12.2.1993 which was retuned as the address was incomplete. Defendant further stated that their return that the alleged fax machine dated 3.3.1993 withdrawing the offer was not received by the defendant as it was sent on the wrong fax number.

The court held that the communication of the acceptance of the offer made by the plaintiff was never made by the defendant and as the defendant failed to communicate his acceptance within the given period, the offeror can withdraw his offer.

# TYPES OF ELECTRONIC CONTRACTS

There are several different forms of electronic contracts, most commonly:

## *Click-Wrapor "Click-Through" or "Web-Wrap*

Click-Wrapor "Click-Through" or "Web-Wrap" contacts are electronic contacts that require the user to scroll through terms and conditions (or multiple web pages on a web site) and to expressly confirm the user's agreement to the terms and conditions by taking some action, such as clicking on a button that states "I Accept" or "I Agree" or some similar statement prior to being able to complete the transaction. Click-Through contracts are often found in software products or on Web sites.

In **Rudder v. Microsoft Corporation (1999), 2 C.P.R. (4th) 474 (Ont. S.C.J.),**the plaintiffs commenced a class action lawsuit alleging breach by Microsoft of certain payment related terms of Microsoft's MSN Member Agreement. The Member Agreement was an on-line "click-wrap" agreement that required each prospective member to scroll down through several pages (computer screen pages) of terms and conditions and then indicate their agreement to the terms by clicking an "I Agree" button before being provided with access to the services. Although the plaintiffs wished to rely on several terms of the Member Agreement, in bringing the action the plaintiff's disputed

the choice of law and forum selection clauses (the State of Washington) that the defendant Microsoft sought to enforce. The plaintiffs asserted that because not all of the Member Agreement was visible at one time they did not receive adequate notice of such provisions and that as a consequence they were not enforceable.

The court determined that the Member Agreement was enforceable stating that scrolling through several pages was akin to having to turn through several pages of a multi-page paper contract and to not uphold the agreement "would lead to chaos in the marketplace, render ineffectual electronic commerce and undermine the integrity of any agreement entered into through this medium". **Boon v. Boon (2000), 585 A.P.R. 143 (N.S.S.C**.*)*

One of the earlier decisions in the United States was **CompuServe, Inc v. Patterson 89 F.3d 1257 (6th Cir. 1996).** The CompuServe case involved, inter alia, a dispute by the defendant Patterson of personal jurisdiction of the federal district court for the Southern District of Ohio over Patterson. In considering the personal jurisdiction issue the court determined that the defendant did maintain sufficient contact with that state such to support the district court's exercise of personal jurisdiction over him, a finding that was supported, in part, by Patterson's online contract (AOL's "Shareware Registration Agreement" that incorporated two other sets of terms and conditions by reference) with AOL that the court determined Patterson had entered into. The AOL agreement required Patterson to type "Agree" at various points in the document, "[i]n recognition of your online agreement to all the above terms and conditions".

In **Caspi v. Microsoft Network L.L.C. 732 A.2d 528 (N.J. Super. Ct. App. Div 1999)**a New Jersey court upheld the validity of a click-wrap agreement that, similarly to the Rudder case, contained scrolling terms and conditions that the user was presented with and had to accept prior to being provided access to the service (despite being able to select either an "I Accept" or "I Don't Agree" button without having to scroll through all of the terms). The court specifically noted in Caspi that registration by the user and use of the service could only proceed after the potential subscriber had the opportunity to review and agree to

the membership agreement, including the provision that was in dispute. *See also* **Scott v. Bell Atlantic Corp. 726N.Y.S. 2d 60 (App. Div. 2001).**

In the case of **Forest v. Verizon Communications Inc. 2002 D.C. App. LEXIS 509**, the question was whether a forum selection clause mandating that claims be brought in a particular jurisdiction should be applied to a class action suit involving plaintiffs' attempts to register for and use Verizon's DSL service. The customer users argued that Verizon "did not provide . . . adequate notice of the [forum selection] clause or its significance." To become DSL subscribers, customers had to agree to all the terms of the subscriber agreement, including the forum selection clause. The clause was found in the final section of the main text of the Agreement, which was available through a scroll box on their computer monitors, where only a small portion of the document is visible at any one time. The top portion of the Agreement stated "PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY". The contract was entered into by the subscriber clicking an "Accept" button below the scroll box. The court determined that users were provided adequate notice of the forum selection clause stating "The general rule is that absent fraud or mistake, one who signs a contract is bound by a contract which he has an opportunity to read whether he does so or not." The court noted that in reading through the Agreement before it was accepted, appellant (and other consumers) would have inevitably discovered the forum selection clause. Furthermore, the court determined that the use of a"scroll box" in the electronic version that displays only part of the Agreement at any one time was detrimental to the provision of adequate notice. The court stated that "A contract is no less a contract simply because it is entered into via a computer."

The jurisprudence in the United States currently tends to support the enforceability of "click-wrap" contracts that otherwise conform to and comply with the requirements of contract formation. Some courts have refused to uphold some click-wrap agreements in circumstances where such fundamental contract principles have not otherwise been satisfied, such as communication of the terms and conditions of the proposed agreement.

## *Browse-Wrap*

Browse-Wrap contracts are terms and conditions of use that to do not require the express agreement of a user. They are often located in software or are posted on a Web site and may make some statement that indicates use of the software or Web site constitutes the user's agreement to the terms. Often such terms may not have been brought to the attention of the user.

The enforceability of browse-wrap contracts are somewhat questionable. While some courts in Canada and the United States appear to have accepted that browse-wraps are, in certain circumstances, enforceable, other courts have concluded that such contracts are not enforceable as they fail to provide sufficient notice of the terms and conditions to the user (or even that any such terms even exist).[134] However, in circumstances where sufficient notice of terms has occurred, conducted stipulated by a party as denoting acceptance of terms and conditions can constitute acceptance that leads to enforceable obligations.

The enforceability of browse-wrap is of particular interest because, notwithstanding the current legal reality that "click wrap" agreements may provide contracting parties with a greater degree of legal certainty with respect to confirming the consent of the other party to terms and conditions of the contractual relationship, beginning in the early days of electronic commerce and continuing to a large degree today, "browse-wrap" appears to often be the choice of many on-line businesses and Web sites. Often less legal-oriented considerations govern such a decision, such as a reluctance by marketing departments to "force" its on-line customers through a legal process that perceptually lessens the users' experience. It doesn't help that business managers considering the issue will often find that their competitors and many other businesses have adopted a similar model (the "if they are doing it, it must be ok" philosophy). Thus, less intrusive, albeit arguably less legally effective, often wins the day with many electronic commerce business decision makers. Unfortunately, in this case, it would seem that less is not necessarily better.

**Kanitz v. Rogers Cable In (2002)**, involved a proceeding under the Ontario Class Proceedings Act to stay a proposed class action by the plaintiffs against Rogers on the ground that an agreement between the parties provided for the arbitration of all disputes. The plaintiffs were subscribers to the Rogers@Home service providing for cable modem Internet access services. Activation of the services required a Rogers technician to attend at a new subscriber's home to install the service. At the time of the installation, customers were required to sign the Rogers@Home service agreement ("Agreement") which contained an amendment provision providing that:

"We may change, amend, modify, add or remove portions of the Agreement at any time. We will notify you of any changes to this Agreement by posting notice of such changes on the Roger@Home web site, or by sending notice via email or postal mail. Your continued use of the Service following notice of such change means that you agree to and accept the Agreement as amended. If you do not agree to any modification of this Agreement, you must immediately stop using Rogers@Home and notify us that you are terminating this Agreement."..

Rogers later amended the Agreement to include an arbitration provision and posted an updated Agreement, including the change, on the Rogers@Home Web site. Rogers also posted notice that the Agreement had been amended. The plaintiffs had launched a class action in connection with service outage problems associated with the Rogers@Home service and asserted that they had not agreed to settle disputes by arbitration. In the plaintiffs' view, Rogers was attempting to unilaterally impose arbitration on them by purporting to amend the Agreement without reasonable notice of the change to them and therefore Rogers was not able to rely on the arbitration clause.

While noting that Rogers could have done more to bring the changes to the attention of the plaintiffs, the court in Kanitz concluded that notice of the amendment had been provided in accordance with the terms of the Agreement (i.e. via a Web site posting). The court determined that the effect of the amending provision in the original form of Agreement was to place an obligation on the customer who is interested in any amendments that Rogers may choose to

make to the Agreement to check the Web site from to time to time (and further that such might involve a little investigative work on the part of the customer to locate the relevant parts of the Web site). Importantly, the court also stated that because the plaintiffs continued to use the service subsequent to the amendment to the Agreement and notice of same, under the terms of the Agreement they were each deemed to have accepted the amendments.

In **Kanitz v. Rogers Cable Inc.** above. In Kanitz the court noted the implied method of electronic communications in the context of online relationships when in stating (in paragraph 32) that: "I am also mindful, in reaching my conclusion on this point, of the fact that we are dealing in this case with a different mode of doing business than has heretofore been generally considered by the courts. We are here dealing with people who wish to avail themselves of an electronic environment and the electronic services that are available through it. It does not seem unreasonable for persons, who are seeking electronic access to all manner of goods, services and products along with information, communication, entertainment and other resources, to have the legal attributes of their relationship with the very entity that is providing such electronic access, defined and communicated to them through that electronic format." otherwise be found to have been agreed to by that other party by virtue of that other party's conduct where that conduct manifests acceptance.

U.S. courts have more often held such contacts under Browse wrap to be unenforceable. In **Register.com, Inc. v. Verio, Inc**.[136] at issue was the enforceability of the terms and conditions on Register.com's Web site concerning the conduct of "WHO IS" database searches. The terms provided that by submitting a search inquiry the user agreed to the terms, however it did not require that the user expressly agree to them. The appellate court upheld the terms indicating the defendant's conduct constituted agreement to the terms.

In **Specht v. Netscape Communications Corp 206 F.3d 17 (S.D.N.Y. 2001)** *306 F.3d 17 (2nd Cir. 2002)* issue was the enforceability of an arbitration clause in Netscape's end-user license agreement. The license agreement was available by hypertext link asking users to review and agree to the terms before

downloading and using the software. No express agreement to the terms was required prior to downloading the software from Netscape. In refusing to uphold the enforceability of the browse-wrap agreement the court emphasized the importance in contact formation of assent to the proposed terms of the bargain. The lack of sufficient notice of the proposed terms when combined with the absence of assent was terminal to the enforceability of the Netscape terms.

In **case of Ticketmaster Corp. v. Tickets.com, Inc 2000 U.S. Dist. LEXIS 12987 (C.D. 2000); aff'd 248. F.2d 1173 (9th Cir. 2001)**, the court refused to uphold the enforceability of Ticketmaster's Web site terms and conditions which Ticketmaster claimed had been breached by Tickets com's practice of deep linking to the Ticketmaster site. The Ticketmaster's home page contained "Terms and Conditions" that were only accessible if the visitor to the site scrolled down to the bottom of the page. The court refuted Ticketmaster's claims that the posting of terms was analogous to "shrink-wrap licenses" and concluded that "It cannot be said that merely putting the Terms and Conditions in this fashion necessarily creates a contract with anyone using the web site".

## WEBSITES AND E-COMMERCE

The main thing a business needs to understand is their website. A business's website is a large asset. It is also very vulnerable to cybercrime. There are a few issues a business must consider when it comes to their website:

a) Who will operate the website?

b) Will it be operated on site or off site?

c) What security measures will be employed?

d) How will email be used, and how will privacy be protected?

It's also important that businesses monitor their IP. A good way to do this is with customer review websites. These sites can both help you identify areas for

improvement and can show you if your IP is being used without your permission.

# CUSTOMERS PROTECTION IN ELECTRONIC TRANSACTIONS ACT

An important part of complying with cyber law is protecting your customer's personal information. This is true even if your business doesn't have a website. Many customers make use of online review sites to explain their satisfaction with a company.

The Legal Regime governing the formation of electronic contracts; securing electronic transactions and consumer protection is the **Electronic Transactions Act, No. 8 of 2011, The Electronic Transactions Regulations, The Electronic Signatures Act, No.7 of 2011The Electronic Signatures Regulations, The Contracts Act, 2010.**

The use of modern means of communication, including electronic means such as email, in conducting business is on the increase. This can partly be attributed to increase in technological developments in the area of information and communication technology and increased access to the internet.

For instance, many transactions are now effected electronically. For example, by the use of automated teller machines (ATMs or cash point dispensers outside banks) and electronic fund transfers (EFTs) transactions are made between financial institutions and at the point of sale. More so, many organisations now exchange data electronically. For example, a large manufacturing company may order components automatically and electronically from its suppliers when stock levels reach a predetermined lower limit.

There are however certain hindrances which may be faced in using information and communication technology in business transactions including, skepticism from consumers, questions on security of information and uncertainty of legal validity of such transactions.

# LEGAL CONSEQUENCES ASSOCIATED WITH ELECTRONIC TRADING

The law requires that some contracts are in a particular form for example, by deed or in writing. (This is now covered under the Contracts Act, which defines written contracts to include data message)

There may be doubts as to when the contract was made and, if the parties are in different countries, which country's law will apply to the contract.

**The evidential weight of electronic documents must be considered and assessed.**

**Evidence is defined in section 2 of the Evidence Act**[80]as means by which any alleged matter or fact , the truth of which is submitted to investigation is proved or disproved and includes statements by accused's persons , admissions, judicial notice , presumptions of law and ocular observations by the court in its judicial capacity.

**Document is equally defined in section 2 of the Evidence Act** as any matter expressed or described upon any substance by means of letters, figures marks, or by one or more of those means intended to be used or which may be used for the purpose of recording that matter.

Traditionally the best evidence rule stated that only primary documents are admissible in court for evidential purposes. To this effect even Uganda's evidence Act recognized this principle under **Section 63 of the Evidence Act,** which requires proof of documents by primary evidence . To this effect section 61 of the Evidence Act defines primary evidence production of the document itself except in the cases where secondary evidence may be admissible.

Section 62 defines Secondary evidence to include certified copies, copies made from the original by mechanical processes and copies compared with those

[80] Cap 6

copies, and counterparts of documents as against the parties who did not execute them.

With the advent of technology and increased online transactions, electronic evidence cannot be underestimated. According to **section 8 of the Electronic Transactions Act**, rules of evidence shall not exclude admissibility of electronic evidence. The burden of proof is established under section 8(2) of the Electronic Transactions Act that anyone who seeks to rely on electronic evidence must prove authenticity of the evidence.

Similarly, when one wants to rely on primary evince, he is obliged to prove its authenticity. The electronic documents are recognized because of the technological developments in Uganda which have paved way for online transactions. Several national and international legislations recognize the legal effectiveness of electronic documents and their admissibility as evidence in legal proceedings. In addition, current legislation specifically grants equal standing to the paper / primary documents in for promoting e- commerce.

Consequently, the evidence from electronic document is functionally equivalent to the handwritten document. The signatory and maker of the document is legally bound respecting the commitments made in the signed document once his knowledge and approval of the content of the document are consciously represented by his electronic signature. The electronic signature acts under **section 4(3) of the Electronic Signatures Act** recognizes admissibility and the authenticity of the electronic document in the same way as the handwritten signature does regarding the paper-based document.

Data message is fundamental to the formation of an electronic contract. A data message is defined under **section 2 of the Electronic Transactions** Act to mean the data generated, sent, received or stored by computer means. The effect of this data message is crucial in presenting evidence in the courts of law because it represents authenticity, non-repudiation and integrity by the sender.

**Integrity** means that the data is not tampered during the transfer.

**Non – repudiation** is to the effect that the sender of the signature cannot later repudiate the authorship.

The non-repudiation service protects the parties involved in a transaction against the other party denying that a particular event or action took place. Non repudiation protects against fraud in electronic commerce. Non repudiation works in the following ways such as Non-repudiation of origin, Non-repudiation of receipt, Non-repudiation of delivery, Non-repudiation of submission and Non-repudiation of transport as discussed in the subsequent chapter.

# WRITING CONTRACTS

**Section 10 of the Contracts Act d**efines a contract as an agreement between two or more parties with an intention of creating legal relations for a lawful purpose. Concerning the mode the Act still recognizes that contracts can be in any form including oral, written form or partly written and partly oral. The written form can be inform of a data message. **Section 2 of the Electronic Transactions Act** defines a data message as message generated and received by computer means.

Similarly **section 2 of the Sale of Goods and Supply of Services Act**[81] defines the form of a contract for sale that it can be in writing or by word of mouth, or partly in writing and partly by word of mouth, or implied from the conduct of the parties.

However as earlier discussed, written contracts are given equal importance just like electronic contracts. And in any case written contracts include electronic contracts because **section 10 of the Contracts Act** is to the effect that written contracts include those entered into by a data message. And yet electronic contracts can be commenced by a data message

[81] 2017

# DISPATCH AND RECEIPT OF A DATA MESSAGE

The term dispatch and receipt of a data message are have a significant impact on electronic commerce and can be considered in conjunction with the common law rules of offer and acceptance and time of contract formation.

## *Dispatch of a data message.*

Dispatch of a data message occurs when the message leaves the control of the originator. It happens when the originator clicks the send button.

An invitation to treat is recognized under **Section 18 of the Electronic Transactions Act**, which states that an expression of interest can be made by way of a data message.

According to **section 15 of the Electronic Transactions Act**, a data message is considered dispatched when it enters a single information system outside the control of the person originating the data. **Section 15(2)** provides that If there are more than two information systems, the dispatch occurs when the data message enters the first information system.

However it should be noted that the principle of freedom of a contract is one of the important concepts governing contract law. The principle of freedom of contract means parties can agree on how their transactions can be governed and in addition to this, section 10 of the contracts Act provides for free consent when entering a contract.

This means that parties can choose not to be bound by the wording in section 15 and agree otherwise on when the contract is made, when the information is dispatched.

## *Receipt of a data message*

Section 16 of the Electronic Transactions Act provides for receipt of a data message. The data message is received when it enters an information system specified by the addressee. The concept of receipt has significant practical impacts.

In the case of **West Pac Banking Corporation V Dixon**[82], the word receipt under the Common wealth Electronic Transactions Act was equated with a requirement to give a notice pursuant to section 64D of the 1966 of the Bankruptcy Act.

In the case of **Falgat Constructions Property Limited V Equity Australia Corporation Property Limited**[83], Hodgson J discussed the meaning of the term 'serve, provide, receipt and made'. He concluded that where a document has actually been received and come to the attention of a person to be served or provided with the document, then that means that there has been service, provision and receipt.

In the case of **Auster Finance V Campbel**[84], it was held that where electronic message is received by the third party rather than the intended receivers computer, and there is no hard copy document unless the receiver accesses the email and transmits it on the printer nothing can be said to have been left at the receivers premises until the email is accessed.

On the Internet, the primary means of forming a contract is through the 'clickwrap' agreements, in which website users typically click an 'I agree 'box after being presented with a list of terms and conditions of use.

In **Nicosia v. Amazon.com, Inc., No. 14–CV–4513, 2015 WL 500180, at 7** the court upheld a clickwrap agreement where the Amazon.com user clicked a box acknowledging terms at the initial signup to the website.

---

[8282] 2011 FMCAA 211
[83] 2006) NSWCA 259
[84] 2007 NSWC 678

Facts of the case: the plaintiff filed a putative class action against Amazon.com, Inc. "contending that Amazon has sold and continues to sell weight loss supplements containing sibutramine, a "controlled substance . . . [that has] never been permitted for sale without a prescription from a licensed physician . . . [and that is] associated with a serious risk of cardiovascular events and strokes," in violation of various federal and state consumer protection laws and in breach of various implied warranties." The *Nicosia* court granted Amazon's motion to dismiss because all claims were governed by a mandatory arbitration clause and class action waiver. The court described Amazon's 2012 Conditions of Use agreement as a hybrid between a clickwrap and a browsewrap agreement. "While the Conditions of Use are only available by navigating through a hyperlink, like a browsewrap agreement, a purchaser using Amazon's website could only place his or her order after viewing a conspicuous hyperlink to the current Conditions of Use and agreeing to make his purchase subject to those conditions."

The court stated: Additionally, a purchaser cannot make purchases on Amazon.com without first signing-up for an account, and in that process, expressly assenting to be bound (in a clickwrap agreement) to the terms of Conditions of Use, which are subject to change.

The standard for enforceability therefore, is whether the user has a reasonable opportunity to review terms and manifest assent. Hence, in ***Inc. v. Neato*, 61 F. Supp. 2d 1074, 1080 n. 11 (C.D. Cal. 1999**). The *Stompo* court explained: A 'clickwrap agreement' allows the consumer to manifest its assent to the terms of a contract by "clicking" on an acceptance button on the website. If the consumer does not agree to the contract terms, the website will not accept the consumer's order. Such agreements are common on websites that sell or distribute software programs that the consumer downloads from the website.

The court held that the user assented to conditions of use posted on Amazon.com each time he completed a purchase, "given (1) the conspicuous placement of the hyperlink to the current conditions of use on the checkout page, (2) the express warning at checkout that his purchases were subject to the terms of the current

conditions of use, and (3) the fact that he expressly agreed, when signing-up for an Amazon.com account, to be bound by the terms of the conditions of use (including a provision notifying him that the conditions are subject to change)."

Browse-wrap means that the terms are accessible via a hypertext link. *In* ***Be In Inc. v. Google Inc*****. 2013 WL5568706 (N.D. Cal. Oct. 9, 2013**) court stated that Browse-wrap agreements are those that purport to bind the users of websites to which the agreements are hyperlinked. Therefore, the 'browse-wrap' agreement is where website terms and conditions of use are posted on the website typically as a hyperlink at the bottom of the screen.

Browse-wrap agreements are generally entitled "Terms of Use" or "Terms of Service."

Browsewraps can take various forms but basically the website will contain a notice that—by merely using the services of, obtaining information from, or initiating applications within the website—the user is agreeing to and is bound by the site's terms of service." ***United States v. Drew*****, 259 F.R.D. 449, 462 n.22 (C.D. Cal. 2009).** These terms may be included on the same page as the notice or accessible via a hyperlink. "A hyperlink electronically provides direct access from one internet location/file to another, typically by clicking a highlighted word or icon.

The Ninth Circuit in ***Nguyen v. Barnes & Noble, Inc*****., 763 F.3d 1171 (9th Cir. 2014**) stated that the: defining feature of browsewrap agreements is that the user can continue to use the website or its services without visiting the page hosting the browsewrap agreement or even knowing that such a webpage exists. No affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website.

Browsewrap agreements purport to bind the users of websites to which the agreements are hyperlinked as the ***Be In Inc. v. Google Inc*****.** court states: Browsewrap agreements are those that purport to bind the users of websites to which the agreements are hyperlinked. Generally, the text of the agreement is found on a separate webpage hyperlinked to the website the user is accessing.

Similarly, in *In* ***re Zappos.com, Inc., Customer Data Breach Sec. Litig*****.,** **893 F. Supp. 2d 1058 (D. Nev. 2012)** the court held that a mass market agreement was unenforceable where the hyperlink to the " 'terms of use' was 'inconspicuous, buried in the middle to bottom of every [defendant] webpage among many other links."

Web-wrap denotes a notice attempting to make entry into and further use of the website conditional on posted terms and conditions. The validity of click-wrap methods of acceptance is well accepted as equivalent to incorporation of terms by signature.

# THE ROLE OF INTERNET INTERMEDIARIES IN ELECTRONIC TRANSACTIONS

The implicit meaning of the word intermediary is that it is located between or among two or more parties, and although they help in the transmission/dissemination process, intermediaries do not initiate decisions to disseminate the content, products or services that transverse their networks or servers

An **intermediary** as espoused by the Organization for Economic Co-operation and Development (OECD), is an entity that "brings together or facilitates transactions between third parties and the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet to provide internet-based services to third parties.

As the scale and scope of the Internet has grown to permeate all aspects of the economy and society, so too has the role of Internet intermediaries who provide the Internet's basic infrastructure and platforms by enabling communications and transactions between third parties as well as applications and services. 'Internet intermediaries' give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties. They offer access to a host of activities through both wired and wireless technologies. Most 'Internet intermediaries' are from the business sector and they span a wide range

of online economic activities including: Internet access and service providers (ISPs), data processing and web hosting providers, Internet search engines and portals, e-commerce intermediaries, Internet payment systems, and participative networked platforms.

Intermediation is the process by which a firm, acting as the agent of an individual or another firm, leverages its middleman position to foster communication with other agents in the marketplace that will lead to transactions and exchanges that create economic and/or social value. The main functions of Internet intermediaries are i) to provide infrastructure; ii) to collect, organise and evaluate dispersed information; iii) to facilitate social communication and information exchange; iv) to aggregate supply and demand; v) to facilitate market processes; vi) to provide trust; and vii) to take into account the needs of both buyers/users and sellers/advertisers. There is sometimes tension between various functions of Internet intermediaries; for example, tension between preserving identity and privacy while personalising products and services in ways that benefit users or between infrastructure provision and usage.

Internet intermediaries are important actors because their services create network externalities such that the benefits from using the service increase as diffusion spreads. Therefore, building a critical mass of users is key for these actors. In addition, these actors often operate in two-sided markets whereby they are an intermediary between two different groups of agents, for example, users and advertisers or buyers and sellers. Two-sided markets have implications in terms of causing intermediaries to adopt particular pricing and investment strategies that will get both sides of the market on board, and that balance the interests of the two sides.

In particular, online advertisers, play an important role as they often enable intermediary platforms to provide increasingly sophisticated content and services at no monetary cost to users. In addition to online advertising, revenue models of Internet intermediaries include subscription and 'on-demand' paid service

models, brokerage fees, donations, as well as community development models for content or software.

E-commerce transactions for both consumers and for businesses have become main stream in OECD countries, experiencing continued growth even during the current economic downturn, albeit at lower levels than before but high compared to their offline counterparts for the same period. Retail e-commerce intermediaries often generate revenue through charging sellers transactions fees, while wholesale intermediaries often use a combination of brokerage fees.

Internet payment is predominantly conducted through traditional (offline) payment networks that provide a platform linking merchants that accept cards for payments and cardholders who use them to pay for goods and services, although there are some new entrants in the Internet payment sector..

The emergence of participative networked platforms, including virtual worlds, is a comparatively recent development and online advertising is seen as a main future source of revenue for this sector. In addition, ancillary linked products - in particular mobile - drive traffic, revenue, engagement, and overall value.

Against the broadening base of users worldwide and rapid convergence to IP networks for voice, data, and video, 'Internet intermediaries' provide increasing social and economic benefits; whether it be through information, e-commerce, communication/social networks, participative networks, or web services. 'Internet intermediaries' provide economic growth with new businesses and productivity gains through their contribution to the wider ICT sector as well as through their key role within the Internet ecosystem.[141] They operate and maintain most of the Internet infrastructure, which now underpins economic and social activity at a global level, and are needed to help ensure there is continued sufficient investment in both physical and logical infrastructure to meet the network capacity demands of new applications and of an expanding base of users.

'Internet intermediaries' also stimulate employment and entrepreneurship by lowering the barriers to starting and operating small businesses and by creating

opportunities for 'long-tail' economic transactions to occur that were not previously possible, whereby businesses can sell a large number of unique items, each in relatively small quantities. Internet intermediaries enable creativity and collaboration to flourish among individuals and enterprises and generate innovation. User empowerment and choice are considered to be very important and positive social side effects of the access to information that Internet intermediaries provide, as well as improving purchasing power with downward pressure on prices. A critical role of Internet intermediaries including through protection of user privacy. By enabling individuality and self-expression, they also offer potential improvements to the quality of societies in terms of fundamental values such as freedom and democracy.

'Internet intermediaries' are mainly from the business sector although there are an increasing number of social platforms. Some of the Current Internet intermediaries include:

1. Internet access and service providers (ISPs)
2. Data processing and web hosting providers, including domain name registrars Internet search engines and portals
3. E-commerce intermediaries, where these platforms do not take title to the goods being sold Internet payment systems, and
4. Participative networking platforms, which include Internet publishing and broadcasting platforms that do not themselves create or own the content being published or broadcast.
5. Social Media Platforms

Several caveats warrant stressing. First of all, it is important to note the differences between the categories of actors being clustered under the concept of 'Internet intermediaries'. Additionally, in practice, categories are often not clear-cut as Internet intermediaries may play more than one role. Moreover, statistical definitions tend to focus on Internet information and service sectors in general and do not necessarily distinguish those with an intermediation role.

In considering the role(s) of Internet intermediaries, it is important to appreciate that Internet intermediaries may have different and potentially competing simultaneous roles as intermediaries, end- users and content/service providers. For example, some Internet service providers deliver their own content. Some e-commerce platforms sell goods that they take title to.

## INTERNET ACCESS AND SERVICE PROVIDERS

ISPs may provide local, regional, and/or national coverage for clients or provide backbone services for other Internet service providers. They include 'pure-play' ISPs as well as wired and wireless telecommunications providers, and cable providers that provide Internet access in addition to network infrastructure. Internet service providers have the equipment and telecommunication network access required for a point-of-presence on the Internet. They may also provide related services beyond Internet access, such as web hosting, web page design, and consulting services related to networking software and hardware.

ISPs are typically commercial organisations that generally charge their users - whether households, businesses or governments - a monthly fee on a contractual basis. Sometimes the fee is bundled with other services, as in the "triple play" offered by cable and telephone companies for television, telephone, and Internet access. Laptop users in Internet cafes or wireless "hot spots" may pay an ISP (directly or indirectly) for daily access or even hourly access. ISPs range from large organisations, with their own geographically dispersed networks, local points of presence and numerous connections to other such networks (Tier 1 providers - usually large telecommunications companies), to small providers with a single connection into another organisation's network

## WEB E-COMMERCE INTERMEDIARIES

Web e-commerce intermediaries connect buyers and suppliers and enable Internet transactions between them. They provide a range of often bundled services such as fixing prices, transaction processing and co-ordination, quality

guarantees, monitoring, as well as, in some cases, stock management. An Internet transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments and other public or private organisations, conducted over the Internet. The goods are ordered over the Internet, while the payment and the ultimate delivery of the good or service may be conducted on or off-line.[147]

For the purposes of this report, e-commerce in service industries is excluded. The reason for excluding e-commerce in service industries is the risk of double counting because services sold on- line, such as ISP services, may also be included in separate Internet intermediary sectors (e.g. that of 'Internet access and service providers'). Similarly, Internet search engines often sell advertising on- line that is categorised as e-commerce service revenue. The following categories of actors are included:

**Business-to-business (B2B)** electronic markets using the Internet: business-to-business marketplaces facilitate business-to-business electronic sales of new and used merchandise using the Internet, often on an auction basis, and generally receive a commission or fee for the service. Business-to- business electronic markets for durable and nondurable goods are included. It should be noted that while several existing definitions of e-commerce include Electronic Data Interchange (EDI), EDI Transactions are excluded from the present report that is limited to 'Web e-commerce intermediaries', because EDI uses proprietary non-Internet networks. This exclusion is significant because a majority of B2B e-commerce is via EDI (for example in 2007, EDI represented 73.5% of merchant wholesalers' e-commerce activity in the United States).

# E-COMMERCE PAYMENT SYSTEMS

E-commerce payment systems generally include: i) payment systems that rely on a credit or bank account to enable e-commerce transactions (e.g. Visa, Mastercard); and ii) payment systems provided by non-bank institutions operating on the Internet and that are only indirectly associated with a bank account (e.g. Paypal).

Banks remain the core providers to end-users for most online retail payment instruments and services. Payments for Internet transactions in most OECD countries are overwhelmingly conducted through credit cards.[150] Payment networks Visa and MasterCard are not-for-profit associations owned by banks and nonbanks that centrally set the fees that the merchants' banks (acquirers) pay to the cardholders' banks (issuers) for transactions. These fees are proportional to transaction volume. The payment networks' choice of fees has typically favoured cardholders, to induce them to use their cards, over merchants, who kept accepting the cards despite relatively high levels of merchant fees.

Online banking-based Internet payments are a growing category of Internet payments, particularly in Europe. Buyers initiate transactions at a merchant's website and are redirected to an interface putting them in touch with their own online bank for payment authorisation. The merchant receives an instant payment confirmation, after which the money arrives as a regular credit transfer. There are three main types of online banking-based payment systems.

a) Multi-bank schemes, where merchants have a connection with all banks, generally via a payment service provider. Examples of multi-bank payment methods include EPS in Austria, e-Dankort in Denmark, iDEAL in the Netherlands, Bancontact/Mister Cash in Belgium, Giropay in Germany, Bank Axess in Norway, Secure Vault Payments in the United States, or Interac in Canada.

b) Mono-bank solutions, whereby merchants need only to connect with one of the participating banks. Mono-bank payment methods include Nordea Solo in Norway, Sweden, Denmark, Finland, and the Baltics or ING, Dexia, and KBC in Belgium.

c) Bank-independent intermediary payment solutions, whereby the online interfaces of intermediary payment solutions enable to connect consumers' to their online banking portals. These include POLi in Australia, New Zealand, South Africa, and the United Kingdom, Mazooma in the United States, or Sofortueberweisung /

DIRECTebanking.com in Germany, Austria, Switzerland, and the Netherlands.

In general, the use of non-card and non-bank payment methods is growing with actors such as eBay with Paypal, Amazon, or Google. Payment applications such as mediating services, mobile payment systems, prepaid cards or electronic currency are available from a wider range of service providers.

Banks now serve as Internet payment portals, transferring payments between payers, payees and their account-holding institutions, and also transferring payments between buyers and sellers who transact through Internet retail storefronts and through online auction sites.

# ROLE OF INTERNET INTERMEDIARIES

Intermediation is the process by which a firm, acting as the agent of an individual or another firm (a buyer or seller), leverages its middleman position to foster communication with other agents in the marketplace that will lead to transactions and exchanges that create economic and/or social value. There are a number of roles that an intermediary can play that lead to the creation of value. They include: aggregation of information on buyers, suppliers and products; facilitation of search for appropriate products; reduction of information asymmetries through the provision of product and transactional expertise; matching buyers and sellers for transactions; and trust provision to the marketplace to enhance transactability.

**The main functions of intermediaries have been studied quite widely in literature and can be summarised as follows:**

1. To provide the infrastructure
2. To collect, organise and evaluate dispersed information
3. To facilitate social communication and information exchange
4. To aggregate supply and demand

5. To facilitate market processes
6. To provide trust; and
7. To take into account the needs of buyers and sellers or users and customers.

To fulfill these functions over the Internet, different types of intermediaries have developed and include: access and storage providers, marketplace exchanges, buy/sell fulfillment, demand collection systems, auction brokers, virtual marketplaces, as well as search-engines, advertising networks, web aggregators, news syndicators or social networking sites.

The value-added chain is the set of relationships of agents with other agents, the network of upstream and downstream businesses, from raw materials to final sale, through which a product travels. At every stage of processing, an intermediary often performs a service which facilitates this flow - adding value but also adding cost. In many cases, this service is information intensive - matching a buyer to a seller, certifying parties in a transaction, providing support for the transaction (e.g. financial services) - and often involves some type of risk sharing. For example, auction e-commerce sites provide trading mechanisms to facilitate market processes, and at the same time provide information and aggregation/matching services by making it known that a given good is on sale, by identifying the tastes of users and signaling when something of interest comes up, by providing means for the buyer to assess the quality or the aspect of the good, the reputation of the sellers, and by providing guarantees to trade safely.

There are often challenges for intermediaries in performing their various functions. For example, there may be challenges For example, there may be challenges in balancing the request for personal information in order to offer personalized services with the need to safeguard individual rights, in particular the right to privacy and the protection of personal data. There may also be challenges to ensure there is sufficient investment in infrastructure to meet network capacity demands, while maintaining the openness that has characterized the Internet's success to date. A related issue is how best to

stimulate "creative destruction"[154] and innovation in communications infrastructure, while at the same time creating an environment that supports investment.

There may also be challenges between ease of use and transparency / disclosure for consumer protection. Taking advantage of the benefits of cloud computing while mitigating the security and privacy risks of having so much online information under third party control is another important challenge, as is enhancing network security while enabling access to the information that users demand and allowing unexpected innovation at "the edges."

## NETWORK EXTERNALITIES

By nature new Internet services create network externalities (or network effects) such that the benefits from using the service increase as diffusion spreads. In other words, the value that one user receives from a product increases with the number of other users of that product. Once a critical mass of users is reached, a virtuous process of demand for the service is initiated.

Therefore, building a critical mass of users is crucial to most Internet intermediary business models. In addition to network externalities, many intermediary platforms benefit from increasing economies of scale (unit costs decrease as sales increase). Internet access and service providers for example have significant network externalities and large economies of scale. The economic models of search engines and participative networked platforms or online auction sites also tend to rely on volume impact, distributing electronic content and services at low marginal cost and high unit margins.

Non-rivalry (one person's consumption does not limit or reduce the value of the product to other consumers) is another characteristic of many intermediary markets. Combined, these factors can tend to lead to 'winner-take-most' markets, creating powerful incumbents and tending away from perfectly competitive markets.

Advertising is an important driver for content and services that are available at no or little direct cost on the Internet, as are, to a lesser extent, ancillary service fees and premium product sales with higher margin returns. On the Internet, intermediary platforms are willing to provide services to their users at no monetary cost in order to generate the audience to attract advertisers, to attract sellers, or to be able to offer premium paid services. Consistent with this trend, economic research on net work has been complemented by the analysis of intergroup externalities present in two-sided markets.

# TWO-SIDED MARKETS

Two-sided markets are economic networks having two distinct user groups that provide each other with network benefits. Examples include Internet search engines and portals - composed of advertisers and users; retail e-commerce platforms - composed of buyers and sellers; or payment networks - composed of cardholders and merchants. Benefits to each group exhibit demand economies of scale. Consumers, for example, prefer credit cards honoured by more merchants, while merchants prefer cards carried by more consumers

A market is two-sided if at any point in time there are: i) two distinct groups of users; ii) the value obtained by one type of user increases with the number or with the 'quality' of the other kind of users; and iii) an intermediary platform is necessary to internalise the externalities created by one group for the other group. Two-sided markets result in intermediaries that supply both sides of the market, that adopt particular pricing and investment strategies to get both sides of the market to participate, and that adopt particular pricing and product strategies to balance the interests of the two sides.29 In a two-sided market, an intermediary platform internalises the inter-group network externalities, e.g. the fact that the volume of advertising generated by a search engine depends on the number of users on the other side.

## *Characteristics of two-sided markets*

The need to get both sides of the market to participate: To succeed, intermediaries in industries such as software, portals and media, payment systems and the Internet, must "get both sides of the market on board."

Pricing strategies and balancing interests: even with both sides "on board," intermediaries need to carefully balance their two demands and consider how price changes on one side of the market may impact the other side.

Multihoming: most two-sided markets seem to have several competing two-sided firms and at least one side appears to multi home, i.e. to use more than one provider. For example, many merchants accept both American Express and Visa; furthermore, some consumers have both Amex and Visa cards. B2B exchange members may buy or sell their products or services on several exchanges, with competitive prices on one market then depending on the extent of multihoming on the other side of the market

In a two-sided network, members of each group have a preference regarding the number of users in the other group, known as cross-side network effects. Cross-side network effects are usually positive (e.g. consumers often prefer retail sites with more products and prefer payment systems supported by more merchants), but can also be negative (e.g. consumer reactions to large quantities of advertising). Each group's members may also have preferences regarding the number of users in their own group, known as same-side network effects. Same-side network effects may be either positive (e.g. the benefit from social networking with a larger number of people) or negative (e.g. to exclude direct rivals from advertising on the same keywords).

In two-sided networks, users on each side typically require very different functionalities from their common platform, which means the platform incurs different costs in serving the two groups of users. With search engines, for example, users require efficient relevant search functionality and potentially other services such as e-mail, etc. Advertisers, on the other hand, may require software and services to help them determine relevant keywords, to place auction bids on keywords, to create ads, manage spending, process transactions, etc.

Value chains of two-sided networks also differ from traditional value chains on the revenue side. A key strategic issue for most Internet intermediaries operating in two-sided markets is to find an optimal pricing structure, i.e. the division of revenues between the two sides of the market that gets both sides to participate. The 'chicken and egg' problem - a platform must have a large installed base of content, products or services to attract users, but advertisers will only pay to finance programmes if they are sure to reach many users - means that the optimal price system can often be to subsidise one side of the market to attract users on the other side, treating one side as a profit center and the other as a loss leader.

Intermediary platforms generally subsidise the more price sensitive user group (e.g. consumers) or the user group that adds platform value (e.g. developers of applications for the iPhone who increase the value or functionality of the network), and charge the side whose demand increases most in response to growth on the other side. Which market represents the profit-making side and which market represents the loss- leader side depends on the tradeoff between increasing network size versus growing network value.

## REVENUE MODELS

As mentioned previously, various Internet intermediaries use different business models including advertising, paid subscriptions or renting hosting space, charging for premium services, commission fees, voluntary donations, or combinations of these business models.

In addition, more complex producer-consumer models are emerging where the intermediary platform providers may have one revenue stream but the producer-consumers have another and there is a symbiotic relationship between the two. Examples might include application developers on Facebook, vendors in Second Life, mod-makers in World of Warcraft, or individuals licensing photographs via Flickr.

## *Advertising model*

The Internet advertising model is an extension of the traditional media broadcast model whereby the intermediary provides content and services for free alongside advertising or branding/co-branding messages. This model works best when the volume of viewer traffic is very large or very specialised (e.g. a search query). The following business model categorisation builds on previous OECD work on digital content.

1. Display ads are advertisements in text image or multimedia format, on portals such as Yahoo! or specialised websites. In some cases, ad servers analyse the content of web pages and automatically deliver advertisements that they consider relevant to users.

2. Classified ads are listings of certain products or services on a webpage, e.g. Craigslist.

3. E-mail advertising consists of ads delivered through any type of electronic mail and may take a variety of forms including links, banner ads or advertiser sponsorships placed within an e-mail message.

4. Referrals are a method by which advertisers pay fees to online companies that refer purchase requests (such as shopping comparison sites) or provide customer information. For example credit card companies often invite their customers to receive commercial messages from "affiliated merchants" such as rental-car companies via e-mail or may ask their customers permission to share some information, such as contact information, with selected "commercial partners."

5. Selling user data involves the sale of anonymous or non-anonymous information about users to market research and other firms.

# PRINCIPLES OF ONLINE CONTRACTING

The postal contract law provides that written acceptance completes the contract once it has been posted. This principle is correspondent to the principle of non-discrimination under e- commerce that there shall be no discrimination made between written documents and electronic data. This common law rule has been adopted widely in the Indian courts. This view was accepted by the Supreme Court of India in **Bhagwan Das V. Girdharilal Co(1996) 1 SCR 656.**

The general rule regarding instantaneous communication was laid down **Entores Ltd. V. Miles Far East Corporation (1955) 2 QB 327 where** Lord Denning held that the contract will only be completed when the acceptance has been received by the offeror. The contract will be made at the place where the acceptance was received and at what time it was received. When this rule was applied to fax, the court found the contract was made where and when the acceptance was received.

In Uganda, we do not have a consumer protection Act. In India however, the Consumer Protection Act, 1986 is applicable even in the context of online e-commerce transactions in the case of **Anupama Purohit V. Make My Trip.com Decided by Consumer Disputes Redressal Forum/ II o**nTthe court held that the defendant had committed both deficiency of services and was guilty of unfair trade practises within the meaning of Consumer Protection Act, 1986 when it failed to allot a room to the complainant despite having received an advance payment and giving confirmation of the same to the complainant. Further the defendant unauthorised debited twice the account of the complainant by using his credit card details and password that were used to make an online payment to the defendant. Therefore courts in India apply consumer protection legislation to transactions in the e-commerce world made by consumers to protect their general interests.

In Uganda, we have a number of laws that attempt to guarantee the consumer some form of electronic protection.

# LIABILITY OF INTERMEDIARIES FOR WRONG ACTIONS

When it comes to the modern supply chain, the linkages between different players are changing. Wholesalers continue to serve an important function in the supply chain. However, their role is no longer confined to purchasing from suppliers to distribute to retailers. In order to survive, they must provide a tangible value adding function that's clear to their customers.

The rise of e-commerce platforms such as eBay, Amazon, Flipkart and ASOS etc. indicates the rise of a whole new type of intermediaries. It's an interesting new way to think about the supply chain. Platforms are an additional rung in the chain and are also merely a medium for those who further up the supply chain to connect with those that are further down, by bypassing traditional linkages. Regardless of its role in the supply chain however, the simple fact remains that the trend towards B2C firms selling through hosted platforms is inevitable. Trust and convenience are the two primary factors giving rise to the role of intermediaries. Backed by big names like Amazon, consumers feel assured that certain consumer protection policies are in place. ASOS for instance, offers a 14 day returns policy. Given the multitude of alternative options on the internet, maintaining trust in the platform is central to its success. Active reviewers are also a big part of creating and maintaining a functional and trustworthy platform. Online reviews have become an integral part of the purchasing process. With online platforms, where sellers can access a larger customer base, there are also likely to be more reviews available for consumers to evaluate their purchasing decision.

At a basic level, the internet's technology requires the insertion of intermediaries between interacting parties in two ways. First, for all the transactions over the internet, the communication necessarily involves the internet itself, as well as the parties necessary to facilitate the particular communication, with the exception of few entities involved in direct internet transmissions. Secondly, commercial transactions on the internet require the use of other intermediaries.

A network service provider represents an interactive network service. It may provide access to the internet only or offer a range of additional resources. Depending upon its functional attributes a network service provider may act as an 'information carrier' or 'information publisher'. A network service provider means any person who provides access to information service in electronic form. They perform two tasks:

a. To provide access to the network.

b. To act as an "intermediary" with respect to any particular electronic message.

The function of a network service provider has to be understood in the terms of its role as a facilitator with respect to any particular electronic message between an "originator" and an "addressee". These network service providers act as intermediaries between the originator and addressee. This does not mean that all intermediaries are network service providers. For instance, a search engine like Google though may be referred to as an intermediary but it is not a network service provider.

It is possible that the "information publisher" is not only publishing its own "in-house" content but also buys from other content providers; this does not make the service provider "less of a publisher". An act of publication includes distribution also. The conditions under which they shall be liable are:

a. The Internet Service Provider (ISP) knows, or has a reason to believe that the information content it is transmitting is unlawful.

b. Regardless of the ISP's knowledge, it benefits directly from the transmission i.e., it receives benefits beyond the indirect benefit that is receives from internet access fees.

c. The ISP fails to take reasonable steps to determine if the information content that it transmits is unlawful.

The ICT laws do not necessary provide that network service providers are liable for every action by third parties. However, there is an obligation placed on them to ensure that crime is not committed on their platforms. This platform is highly contentious given the limited control of service providers over their consumers' needs and choices.

# ADVANTAGES AND DISADVANTAGES OF E-COMMERCE

## *Advantages of E-Commerce*

**Availability.** The sites are available full time. Allowing visitors to browse, and shop at any time.

**Speed of access.** While shoppers in a physical store, can be slowed by crowds, e-sites run quickly which is determined by compute and bandwidth considerations on both consumer device and e-commerce site. Product pages and shopping cart pages load in a few seconds or less. An e-commerce transaction can comprise a few clicks and in less than five minutes.

**International reach.** Other physical business sites can sell to customers who can access them. / visit them physically. With the e-commerce, businesses can sell to any customer who can access the website.

**Wide availability**. It enables brands to make a wide array of products to make wide array of products available, which are then shipped from a ware house after purchase is made. Customers are more likely to have chances of succeeding in getting what they want.

## *Disadvantages of E-Commerce*

**Limited customer services**. Consumers are not able to see or touch a product prior to the purchase and wait time for product shipping. A customer in a physical store can inquire from the cashier, or attendant in a physical store in

case of anything. In an e-commerce store, customer service be limited. The site may only provide support during certain hours of the day or a call to customer service phone number may keep the customer on hold.

**Not being able to touch or see**. With images on websites can provide a good sense about a product. It is different from experiencing it directly. E-commerce can lead customers to receive products that differ from their expectations.

**Security Problems**. Skilled hackers can create authentic websites that claim to sell products . Instead the site sends customers forfeit or imitation versions of those products. Or simply collects customer's credit information.

The validity of click-wrap methods of acceptance is well accepted as equivalent to incorporation of terms by signature.

CHAPTER 09

# ELECTRONIC SIGNATURES

## INTRODUCTION

During the start of mid-19th century, the contracts and business transactions were carried out using telegraph machines; Morse code encryption signature was used to verify the authenticity of the signer. From then the digital signature law was born. **Lamport signatures, Markel signatures, Rabin** signatures were the early digital signatures those were developed, but they were not efficient. In 1989, the first well known digital signature software package Lotus 1.0 was released.

The legality of digital signatures was upheld in a New Hampshire supreme court ruling as early as 1869. Then the fax machines were used widely, so the digital signature law was revised accordingly. After that the ATM's, click-to-accept the software license; digital signature law has been revised again and again to match the growth of technology. Recently the growth of e-commerce and e-business has altered the digital signature and its law. The UN published the UNCITRAL Model Law on Electronic Commerce in 1996 that gave uniform standards for digital signature legislation for the e-business and e-commerce, which has a global game. Soon some governments started implementing the digital signature law.

Despite the security risks, data is routinely transferred over the Internet throughout the commercial world. Paper is rapidly giving way to purely electronic forms of documentation. This trend includes the increased use of electronic, documents in the formation of contracts. Electronic contracts, like their paper counterparts, are subject to contract formalities requiring "signatures". There are many ways to "sign" an electronic contract. A simple text signature closing an e- mail message is a common example. Another example is a "mouse click" that indicates the intent to be bound by certain legal terms on a Web page. Although simple methods such as these theoretically may satisfy the formality of signature, they lack many of the inherent security attributes of signed paper documents, such as "semi permanence of ink embedded in paper, unique attributes of some printing processes, watermarks, the distinctiveness of individual signatures, and the limited ability to erase, interlineate, or otherwise modify words on paper." Furthermore, in order to overcome the Internet's inherent security risks, electronic signatures must serve three critical purposes;

a) To identify the source or sender,
b) To indicate the sender's intent (for example, to be bound by the terms of a contract), and
c) To ensure the integrity of the document signed. Text e-mail signatures, mouse clicks, and the like apparently fail to serve these purposes.

The term "digital signature" usually describes an electronic signature, which has been produced through the use of public key cryptography. Often both terms seem to be used interchangeably. Electronic signatures today are based on a so-called asymmetric cryptosystem, which uses two keys, a private one and a public one. Only the originator can generate the digital signature, but anyone can verify the message with the public key. This method makes it possible to ascertain whether the data has been encrypted with a certain private key, which in turn is particular to a certain signatory. Digital signature technology was developed to address the authentication needs of companies and consumers as they engage in transactions online, allowing parties to authenticate their electronic documents in

the open network of the Internet to compensate for the lack of printed documents. The digital signature becomes a part of a message, which indicates the source of the message and shows that the message has not been altered in transit.

## DEFINITION OF ELECTRONIC SIGNATURES

Simply put, Electronic signature means data in electronic form, which is attached to other electronic data and which serves as a method of authentication.[85]

This system asks for someone-called a "Trusted Third Party"-to be responsible for the attribution of a key to a certain person. The private key is allotted to a signatory by a certification authority, which may be either a public or a private organization. The certificates handed out and administered by these certification service providers serve to identify the signatory. The individual seeking to be certified is called a "subscriber," and the party using the certificate to identify the subscriber is known as the "relying party." Electronic commerce depends on the development of trusted certification services, which support the electronic signatures that will permit users to know who they are communicating with on the Internet.

**Section 2 of the Electronic Signatures Act, [86]** defines an electronic signature to mean data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message. It is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient. e-Signatures demonstrate an individual's consent to any agreement.

[85] Chanakya Jayadeva – Electronic Signatures – Perspectives and Problems
[86] 2011

Online authentication is necessary in the fast growing digital environment. Lot of different kinds of electronic signatures are available to authenticate, in which electronic signature is one of the powerful authentication method. Digital / electronic signature not only authenticates the person, who sends the data, also ensures the integrity of the data transferred, making sure that the data has not been tampered while it is transferred. Digital signature software is a powerful business tool in recent years that is used to sign documents, contracts, e-tax filing etc.

Electronic signature cryptosystem is based on public key cryptography where there is a key pair that consists of a public key, publicly known, and a private key, only known by the signatory. Other configurations where the private key is stored in a central key management system for key escrow and further recovery may be implemented.

Using electronic signature cryptosystem, the signatory can generate a digital signature on certain data by using his private key. Afterwards, a relying party or verifier can use the public key to verify the digital signature. Therefore, a digital signature based on public key cryptography can be used to authenticate the signatory as the signature is created using means that the signatory can maintain under his

The United Nations published the **UNCITRAL Model Law on Electronic Commerce in 1996** that gave uniform standards for digital signature legislation for the e-business and e-commerce. Most of the countries started following it. The document is legally bounded when it is digitally signed.

UNCITRAL defines electronic signature as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".

Digital or electronic signature law may slightly vary between countries. The awareness and percentage of people using digital signature also varies between countries. In developing countries, percentage of internet users are very less

when compare to the developed countries, which is directly proportional to the users of digital signature.

The emerging trades between countries are made easy and more secure by using digital signature. Thus knowledge about the digital signature law in different countries and the perspective of people towards digital signature becomes important. The purpose of digital signatures is to authenticate digital documents and give them a purpose.

In today's business world, complex work flow formats and convenient interfacing allow us to introduce attacks that are mere manipulations of the internal ability of workflow format to introduce dynamic content.

The electronic signature has become a key element in the information society. Several national and international legislations recognize the legal effectiveness of electronic signatures and their admissibility as evidence in legal proceedings. In addition, current legislation specifically grants electronic signatures an important role for promoting e- commerce.

Consequently, the electronic signature is functionally equivalent to the handwritten signature. The signatory is legally bound respecting the commitments made in the signed document once his knowledge and approval of the content of the document are consciously represented by his electronic signature. The electronic signature acts as instrument of evidence regarding the authenticity of the electronic document in the same way as the handwritten signature does regarding the paper-based document.

An electronic signature which conforms to these requirements (functional equivalence) will have legal effect, no matter its nature or technical background. This model grants to market forces the power to decide what constitutes an electronic signature.

**Section 4** of the **Electronic Signatures Act, 2010 (ESA)** provides that;

1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as

reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of all the circumstances, including any relevant agreement.

2) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subsection (1)

It must fulfill the following requirements; i.e if—

a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;
c) any alteration to the electronic signature, made after the time of signing, is detectable; and
d) where a purpose of legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable,

The reliability of a signature is challengeable. Subsection 4 allows that a person may adduce evidence proving the unreliability of an electronic signature.

**Neocleous v Rees (2019) EWHC 2462** concerned informal e-mail sign-off plus auto-appended name and contact details which were held to satisfy statutory requirement for a signature.

In English law a contract for the sale of land must be "signed by or on behalf of" the seller and purchaser. In this dispute, the seller's solicitor sent an e-mail offering terms for the sale of his client's land. He finished 'Many thanks', then pressed Send. The firm's e-mail system automatically appended his name and contact details to the foot of the e-mail. The purchaser's solicitor accepted the offer. The judge rejected an argument that a handwritten name, or at least a facsimile of such handwriting, was required.

A qualified electronic signature is legally equivalent to a hand-written signature, complying with the formal requirements established for the latter. The European Directive indicates that these electronic signatures "satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data". Notwithstanding, electronic signatures not considered as qualified are legally recognized as well according to the European Directive and the Spanish Law. **Article 5.2 of the Directive** states that "Member states shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device". In Uganda, **section 7 of the electronic Transactions Act** provide for admissibility of electronic evidence.

**What is a "Signature "for?**

A manuscript signature is accepted without question as legally effective in all jurisdictions, assuming it has not been procured by fraud, and it is rarely asked what effects such a signature is required by law to achieve. However, in those cases where the validity of alternatives has been considered, other methods of signing a document, such as signature by means of a printed or rubber stamp facsimile, have been assessed for validity. The most common approach is to define the functions that a signature must perform, and then to treat signature methods that affect those functions as valid signatures.

The primary function of a physical signature is to provide evidence of three matters:

- the identity of the signatory
- that the signatory intended the signature to be his signature
- that the signatory approves of and adopts the contents of the document.

In **M. Kantha v. P. Valmurthy**[87] It was argued that the appellant at the time of signing the contract was drunk and had no mental equilibrium and so that the respondent cunningly obtained the signature and document. Court expounded on the importance of a signature in signed documents as was an issue too in **L'estrange v. Graucob.**

Manuscript signatures meet these functional requirements in a number of ways. Identity is established by comparing the signature on the document with other signatures that can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that, therefore, such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signatures are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Also, intention to sign is normally presumed because the act of affixing a manuscript signature to a document is universally recognized as signing[88]. Intention to sign is normally only disputed where the affixing of the signature has been procured by fraud, and in those cases the signatory bears the burden of displacing the presumption that he intended to sign. Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.

In the context of Internet communications, the thing to be signed, an electronic document, exists more as a matter of metaphysics than as a physical object. For this reason, it is very difficult for an electronic signature method to meet any physical requirement of form. For example, some of the English cases and statutes on physical world signatures appear to state that a signature must take the form of a mark on a document

[87] Appeal suite no. 493 of 2008 [2011]

[88]Bluesky International Marketing, Market Facts Index, at http://www.blueskyinc.com/factindx.htm (last visited Dec. 5, 2021).

# THE VALIDITY OF E-SIGNATURES

It is a fundamental requirement of electronic commerce that the transactions entered into via electronic communication should be legally binding on the parties. For a large class of business-to-consumer (B2C) transactions, this presents no real difficulty. The physical world carries out B2C transactions without any formalities at all but this is not the same case for the digital world.[89]

Often as it is that in every contract, there must be acceptance to an offer made therein[90], so electronic signatures are to the effect that they fulfill this contractual requirement. Acceptance is one person's compliance with the terms of an offer made by another person or it is the unconditional consent to the terms of the offer. It is important that for a contract to be binding, the acceptance is in specific reference to the offer and that the offeree must accept all the terms of the offer as emphasized in **International Bus MachsCorp v. Johnson[91].** This is also captured in the contractual element of "consensus ad idem." In **Bhagwandas Goverdhandas V. M/s. Girdharilal (1966),** court stated that acceptance and intimation if acceptance of offer are therefore both necessary to result in a binding contract. A common way to signify acceptance in E-contracts is for two parties to sign a document together and the rule of signed documents takes effect as established in **L'Estrange v. Graucob Ltd[92]**and expounded on in the Ugandan case of **Opia v. Chukia[93]**

Thence, the requirement of a signature, be it an electronic signature is to authenticate acceptability to an offer or any transaction. Borrowing from article 1366 of the French Civil code; an electronic riding has the same evidentiary values as a paper based writing, on condition that the person from whom it emanates can be duly identified and that it be created and preserved under conditions guaranteeing its integrity.

---

[89] Chanakya Jayadeva – Electronic Signatures – Perspectives & Problems accessed at https://www.lawnet.gov.lk on 16th Dec, 2021
[90] See section 10 of the Contracts Act 2010
[91] 629 F. Supp S.DN.Y (2009)
[92] [1934] 2kb 394
[93] 5 ors CS 22 OF (2013)UGHCCD 117

"An electronic signature is capable in law of being used to execute a document (including a deed) provided that

(i) The person signing the document intends to authenticate the document and

(ii) Any formalities relating to execution of that document are satisfied." There is support for this in **Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd (2012) EWCA Civ 265.** This case represents a situation where Cases in which an informal electronic signature has been held to satisfy a statutory requirement for a signature.

This case concerned a contract of guarantee, which under S.4 of the Statute of Frauds 1677 had to be signed by or on behalf of the guarantor in order to be enforceable. The contract was said to be formed in a series of e-mails. It was common ground between the parties in the Court of Appeal that for the purposes of s.4 "an electronic signature is sufficient and that a first name, initials, or perhaps a nickname will suffice".

When judicial decisions have arisen, the dispute has tended to be about whether a specific statutory signature requirement was satisfied, whether informal insertion of a name was intended to be a signature, or whether the correct person applied the electronic signature.

Although informal electronic signatures, such as typing a name at the end of an e-mail, can readily count as a signature in English law, they, however, have greater potential to give rise to uncertainty and disputes than does an electronic signature applied using the kind of structured processes and evidential records available in an electronic signature signing platform, such as DocuSign eSignature.

In multiple cases, informal electronic signatures have been held to satisfy a statutory requirement for a signature.

In **Bassano v Toft**[94]it was held that Clicking on an "I accept" button held to satisfy a statutory requirement for a signature. This case concerned a consumer loan agreement, which under consumer credit legislation had to be signed by the borrower. The judge held that clicking on an "I accept" button in an electronic document satisfied the signature requirement.

# TYPES OF ELECTRONIC SIGNATURES

**Qualified signature**

That means that, if it is proved that the signature is a qualified one, the alleged signatory must provide evidence that questions, beyond reasonable doubt, its security in case its authorship, and thus of the signed document, is repudiated. The onus of proof is legally reversed, moving the burden of proof to the alleged signatory instead of to the verifier.

**Advanced or basic signature**

In case of a basic or advanced signature, the alleged signatory is also capable of repudiating the authorship but it is the other party the one who must provide evidence that support the reliability of the signature.

Advanced electronic signatures are electronic signatures which are uniquely linked to the signatory, are capable of identifying the signatory, are created using means that the signatory can maintain under his sole control, and are linked to the electronic data to which they relate in such a manner that any subsequent change of the data is detectable. Thus, an advanced electronic signature is apt to both identify the signatory and to provide proof against falsification of the data it accompanies. According to ***section 2*** of the ***Electronic*** **Signatures Act, 2010,** "advanced electronic signature" means an electronic signature, which is

a) uniquely linked to the signatory;
b) reliably capable of identifying the signatory;

[94](2014) EWHC 377

c) created using .secure signature creation device that the signatory can maintain; and
d) Linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable;

Advanced signatures are mentioned in **section 10** which states that;

a) An advanced electronic signature, verified with a qualified certificate, is equal to an autographic signature in relation to data in electronic form and has therefore equal legal effectiveness and admissibility as evidence.
b) the authenticity and validity of the certificate required at the time of signature verification are verified;

In **Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd (2012) EWCA Civ 265** it was held that a first name, initials, or perhaps a nickname can amount to an authentic electronic signature.

Some authors make the assumption that the qualified signature is given a iuris tantum presumption of authenticity that is, the alleged signatory is given the chance to provide evidence that contradicts the established presumption of authenticity of the signature.

The situation would be different if the presumption of authenticity followed the iuris et de iure principle, supported by other authors, and that implies that the alleged signatory is not given the chance to refute the authenticity of the qualified signature. Here, the alleged signatory is automatically assumed to be the actual signatory, having to deal with the consequences always. Take for instance, the **UNCITRAL Model Law on Electronic Commerce** indicates that a receiver is entitled to regard a data message as being that of the originator, and to act on that assumption, if, in order to ascertain whether the data message was that of the originator, the receiver properly applied a procedure previously agreed to by the originator for that purpose (e.g. use of certain type of electronic signature). It is important to make reference to the **Digital Signature Guidelines**

**of the American Bar Association**. The Digital Signature Guidelines of the American Bar Association refers to the equitable principles as a means to not give the signatory the chance to repudiate the signature.

If the technology used to produce the electronic signature is based on digital signatures, and a digital certificate issued within a PKI is owned by the signatory, then the certificate revocation could limit the liability derived from such signature. Four possibilities exist regarding the phases inherent in the revocation process.

An electronic signature associates a digital sequence with an electronic document to represent a handwritten signature on a paper printed document. This digital sequence should be considered similar to a handwritten signature. In principle, an electronic signature is based on the use of two different digital keys known as a key pair. Each key pair is made up of a private key and a public key. The two are interdependent but can be used separately. Typically each key pair may belong to a specific key holder. The algorithm works in such a way that it is computationally infeasible for a third party to compute the private key even if they are in possession of the public key.

# FORMATION OF ELECTRONIC SIGNATURE

The idea of digital signature uses derived from two concepts namely Asymmetric cryptography and RSA algorithm.

**Cryptography**

Cryptography is an art of transferring data from one point to other in a form than the third party can't understand it. The data can be in any form. Cryptography is done by following two basic steps encryption and decryption and that is by Encryption which means the converting the original information into unreadable cipher information by using a key (or in other words set of rules), this happens in the senders end. Special class of electronic signatures that use public key cryptography to give electronic signatories a unique digital identification. Used

properly, digital signatures identify the sender, ensure message integrity, and render the message non-repudiative.

**Decryption.**

Decryption is converting back the cipher information into the original information by using a key (or in other words set of rules), this happens in the receivers end.

By these two steps the cryptography protects the information from sharing it with other than the desire person while transferring it.

Electronic signatures are used to authenticate digitally transferred data and to ensure that the content of the message or the document sent has no changes. Electronic signature cannot be imitated and can be time stamped automatically, avoiding the chances of the sender to repudiate it later. Electronic signature of the digital certificate issuing authority is also included in the digital certificate, so it is possible to check the originality of the certificate by anyone.

**The electronic signature provides four main characters;**

**Confidentiality and Privacy:** As the data is encrypted the confidence and privacy of the data is confirmed.

**Authentication:** The identity of the sender is ensured by the digital certificate. So, the receiver can verify the identity of the sender. Authentication should be understood as a means of identifying the signatory but also indicating the signatory's approval of the signed data, as interpreted in the incorporation of the Directive into the national laws by most Member States.

The signature is binding between the public key used to verify the signature and the identity of the signer, by means of a digital certificate issued by a trusted authority. Thereby, the origin of the evidence (authenticity) is verifiable by the relying party. As it ensures the authenticity of the sender, The falsely deny of the sender is also not possible. For instance, the digital Signature purpose is intended

to be used in authentication services, data origin authentication services, and/or integrity services.

**Section 16** of the Electronic Signatures Act provides that digitally signed document are taken to be written documents.

(1) A message shall be as valid, enforceable and effective as if it had been written on paper if;

(a) It bears in its entirety a digital signature; and

(b) That digital signature is verified by the public key listed in a certificate which;

(i) Was issued by a licensed certification service provider; and

(ii) Was valid at the time the digital signature was created.

**Integrity:** digital signature ensures that the data is not tampered during the transfer. Due to the cryptographic properties of digital signatures, any modification of the signed information or the signature itself is detected, assuring the integrity of the evidence and the signed information

**Non - repudiation:** A digital signature is data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery by the recipient. It is a non-repudiation token generated using asymmetric techniques, and that is exchanged during a protocol and which can be used subsequently, by disputing parties or by an adjudicator, to arbitrate in disputes. The originator of the signature (the signer) cannot later repudiate the authorship, since he is the only one that (theoretically) knows the private key.

The digital signature must be verified in conjunction with the signed information, the validity of the signature must be satisfied, and the digital certificate must be valid at the time the signature was computed. When these requirements are met, the evidence is considered as valid. Consequently, a digital signature acting as non-repudiation evidence and that is correctly verified

according to the particular non-repudiation policy is suffice to resolve a possible dispute, avoiding the alleged signatory to successfully repudiate the commitment made in the transaction.

In the same way, a digital signature acting as non-repudiation evidence can be verified by any of the next entities but using the public key certificates and certificate revocation lists which were all valid at the time the evidence was generated:

The non-repudiation service protects the parties involved in a transaction against the other party denying that a particular event or action took place. Non-repudiation services permit to design protocols and applications where strong commitments are made between the participant entities. Electronic commerce protocols or e-Government services are among those scenarios that must protect the entities against fraud and misbehavior. In non-repudiation services, digital evidence permit to enforce the responsibility that each entity takes on in the transaction, avoiding a further successful repudiation of the commitments made.

**Non repudiation works in the following ways**;

**Non-repudiation of origin,** intends to protect against the originator's false denial of having created the content of a message and of having sent a message, covering both non-repudiation of creation and non-repudiation of sending.

**Non-repudiation of receipt,** intends to protect against a recipient's false denial of having received a message.

**Non-repudiation of knowledge,** intends to protect against a recipient's false denial of having taken notice of the content of a received message.

**Non-repudiation of delivery,** intends to protect against a recipient's false denial of having received a message and recognized the content of a message, covering both non-repudiation of receipt and non-repudiation of knowledge.

**Non-repudiation of submission,** intends to provide evidence that a delivery authority has accepted a message for transmission.

**Non-repudiation of transport,** intends to provide evidence for the message originator that a delivery authority has delivered a message to the intended recipient.

Evidence is information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Proof is the corroboration that evidence is valid in accordance with the non-repudiation policy in force. Though evidence does not necessarily prove the truth or existence of something, it contributes to the establishment of such proof. On the other hand, the non-repudiation policy is whatever set of criteria for the provision of the non-repudiation service, that is, the set of rules to be applied for the generation and verification of evidence and for adjudication.

A trusted third party which is an entity trusted by the entities involved in the service provision, may be necessary during the protocol execution. The degree of participation of the Trusted Third Party during the evidence exchange varies, existing trusted Third party that intervene in every message transmission (inline), only in certain transmissions (online), or just when a protocol interruption or entity misbehavior occurs (offline). Depending on the type of evidence being produced and the trusted third party involved in the non-repudiation service, the evidence generation, transfer, storage, retrieval and verification phases differ.

The non-Repudiation /content Commitment purpose means that the signer cannot later repudiate having performed the signature. Thus, this key usage is completely needed if the signer has to consume a non-repudiation service, or when the signature has to legally bind the signer respecting the signed data

Digital signature is one of the concepts in public Key Infrastructure, the information or the identity of the user is tied to the public key. The Digital certificate is signed by the Certification Authority that provided it, to ensure trust in the signed data.

Digital signature software became a powerful business tool in recent years. It provides ability to sign online. Documents, contracts, different kinds of form, tax

filing can be executed online. This technology is secure, legally robust, and efficient, and saves all parties time, money, and hassle.

# DIFFERENCE BETWEEN DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

Digital signature and Electronic signature are used interchangeably, but they are not same. Digital signature is one of the kinds of e-signature. Digital signature, electronic signature or the signature on a paper the old-fashion way, the intention is the same, agreeing with the terms. But they have different legal weight and a different technological perspective.

An e-signature or electronic signature includes all types of electronically approval methods. It could be an audio file, graphical stamp, a process, or even pressing the "Agree" button in most of the terms and conditions tab, etc. It includes simple forms like pressing "place order" to complex forms like biometric signature.

For a business contract or tax filling, it is not advisable to use any kind of e-signature, since not every e-signature has the same legal value and secured. The signature should be authenticable, have integrity and security, when it comes to legal documents. So, in these situations the use of biometric signature or digital signature would be more appropriate. And these complex signature types are legally binding and are more secured and unique, which helps in trusting the document.

## *Statutory/Legal Requirements of electronic signatures*

**Evidence of the Signatory's Identity**

An electronic signature, by itself, cannot provide sufficient evidence of the signatory's identity. To explore this matter further, evidence is required that links the signature key or other signature device to the signatory himself. But the

recipient wishes to be able to rely on the signature without needing to collect evidence for use in the unlikely event that the signature is disputed.

For this reason, most electronic signatures used for e-commerce communications are likely to be accompanied by an ID Certificate issued by a Certification Authority. The Certification Authority takes traditional evidence of identity[95] for example, by examining passports, and, in the case of public key encryption digital signatures, checks that signatures effected with the signatory's secret key are verifiable using the public key. Once the Certification Authority is satisfied as to the signatory's identity, it issues an ID Certificate, which includes, inter alia, a certification of the signatory's identity and of his public key. This certificate may be used by the recipient to prove the signatory's identity.

**Evidence of Intention to Sign and Adoption of Contents**

Once identity has been proven, the very fact that an electronic signature has been affixed to a document should raise the same presumptions as manuscript signatures the signature is effected by selecting from an on-screen menu or button, with the signature key stored on the signatory's computer the signature key is stored on a physical token, such as a smart card, which needs to be present before the signature software can affix the signature.

In either case, a third party who had access to the computer or to the storage device would be able to make the signature. For this reason, an electronic signature should be considered as more closely analogous to a rubber stamp signature. The party seeking to rely on the validity of the signature may need to adduce extrinsic evidence that the signature was applied with the authority of the signatory until the use of electronic signatures becomes so common that the courts are prepared to presume that a third party who is given access to the signature technology has been authorized by the signatory to sign on his behalf, or unless a statute introduces a presumption as to the identity of the signatory.

[95]See Saunders v. Anglia Building. Society [1971] AC 1004 (U.K.).

In **Green v Ireland**[96] It was held that Clicking on an "I accept" button held to satisfy a statutory requirement for a signature. This case concerned an alleged email contract to create a charge over land. Under the relevant legislation it had to be "signed by or on behalf of" the respective parties. There was no dispute that they had, by inserting their names at the end of the emails that they had sent, signed them for the purposes of the legislation.

In **Neocleous v Rees (2019) EWHC 2462** an Informal e-mail sign-off plus auto-appended name and contact details were held to satisfy statutory requirement for a signature. The name and contact details of the seller's solicitor had consciously been entered into the firm's e-mail settings by someone at some stage. The solicitor knew that the system would automatically append his name and contact details. Writing 'Many thanks' at the end of the e-mail suggested that he was relying on that happening. In those circumstances it was difficult to distinguish that process from manually adding the name each time an e-mail was sent. The recipient would have no way of knowing whether the details had been added manually or automatically. Objectively, the presence of the name indicated a clear intention to associate the sender with the e-mail – to authenticate or sign it.

**Mehta v. J Pereira Fernandes** [97] it was held that the sender's automatically inserted e-mail address was not included with intent to be a signature. Under S.4 of the Statute of Frauds 1677 a guarantee had to be signed by or on behalf of the guarantor in order to be enforceable. Mr Mehta's name or initials did not appear at the end of the e mail or anywhere else in its body. The judge was in no doubt that if someone creates and sends an electronically created document, then he will be treated as having signed it to the same extent that he would be treated as having signed a hard copy of the same document.

However, he rejected the argument that the appearance of Mr Mehta's email address at the top of the email was a signature for the purposes of the section, since it had not been included with the intention of giving authenticity to the document. Its inclusion was not intended as a signature.

[96](2011) EWHC 1305.
[97]SA (2006) EWHC 813

In cases where an electronic signature that has previously been acknowledged by the signatory is effected by an unauthorized third party, however, the apparent signatory should be estopped from denying that it was his signature. The objection that an electronic signature fails to meet the evidentiary requirements because a successful forgery cannot be detected is easily dismissed by pointing out that no such requirement is imposed for manuscript signatures. Indeed, signatures in pencil have been held valid under English law for such important commercial documents as bills of exchange and guarantees. In fact, electronic signatures are normally much harder to forge than manuscript signatures. Thus, the only function that electronic signatures cannot provide is that of making a mark on a document.

In **Morion v. Copeland [1855] 16 CB 517, 535 (Maule J)** it was held that signing "does not necessarily mean writing a person's Christian and surname, but any mark which identifies it as the act of the party.

## THE ROLE OF ID CERTIFICATES

Where the parties have had no previous dealings, the recipient will have no knowledge whether the public key does in fact correspond to the purported identity of the signatory. This is where the ID Certificate comes in. It contains: a copy of the signatory's public key, a statement that the issuer of the Certificate has checked the identify of the signatory, that the signatory does in fact possess the signature data that corresponds to the public key, and that the issuer has checked that the public key validates the identified person's electronic signature.

Thus, where an electronic signature is made on a document, the accompanying ID Certificate provides evidence from an independent third party that the person named in the certificate did in fact have access to the unique signature data so long as the public key included in the certificate validates the signature. In the absence of evidence from the alleged signatory that some third party forged his signature, a court should be satisfied by the evidence that the purported signatory was responsible for the electronically signed document.

# IMPORTANCE OF ELECTRONIC SIGNATURE

Electronic signatures are likely to be used for a wide range of transactions, which have legal consequences, including:

The formation of contracts

Transactions where the recipient of the communication is required to identify its customer, for example, funds transfers to which money laundering controls apply the provision of legally required information to government agencies where there may be a need to ensure that the information source is correct, or more commonly where there are penalties for supplying incorrect information, for example, on tax returns.

Electronic signatures are also likely to be required for **identification purposes** where the user is requesting information that should not be released to third parties, such as information about the user's bank account. In addition, there are a several types of commercial transactions where digital identification will be useful to one of the parties.

Electronic signatures are used to show originality of a data message and who is the signor of a document.

**Section 17** states that a digitally signed document is deemed to be original document.

A copy of a digitally signed message shall be as valid* enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

Signatures serve as the means to establish higher level of security requirements for the signatures of a transaction, filling the gap left by the key usage. The signer can select the desired commitment type, and include it as a signed attribute of the signature. Moreover, the signer must indicate in the electronic

signature which policy it complies to. For that purpose, a reference to the signature policy has to be included as a signed attribute as well.

The reference consists of the unique policy identifier (OID), the hash value of the policy and the hash algorithm identifier used to compute the hash value over the signature policy description. If a dispute arises, the signature can be used to provide supportive evidence over the procedure associated with a specific signature in use. Implicit references to the signature can be made as well but the structure or semantics of the document that a user is signing must be well defined. It is worth noting that the signature policy reference is a signed attribute inside an electronic signature format and therefore it is not possible to substitute the policy used during the signature generation without invalidating such signature. This prevents the possible situation where an attacker wants to limit the requirements under which the signature is considered to be valid by replacing the policy by a less demanding one.

Notwithstanding, a conceptual relationship between both sets exist. A signature intended to bind the signer with the signed content should use a certificate with the non Repudiation bit set to '1'. In the same way, the commitment type chosen from those available in the signature policy should cover that intention (e.g. content approval). Though not every combination of key usages and commitment types are coherent, a matrix of correspondence or consistent combinations could be traced. However, as commitment types of a signature policy are context specific, this matrix should be implemented in a case by case basis.

An important contribution of signature policies is that they enforce enclosing the consequences that can be derived from a signature. Used in conjunction with appropriate key usages, the signer can obtain a certain level of confidence respecting the type of signature that is being generated.

However, the increase of paper-based processes being transposed into the digital realm makes current signature policy definition insufficient to cope with the new needs that arise. Very often, documents require more than one signature to give it legal validity or to make a transaction effective. This limitation was pointed

out by ETSI in a technical report published in 2003 ETSI report studies business needs that may need multiple signatures, and provides a foundation for further work in relation to the technical implementation of a signature policy governing multiple signatures, and a general guidance on a methodology for the validation of multiple signatures. ETSI report assumes that each signature will be validated under a signature policy for single signatures such as The challenge raised by ETSI is the specification and validation of the relationship of each required signature against the others. At the time of writing this thesis, no technical solution covering this need had been proposed

## INFORMATION LICENSING

A subscriber may apply for a license from a certification service provider and the latter upon receiving such application, shall consider that the applicant has all necessary requirements as stated in the law.

For one to obtain license to operate as a certification service provider;

An application for a license is made under **section 25** which provides that;

25. Application for licence.

(1) An application for a licence under this Act shall be made in writing to the Controller in such form as may be prescribed.

(2) An application under subsection (1) shall be accompanied by such documents or information as may be prescribed and the Controller may, at any time after receiving the application and before it is determined, require the applicant to provide "such additional documents or information as may be considered necessary by the Controller for the purposes of determining the suitability of the applicant for the licence.

(3) Where any additional document or information required under subsection (2) is not provided by the applicant within the time specified in the requirement or any extension granted by the Controller, the application shall be taken to be

withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

The grant or refusal of license is provided for under **section 26** and in addition, it provides that;

(2) A licence granted under subsection (1) shall set out the duration of the licence and the licence number

(3) The terms and conditions imposed under the licence may at any time be varied for just cause or amended by the Controller but the licensee shall be given a reasonable opportunity of being heard.

(4) The Controller shall notify the applicant in writing of his or her decision to grant or refuse to grant a license within thirty days of receiving the application.

This license may be revoked under section 27, if proved that the certification service provider has failed to comply with an obligation imposed upon them under the Act or that they have contravened any other condition imposed on them under any other written law.

The aggrieved person may appeal under section 28 giving sufficient grounds therefore and this appeal shall be determined by the minister in 30 days but if the person is not satisfied still, they may appeal to the High court. The license is renewable under section 35.

# ATTRIBUTION OF AN ELECTRONIC SIGNATURE/ AUTHENTICATION

An electronic authentication, display, message, record, or performance is attributed to a person if it was the act of that person or its electronic agent, or if the person is bound by it under agency or other law. The party relying on attribution of an electronic authentication, display, message, record, or performance to another person has the burden of establishing attribution.

a) The act of a person may be shown in any manner, including a showing of the efficacy of an attribution procedure that was agreed to or adopted by the parties or established by law.
b) The effect of an electronic act attributed to a person under subsection (a) is determined from the context at the time of its creation, execution, or adoption, including the parties' agreement, if any, or otherwise as provided by law.

If an attribution procedure exists, to detect errors or changes in an electronic authentication, display, message, record, or performance, and was agreed to or adopted by the parties or established by law, and one party conformed to the procedure but the other party did not, and the nonconforming party would have detected the change or error had that party also conformed, the effect of noncompliance is determined by the agreement but, in the absence of agreement, the conforming party may avoid the effect of the error or change.

# SIGNING AND VERIFICATION IN DIGITAL SIGNATURE

digital signatures are to be authenticated by a certificate issued by a licensed certification service provider as an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of express acknowledgement appear with' the digital signature and regardless of whether the signer physically appeared before the licensed certification service provider when the digital signature was created, if that digital signature is

a) verifiable by that certificate; and
**b)** was affixed when that certificate was valid. per **section 18 of the Electronic Signatures Act (ESA.)**

The digital signature for the data is generated in two steps:

1. Generation of the message digest: The message digest is generated using hash algorithm. This gives a binary message of the original message.

2. The generated message digest is encrypted by the sender's private key. The encrypted message digest is known as the digital signature.

In conclusion, an electronic signature are an important part of contract law as a whole and has a lot in it that has modernized and standardized today's business transactions. In an era of unity in diversity such as we are in now, uniformity of laws and its comprehensiveness are important to produce not only a better realization of the right to access the internet but also to make life and business better.

CHAPTER 10

# THE RIGHT TO PRIVACY AND DATA PROTECTION

## DEFINITION OF PRIVACY

In the case *of* ***R v Brown,*** Lord Hoffman defined Privacy as a right to keep oneself to ourself, to tell other people that certain things are none of their business is under technological threat due to the different and various types of surveillance e.g. surveillance cameras, telephone bugs e.t.c that are used by individuals in the society today.

Privacy is a fundamental human right embedded in various international human rights legal instruments. For example, **Article 17 of the International Covenant on Civil & Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR**), which states inter alia, that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks". Express protection for "private life" is also found **in Article V of the 1948 American Declaration of the Rights and Duties of Man, and in Article 11 of the American Convention on Human Rights (ACHR) of 1969.**

Further, these provisions have been embedded in different jurisdictions in national constitutions and in acts of Parliament.

In Uganda, the Right to Privacy is also contained in **article 27** which provides that; No person shall be subjected to

(1) Lawful search of the person, home or other property of that person; or unlawful entry by others of the premises of that person.

(2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

# INTERNET/ONLINE PRIVACY

Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via of the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing.

Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.

Internet privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development Internet privacy is also known as online privacy.

Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website. PII refers to any information that can be used to identify an individual. For example, age and

physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

## PRIVACY ON THE COMPUTER

Consumers' private information can be violated through illicit use or infiltration of a consumer's computer or network in a number of ways:

Installing Software programs, such as games, anti-virus programs, and word processors, can potentially access to users' private information or expose that information to security vulnerabilities.

Transferring liability to the Computer (hardware) maker, Computer manufacturers may be held responsible for security vulnerabilities in their hardware that may jeopardize purchasers' private information.

Crimininalizing Third-party data collectors. Computers can be vulnerable to having private information illegally intercepted or transmitted over server networks, the internet and other networks. Unauthorized collection of data may be illegal under various state and federal consumer protection laws.

Establishing liability for the Internet websites & companies. Illicitly transmitting or collecting information via online stores, social networking sites, and other websites may put users' private information at risk. When internet privacy violations occur, those websites and internet companies may be liable.

## PRIVACY AND THE MEDIA/ FREEDOM OF EXPRESSION

Privacy and freedom of expression are intertwined rights in human rights law. They appear together in international instruments, national constitutions and laws. Together they ensure the accountability of the state and other powerful actors to citizens.

It is important to note that the rights are mutually supportive. Freedom of expression and freedom of information allow individuals to investigate and challenge abuses to human rights including violations of privacy. Privacy allows individuals to work and communicate in a space unhindered by authority. As a practical matter, limits on privacy affect the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and other sources. Privacy laws can support freedom of expression by placing limits on the unlawful collection of personal information for political purposes, such as bodies creating dossiers or collecting data through surveillance activities to put pressure on journalists and others.

Privacy and the protection of personal data play a key role for the exercise of fundamental rights in a broader sense. Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. Freedom of thought, freedom of expression, freedom of assembly and association, but also the freedom to conduct a business will not be exercised fully by all citizens in an environment where the individual feels that each of her or his moves, acts, expressions and transaction is subject to scrutiny by others trying to control him or her.

# PRIVACY AND LAW ENFORCEMENT

Information privacy law or data protection laws prohibit the disclosure or misuse of information about private individuals. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws. The European Union has a data protection Regulation, in force since May 25, 2018. The United States is notable for not having adopted a comprehensive information privacy law, but rather having adopted limited sectoral laws in some areas.

These laws are based on Fair Information Practice that was first developed in the United States in the 1970s by the Department for Health, Education and Welfare (HEW). The basic principles of data protection are:

1. For all data collected there should be a stated purpose.
2. Information collected by an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual
3. Records kept on an individual should be accurate and up to date
4. There should be mechanisms for individuals to review data about them, to ensure accuracy. This may include periodic reporting
5. Data should be deleted when it is no longer needed for the stated purpose
6. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited
7. Some data is too sensitive to be collected, unless there are extreme circumstances (e.g., sexual orientation, religion)

# STATE OF PRIVACY AND PERSONAL DATA PROTECTION IN UGANDA

## *Status of International Laws on Privacy*

Uganda has signed and ratified key international human rights instruments which provide for the right to privacy as a fundamental human right. These instruments include the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights whose articles 12 and 17 provide for the right to privacy respectively.

Africa on June 27, 2014 adopted the **African Union Convention on Cyber security and Personal Data Protection** which is the main guiding instrument on privacy and personal data protection. Uganda is also a signatory of several international conventions with privacy provisions, including:

1. The Universal Declaration of Human Rights;
2. The International Covenant on Civil and Political Rights;
3. The African Charter on Human and Peoples' Rights;
4. The Convention on the Rights of the Child; and
5. The African Charter on the Rights and Welfare of the Child.

Worse still, there is no specific instrument to govern data protection and privacy at the East African Community (EAC) save the EAC legal framework for cyber laws which has no serious legal effect.

## *National Laws Data Protection and Privacy in Uganda*

Uganda now has the Data Protection and Privacy Act, 2019. There are also scattered provisions traceable in various pieces of legislation including the Constitution of the Republic of Uganda, and the law which are briefly highlighted below.

## *The Constitution of the Republic of Uganda, 1995*

The Uganda Constitution provides for the right to privacy under article 27 to the effect that no person shall be subjected to: unlawful search of the person, home or other property of that person; unlawful entry by others of the premises of that person; and interference with the privacy of that person's home, correspondence, communication or other property. From the proviso, protection of data protection and privacy extends to unlawful entry and searches, property, and correspondence or communication. While the Constitutional provision is quite elaborate, it requires a specific law that addresses all issue concerning the

privacy of the individual. It is important to note that the Parliament enacted the law on privacy and data protection the Data Protection and Privacy Act,2019 and Data Protection Regulations2021.

## *Uganda Communications Act, 2013*

Uganda Communications Commission is established by section 4 of the Uganda Communications Act, 2013. Its functions are listed under section 5 as including among others: implementing the Act; monitoring, inspecting; licensing, supervising; controlling and regulating communications services; and processing of applications. Further, section 6 of the Act provides for the powers of the commission as including among others; charging of fees, imposing fines, classifying communication services and licences and confiscation of communication apparatus. This Act gives the Minister extensive powers which have been used overtime to interfere with the operations of the communications sector. The Commission has for instance issued a notice to all online data communication service providers in which all online news platforms and online radio and television operators are effective April 2, 2018 required to apply and obtain authorisation for their online services. This is an obligation that goes to the root of individual privacy in communication.

Under the same law, Ugandans had to repeatedly register and register their SIM cards as aspect that involves consistent data breaches since there is no specific data protection law in Uganda.[79] Further, SIM cards of non-compliant citizens, who had failed to submit or verify their national identity card details were switched off.[80]

On a positive note, the Uganda Communications Commission together with Uganda Media Council established by section 8 of the Press and Journalist Act Chapter 105 recently passed a decision which is important for the exercise and realisation of the right to privacy in Uganda. In this decision, Faridah Nakazibwe brought a case against the Hello Tabloid and its Richard Tusiime on allegations of publishing 38 articles about the complainant in the tabloid, causing her mental anguish and a lowering her esteem in the eyes of her children, family and

society. The Committee found that there had been breach of the complainant's privacy and therefore degraded her dignity and awarded her Uganda shillings 45 million ($12014.58).

## *Technology Authority National Information Act, 2009*

The National Information Technology Act establishes the National Information Technology Authority (NITA-U) under section 3 and its functions under section 5 inter alia include; creating and managing the national databank, monitoring and regulating data standards; and promoting and providing technical guidance for the establishment of e-Government, e-Commerce and other e- Transactions in Uganda. NITA-U is part of the three agencies that have been at the fore of registering Ugandan citizens through collecting and processing of personal data without a particular law to guide handling individuals' data.

## *Registration of Persons Act, 2015*

The Registration of Persons Act was passed to harmonise and consolidate the law on registration of persons. **Section 4 of the Act** establishes the National Identification and Registration Authority (NIRA) which is mandated by **section 5** to register citizens and non-citizens and births as well as issuing unique identification numbers to persons registered and issuance of national identity cards. As part of its mandate, NIRA together with the Uganda Communications Commission in absence of data protection law or a data protection commission embarked on a national wide issuance of identity cards which entailed among others, the collection and processing personal data before issuance of cards. There is thus no guarantee of protection of the data collected by the authority.

## *The Computer Misuse Act, 2011*

The Computer Misuse Act, 2011 under section 3 and 6 makes strides in regulating access to data held on computers. Further, it provides for cases where access and modification may be deemed unauthorised under **sections 12 and 8 and 12** respectively. Further, computer misuse offences are provided as

including unauthorised access **(section 13); un** authorised modification of data **(section 14**); unauthorised use or interception of computer services **(section 15);** unauthorised disclosure of access codes (section 17); and unauthorised disclosure of information (**section 18).**

However, this Act makes provision for preservation orders for data in cases of data vulnerability or loss under section 9. Further, under sections 9 and 11, investigation officers may apply for orders of investigation and production of data for purposes of criminal investigations. The Act also provides for searches and seizure which though on orders of the Magistrate may interfere with the privacy of the individual.

This Act has previously been used to supress critical voices of the government evidenced in the arrest and prosecution of social media critic Stella Nyanzi. Nevertheless, this law has also been partly used in efforts to enforce rights related to defamation, harassment, defamation and privacy of the individual as evidenced in the feud between Justine Nameere and Faridah Nakazibwe.

## *Regulation of Interception of Communications Act, 2010*

The Regulation of Interception of Communications Act, 2010 is solely for lawful interception and monitoring of communications in the course of their transmission whether through telecommunication media or postal services or any other service. **Section 2 of the Act** bars unlawful interception of communication by any person save where there is consent or an authorised warrant. Despite the protection guaranteed in section 2, section 3 established a monitoring centre for the interception of communications which is placed under the Ministers responsibility. Further, the Act lists a number of individuals who are authorised to apply for a warrant of interception to a judge as including the: Chief of Defence Forces or his or her nominee; Director General of the External Security Organisation or his or her nominee; Director General of the Internal Security Organisation or his or her nominee; and the Inspector General of Police or his or her nominee. Further, section 5 read with sections 6, 7, 8, 9, 10, 11 and 12 provide for grounds, ways and processed for which interception may be

authorised by a judge as including; gathering information that threatens life or loss of life, trafficking in drugs and humans, actual threat to national security, public safety or to any national economic interest and threat he national interest involving the State's international relations or obligations. This act also requires providers of postal or telecommunications systems. Similar grounds may be applied to postal communications as listed in sections 13 and 14 of the Act.

## *The Electronics Signatures Act 2011*

The Electronics Signatures Act 2011 regulates the use of electronic signatures. Section 81 provides for the obligation of confidentiality. It is to the effect that no person shall obtain access to any electronic record, book, register, correspondence, information, document, other material or grant access to any other person unless under the order of Court. Further, the Act under section 86 provides for a search warrant which may be granted by a magistrate to a police officer not below the rank of Inspector to enter premises and carry put a search. On the other hand, such police officer may forego the warrant and search premises under section 87 of the Act. While these provisions in the law suggest authorisation before search, the law does not rule out cases of violation of privacy and does not guarantee total respect for the individual's privacy. The Electronic Signatures Act in the foregoing provisions potentially affects freedom of expression online as well as the right to privacy online.

## *The National Information and Communications Technology Policy for Uganda Policy, 2014*

In 2014, the government of Uganda adopted that National ICT Policy with the aim of enhancing the Telecommunications, Postal services, Broadcasting, Information Technology and Information management Services for economic development and transformation of the country. The policy among others identifies and lists some of the government strategies as developing legislation that address privacy and data protection of the individual in all spheres of life.[87] The areas of covered by the policy *inter alia* include health, e-commerce and

consumer protection, information security and education. However, this policy is yet to be fully implemented especially in the absence of a specific law on privacy of the individual to guarantee data protection.

## GUIDELINES AND ICT STANDARDS

Besides the use of laws and policies, there are other guidelines and IT standards which are highly recommended for ensuring privacy. For instance, the government through National Information Technology Authority-Uganda (NITA-U) calls on government ministries, departments and agencies (MDAs) to issue a disclaimer alerting users when they are no longer on a government site and that the site's own privacy policy applies.[88] Further, MDAs are called upon to; guard against identity theft, respect privacy of others, choose more secure modes of communication and to report all cases of abuse or misuse of social media platforms.[89]

Further, NITA-U has put in place the: NITA-U Standards Catalogue 2017;[90] Online E-Safety Educational Toolkit for Young People in Uganda;[91] Guidelines for Development and Management of Government Websites;[92] Guidelines for Operation, Usage and Management of IT Infrastructure in MDAs & Local Government;[93] Standards for Structured Cabling for Government MDAs;[94] and the Guidelines and Standards for Acquisition of IT Hardware & Software for MDAs.[95] The foregoing instruments emphasize the importance of data protection and privacy alongside ICT development in the country.

There is no specific law on data protection and privacy in Uganda. What exists are scattered provisions in various pieces of legislation discussed above. It is important to note that what is available impacts data protection and privacy positively and negatively. In some of the provisions and existing practices, privacy and data protection are upheld while in some of the legislation, promote the curtailment of data and privacy rights.

# HEALTH AND GENETIC PRIVACY

Patients of Uganda's overburdened health sector often have little privacy; maintaining confidentiality is difficult in circumstances where multiple patients are often treated in the same rooms. A draft Patients' Rights and Responsibilities Bill (2015), reportedly contains some provisions ensuring patient privacy and the confidentiality of medical information.

# PRIVACY AND GOVERNMENT RECORDS AND DATABASES

The National Information Technology Authority-Uganda (NITA-U) is mandated by the NITA-U Act of 2009 to "promote and provide technical guidance for the establishment of e-Government, e- Commerce and other e-Transactions in Uganda."

The government is engaged in various e-governance initiatives including: the Nationwide ICT Backbone and e-Government Infrastructure and central government intranet system; the Ministry of Finance's Integrated Financial Management System (IFMS); the Uganda Revenue Authority's tax filing system; the Ministry of Health's Health Management Information System; and the Ministry of Public Service's Integrated Personnel and Payroll System (IPPS).

## *Case law in Uganda*

**Asege Winnie V Opportunity Bank and Maad Limited**[98] , Maad limited Company which had been contracted by Opportunity bank to make an advert used the photo of Asege Winnie without her permission and so the bank used her photo on bronchures, calenders and flyers thus commencement of the suit. Court held that Opportunity Bank and Maad Limited were liable for breach of privacy .

[98]Asege Winnie V Opportunity Bank and Maad Limited. High Court Commercial Division 756 of 2013.

Bassajabaka Yakub v MTN Uganda Limited , the plaintiff sued MTN Company for using his photo on a billboard without his consent. Court held that the plaintiff's right to privacy was breached and awarded him forty million damages.

# COMMUNICATION SURVEILLANCE.

## *Surveillance laws.*

Communications surveillance is primarily regulated by the Regulation of Interception of Communications Act (RICA) 2010. Other acts also grant the security services wide-ranging communications surveillance powers.

RICA requires intelligence officials and the Police to seek judicial authorisation for the interception of communications. The law authorises intelligence officials to apply to intercept specific communications subject to a warrant that is issued by a designated judge. However, RICA does not replace the provisions for interception contained in the Anti-Terrorism Act (2002) — it appears to contradict them. This law gives almost unfettered discretion for state officials to conduct surveillance without the need to obtain judicial authorisation. The powers of surveillance are broad. These include the interception of phone calls, emails or other communications, 'electronic surveillance', as well as monitoring of meetings, or doing "any other thing reasonably necessary" for the purpose of surveillance (section 19(5)). The justifications of such surveillance are very broad, including safeguarding public interest, and protecting the national economy from terrorism (section 19(4)).

There is no clear oversight mechanism to either RICA or the Anti-Terrorism Act.

**Section 11 of RICA** requires service providers to retain metadata, although the terms and conditions of the retention are not specified in the Act.

The Act also provides for the establishment of a Monitoring Centre under the control of the Minister As of late 2015, the monitoring centre was not operational though seven international firms were invited to bid for the project. It had been delayed in part because service providers have contested Government orders that they pay to connect to the future system, according to sources in the technology industry. However, Israeli firm NICE Systems is reported to have won the contract, according to Intelligence Online.

RICA requires service providers to foot the bill of connecting to the new centre or otherwise complying with the Act, a considerable cost. Current data retention capacity of the main networks including MTN Uganda was estimated at around 6 months' worth of call metadata in 2015.

## *Surveillance Actors*

The power to gather intelligence and conduct surveillance are concentrated around three institutions: the Uganda People's Defence Force (UPDF), the Uganda Police Force (UPF), and the Office of the President (State House). The President exercises control over sensitive intelligence operations while day-to-day spying for intelligence gathering appears less centralised. Senior leaders and technical experts within intelligence circles are often reshuffled and reassigned among these agencies on Presidential direction.

**Intelligence and security agencies**

The 1987 Security Organisations Act established the Internal Security Organisation (ISO) and External Security Organisation (ESO). These two agencies are directed by Directors General appointed by and accountable to the President, and exist to collect intelligence and provide advice on Uganda's security directly to him.

The National Security Council, established in 2000, reports directly to the President and comprises cabinet ministers, ISO, ESO, army and police officials, most of which are appointed by the President and up to five additional members, also appointed by the President and approved by Parliament. The Joint

Intelligence Committee, composed of security experts appointed by the President and chaired by the Minister of Internal Affairs, reportedly meets once a week to share intelligence on national security threats. An Information and Communication Technologies (ICT) Technical Committee within the Joint Intelligence Committee advises on technology purchases and is responsible for many decisions related to defence and intelligence procurement. These powers are discussed in more detail in a report by Privacy International.

**Law Enforcement Agencies**

The 2004 Police Act gives the President the power to appoint the Inspector General of Police and his deputy, as well as the majority of the members of the Police authority which oversees police functions, and veto power over any potential dismissals of senior-ranking officials. As Commander- in-Chief of the defence forces, the President may appoint the Chief of Defence Forces and virtually all high-ranking officials. The President enjoys discretionary powers over the activities of the High Command.

## *Surveillance capabilities*

The Regulation of Interception of Communications Act (2010) provides for the establishment of a monitoring centre. In late 2015, the monitoring centre was not operational though seven international firms had been invited to bid for the project. These seven firms included: ZTE and Huawei (China), Verint Systems Ltd and NICE Systems (Israel), Macro System (Poland), RESI Group (Italy) and Gamma Group International (UK). The monitoring centre project had been delayed in part because service providers contested government orders that they pay to connect to the future system, according to sources in the technology industry. NICE Systems was reported to have obtained the monitoring centre contract in November 2015. It is unknown if the monitoring centre is operational.

In recent years the security services have invested heavily in cyber defence. In 2013, a new forensic lab for the analysis of computer crime opened in Kampala

and the UCC launched a Computer Emergency Response Team to investigate cybercrime. Despite these developments, the police's ability to actually conduct forensic analysis on devices and trace cybercrimes is rudimentary. The police and investigating agencies often turn to private forensic companies to assist in complex investigations, according to an October 2015 investigation by Privacy International.

In 2014, the UCC opened a media monitoring centre with "digital logger surveillance equipment". This appears to be targeted at recording and analysing public radio, television and print media rather than private communications. The police also signed an accord with the UCC to cooperate more closely on the investigation of cybercrime.

In August 2016, the government announced that it had contracted a South Korean company to supply a "pornography detection machine" with the budget of 2.6 billion Uganda shillings. The purchase was intended to aid the Parliament's anti-pornography committee to monitor and implement Uganda's anti-pornography laws by detecting pornographic pictures, videos or graphics taken or saved on individual phones, computers or cameras, Surveillance oversight, checks and balances, there are no clear specific oversight roles on surveillance in Uganda

## *Examples of surveillance*

State authorities have proactively cultivated the popular perception that surveillance is systematic, centralised and technically sophisticated. This is not the case; not yet, at least. Nevertheless, human rights defenders and activist groups are regularly targeted for physical surveillance and break-ins and seizure of digital material by the police are common.

According to a **Privacy International investigation in** 2015, the attributes that have made Uganda's human intelligence network strong and allowed it to infiltrate opposition and other circles considered threatening to the government are poorly suited to conducting communications surveillance on a large and

automated scale. Poor levels of technical training, low pay and a culture of bribe-taking has alienated the few educated and technically competent engineers that would be required to operate a nationwide surveillance system beyond monitoring a relatively small number of high-value targets, according to industry and government sources.

The government has also reportedly placed agents within the telecommunications switching centres, but their skills vary and assignments appear to be relatively simple for example, the generation of call and contact lists, the location of callers using cell tower data, and audio recordings of specific lines based on human intelligence.

**Identification Schemes ID cards and databases**

In 2015, the Ugandan parliament passed the Registration of Persons Act to harmonize existing laws on the registration of persons, establish a single central registration body and a national identification register of all persons in Uganda, and provide rules to govern the access and use of this information. The act established the National Identification and Registration Authority, which oversees the issuing of national identity cards. The act makes it compulsory for all Ugandan citizens to register with the Authority and to register minors in their care.

Commentators noted that the act does not contain data protection clauses. This could potentially lead to violation of Article 27 of the Uganda constitution, which guarantees the right to privacy.

In 2016, Ugandan media reported that according to internal memos circulated to all ministries heads of departments, as well as chief administrative officers and town clerks across the country, public servants who failed to obtain national identity cards by July 1 would have their names removed from the government payroll.

**Voter Registration**

According to the Electoral Commission, all Ugandan citizens over the age of 18 are entitled to vote. Voters must reside or originate from the parish in which they intend to vote. Voters must be registered in the Photo-Bearing Voters' Register (PVRIS or NVR) which holds the following data: photograph, names, electoral areas including polling station, date of birth, sex, and voter's code number.

**SIM Card Registration**

Registration of SIM cards has been mandatory in Uganda since March 2012, following a campaign by the Uganda Communications Commission, citing the Regulation of Interception of Communications Act (2010).

The UCC stated that SIM registration information would be stored confidentially by telecommunications operators in a secure database. The UCC justified the initiative as necessary to "[h]elp law enforcement agencies to identify the mobile phone SIM card owners", "[t]rack criminals who use phones for illegal activities", "curb other negative incidents such as; loss of phone through theft, nuisance/hate text messages, fraud, threats and inciting violence", and "[h]elp service providers (network operators) know their customers better." In 2015, the Ministry of Security reportedly ordered the UCC to verify information provided by telephone users in the SIM card registration exercise by matching data collected during the National Identity card registration exercise with that gathered in the SIM card registration exercise.

The UCC ordered telecommunications providers to deactivate all unregistered SIM cards by 30 August 2017. The UCC directive ordering the verification exercise had previously been challenged by the Uganda Law Society.

# POLICIES AND SECTORAL INITIATIVES CYBER SECURITY POLICY

Uganda has a national cyber security policy, the National Information Security Policy, published in 2014. The policy outlines the mandatory minimum security controls that must be applied by all public and private sector organisations that use, own and/or operate protected computers, and handle official communications and personal data to reduce their vulnerability to cyber threats. The policy also defines 'critical infrastructure' and 'critical information infrastructure'. Uganda also has a National Information Security Strategy (NISS), according to the National Information Technology Authority (NITA). The National Information Security Strategy (NISS) does not provide specific actionable directives related to cyber security.

As regards privacy, the National Information Security Policy requires all organisations to "Ensure that remote access solutions, including contracts with IT suppliers, comply with applicable legislative or regulatory constraints in particular the Official Secrets Act, 1964 and the Access to information regarding the handling of information, which is likely to prejudice the security of the State or interfere with the right to the privacy of any other person."

The Uganda National Computer Emergency Response Team (CERT-UG) was established in 2014 to coordinate cyber security incident response. In July 2017, the Daily Monitor reported that the Chinese government had agreed to offer Uganda a comprehensive cyber security solution through a statutory company. The solution would reportedly include technical capacity to monitor and prevent social media abuse.

# SURVEILLANCE AND PRIVACY (PHONE-TAPPING AND CCTV)

The Ugandan government has been investing heavily in CCTV. The number of cameras in the capital Kampala appears to have increased over the last several years and the government periodically announces new purchases of CCTV technology, primarily in Uganda's main cities.

In 2014, it was reported that a Chinese telecommunications technology company, Huawei, had donated a multi-tracking system worth US$ 750,000 to the Kampala Capital City Authority of the Ugandan government. In March 2017, President Museveni announced that new CCTV cameras would be installed in all major towns of Uganda and along highways following the murder of a senior police officer. In February 2015, the Ugandan Parliament reportedly spent UGX 28 billion (over US$ 9.8 million) on CCTV cameras and other security measures provided by Chinese technology firm ZTE. Nevertheless, the police requested a further investment of 203 billion UGX (US$ 43 million) in CCTV in April 2017,

In early 2017, the Uganda Police Force launched a new smartphone app to encourage citizens to report crimes. Civil society groups including PI partner Unwanted Witness raised concerns about the wide range of access permissions the app requires from its users.

# AFRICAN PERSPECTIVES ON DATA PROTECTION AND PRIVACY

Privacy and personal and data protection in Africa has gained important relevance at the national, regional and international levels. Presently, there are sixteen countries in Africa with Privacy and Data Protection laws including Angola (2016), Equatorial Guinea (2016), Mauritania (2017), South Africa (2013), Burkina Faso (2004), Mali (2013), Gabon (2011), Benin (2009), Ghana (2012), Ivory Coast (2013), Lesotho (2012), Madagascar (2014), Morocco (2009), Senegal (2008), Tunisia (2004), Zimbabwe (2003). Others including Kenya, Niger, Nigeria, Tanzania and Uganda have drafted bills which are

awaiting enactment. There are currently over 800 telecom operators and 300 broader mobile ecosystem of;[97] handset and device makers, equipment providers and internet companies, software companies as well as organisations in adjacent industry sectors. There is also increased demand for mobile telecommunications. Globally, by the end of 2016, two thirds of the world's population (4.8 billion) had a mobile subscription. It is expected that by 2020, close to three of the world population (5.7 billion people) will subscribe to mobile services. By the end of 2016, Sub Saharan Africa had over 420 million mobile subscribers with an equivalent penetration rate of 43%, a Compound Annual Growth Rate of 6.1% over the five years to 2020 making it higher than the global average by 50%.[100] Due to progressive increment in mobile subscriptions, there is reciprocal increment in regulation of mobile service users and therefore increased personal data collection as well as interference with privacy rights. Nevertheless, most of the people in Africa are neither familiar nor aware of privacy and data protection laws even where they exist.

Africa has not been silent. Adopted at the 23rd Ordinary Session of the Summit of the African Union in Malabo, Equatorial Guinea, 2014, the African Union Convention on Cyber security and Personal Data Protection (AU Convention on Cyber Security and Personal Data Protection) is the first all African Union Member States guiding instrument on privacy and personal data protection. The AU Convention on Cyber Security and Personal Data Protection is *inter alia* inspired by Africa's commitments to regional and international initiatives as well as individual state initiatives establishes a legal framework for Cyber-security and Personal Data Protection especially in e- commerce. It outlines internationally recognised principles in personal data collection, storage and processing. The AU Convention further calls upon African Union (AU) member states to establish legal and institutional frameworks for data protection and cyber security such as legislation and data protection authorities.

Worryingly, the AU Convention on Cyber Security and Personal Data Protection has been signed by nine (9) member States - Benin, Chad, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia -

and has only been ratified one state- Senegal. This by implication shows that the Convention is largely unimplemented.

It is important to note that prior to the AU Convention on Cyber Security and Personal Data Protection, there were sub-regional and individual states' initiatives on privacy and personal data protection as briefly outlined below. For instance, there were existing frameworks which attempt to address privacy issues such as the Declaration of Principles on Freedom of Expression in Africa (2002) (Part V), the Resolution on the Right to Freedom of Information and Expression on the internet in Africa – ACHPR/Res. 362(LIX) 2016, and the African Declaration on Internet Rights and Freedoms

However, the African Union Convention on Cyber Security and Personal Data Protection is prone to abuse by a highly politicised Africa that, that usually affords politicians, especially those in power to unlawfully access and manipulate personal data for their political interests. Worse still, there is no emphasis of strict judicial oversight over the implementation of privacy rights. The AU Convention on Cyber Security and Personal Data Protection is also susceptible to ignore by virtue of the state sovereignty doctrine that allows states to enjoy internal and external autonomy uninterrupted. The doctrine of state sovereignty has been widely witnessed in state enactment of laws that undermine privacy and data protection despite international commitments in countries like Uganda, Zimbabwe and Tanzania among others on regulation of SIM Cards registration and freedom of expression online.

# AFRICA'S RESPONSE TO PRIVACY ISSUES REGIONAL INITIATIVES

AU Convention on Cyber Security and Personal Data Protection recognises existing commitments of AU Member States at sub-regional, regional and international levels to build the information society. These commitments include Cyber Security, Personal Data and privacy Protection. Regional Economic Communities (RECs) usually adopt treaties or issue model laws which are essential for good governance of member states' relations. In this particular case,

the Southern African Development Community (SADC), the Economic Community of West African States (ECOWAS) and the East African Community (EAC) have taken some measures on privacy and personal data protection, as discussed below.

The SADC model law presents an ideal piece of legislation that may be wholly adopted by member states for uniformity purposes across the region by just inserting the date of publication in the Gazette and the name of the country as indicated in its preamble. Such would be ideal for protection of portability of data issues within the region.

Nevertheless, this model law lacks a supranational element and is therefore subject to national laws of member states as indicted in Part II, section 2 (5). Further, in terms of limitations, it presents blanket conditions under section 42 (1) of state security, defence, public interest, preservation of the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures or violation to professional codes of conduct in the case of a regaled profession and exercise of official authority. These limitations have in practice been overly used to abuse citizens' rights across Africa and are therefore open to misuse such as in, illegal access and processing of personal data.

Further, the SADC in 2013 adopted a model law on Computer Crime and Cybercrime. The main objective of this model law is to criminalize all cases cybercrimes and provide for investigatory measures for such crimes. The model law lists offences of a cyber natures, addresses issues of jurisdiction, presents admissibility of evidence and the associated procedures for prosecution of cybercrimes and as well enlists liability from cybercrimes. Similar to the above is the SADC Model Law on Electronic Transactions and Electronic Commerce of 2013 which applies to electronic transaction or electronic communication including consumer protection, e-commerce and the duties and obligations of service providers. The protectionism of the law is linked to privacy and personal data protection.

These models are however not binding on States and may be superseded by individual state sovereignty, a factor that undermines their importance.

## THE ECONOMIC COMMUNITY OF WEST AFRICAN STATES

The ECOWAS in 2010 at the 37th session of the authority of heads of state and government adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS. Among others, this supplementary Act calls upon member states to establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data. Unfortunately, the supplementary Act under 2 places interests of the above privacy and personal data protection rights of the individual, a fact that may undermine the enjoyment of individual rights at the whims of the member states.

Additionally, the ECOWAS has issued a Cybercrime directive: Explanatory notice which is an important step to fighting cybercrime in the region as it aims at helping ECOWAS member States increase their understanding cybercrime and establish sound legal basis for cyber protection of the consumer. Among the key issues raised include fraudulent access computer systems, computer data and usage of the same for fraudulent purposes as well as child pornography.

It is important to note that despite the provisions in the above instruments, the instruments are not binding on ECOWAS member states but only offers guidelines on the ideal state of enjoyments of privacy and personal data rights and penalisation and associated procedures on cybercrimes respectively.

## THE EAST AFRICAN COMMUNITY

The EAC has not adopted specific legislation on data protection and privacy. However, it has a Framework for Cyber laws developed in 2008 to guide the member states on regional and national processes facilitating a harmonised legal regime on electronic commerce and curbing unlawful conduct. The framework law calls for member states to enact laws that protect personal data.

Nevertheless, it is a framework that creates no binding obligations or measures for EAC member States. Thus, by its nature and scope, EAC member States can either take on its guidance or depart from it. In the circumstances, it becomes hard to achieve uniformity in the REC.

It is important to observe here that all the RECs under study acknowledge the importance of privacy and data protection. In so doing, they have responded by putting in place guidance and regulatory measures for their member states. Amongst the key outstanding recommendations is that for the establishment of data protection authorities. Data protection authorities are important for ensuring personal data is managed subject to accountability to data subjects. Nevertheless, regional efforts are not binding on member states. Implementation of the respectively presented legislation in the RECs is subject to the choice of a given member states. While the vision of regional efforts is to ensure that the individual is guaranteed privacy and personal data protection, this aim is watered down by the sovereignty doctrine of member states.

# AFRICAN STATE INITIATIVES

A number of states in Africa, such as Uganda, Tanzania, Kenya, South Africa, Zambia, Zimbabwe, Democratic Republic of Congo, Ghana, Nigeria, Sierra Leone, Egypt and Botswana recognise the right to individual privacy in their national constitutions as a fundamental human right.[118] These provisos are acknowledged in the preamble to the AU Convention on Cyber security and Personal Data Protection, para 6 inter alia that; "considering that the establishment of a regulatory framework,-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law…".

Further states have embarked on a journey to implementing data protection laws. Nevertheless, implementation has generally taken a slow path. For instance, there are only sixteen (16) listed above out of 55-member states of the African Union with privacy and data protection related legislation while others like

Uganda, Tanzania and Zambia have grappled with bills on the privacy and data protection for an average period of not less than three years for each.

On the contrary, African Union member states have been fast on narrowing the space within which privacy is enjoyed online by enacting legislation that limit freedom of expression, freedom of association and access to information with little regard to the provisions of international human rights instruments and specifically in Africa, the African Charter on Human and Peoples Rights, the Declaration of principles of freedom of expression in Africa (2002) and the African Declaration on Internet Rights and Freedoms, among others.

For instance, Uganda is largely criticised for the enactment of the Uganda Communications Act 2013 as amended 2017; Regulation of Interception of Communications Act, 2010, Electronics Signatures Act 2011, Computer Misuse Act, 2011, Anti-Terrorism Act, 2002 as amended 2015 and 2016, and the Anti-Pornography Act, 2014 which require among others, compulsory SIM Card registration and interception of communication that have a direct and chilling effect on privacy, freedom of expression, freedom of association and access to information.

# COMPARATIVE ANALYSIS WOTH OTHER COUNTRIES

Democratic Republic of Congo through its Framework Law 013/2002 on Telecommunications, Decree-Law No 1-6l of 25 February 1961, Ministerial Decree No.003/CAB/MIN/PTT/K/2000, Ministerial Order No. 25 / CAB / VPM / MIN / INTERSEC / 024/2015. Zambia through the Information and Communication Technologies Act of 2009, Independent Broadcasting Authority Act, 2002, Electronic Communications and Transactions Act No 21 of 2009, Penal Code Act 2012, Statutory Instrument on the Registration of Electronic Communication Apparatus No. 65 of 2011 have limited the enjoyment of privacy and data protection related rights. Further Zimbabwe through the Access to Information and Protection of Privacy Act Chapter 10:27, Broadcasting Services Act Chapter 12:06 as amended 2007, Censorship and Entertainments

Control Act, Chapter 10:04, Criminal Procedure and Evidence Act Chapter 9:07 as amended 2006, Interception of Communications Act Chapter 11:20, No. 6/2007, Postal and Telecommunications Act Chapter 12:05 and the Printed Publications Act Chapter 25:14.

Botswana through the; Communications Regulatory Authority Act, 2012, Cybercrime and Computer Related Crimes Act Chapter: 08:06 and Rwanda through the law No 02/2013 of 08/02/2013 regulating media, law Number 09/2013 of 01/03/2013 establishing Rwanda Utilities Regulatory Authority, ICT law number 24/2016 of 18/06/2016, Law number 18/2010 of 12/05/2010 on electronic messages, electronic signature and electronic transactions, Code of Criminal Procedure, under Law n° 30/2013, Law No.60/2013 Regulating the Interception of Communications and regulation of SIM Card registration 001/ICT/RURA /2013 have not got any better criticism than failure to comprehensively protect the right to privacy of the individual especially in light of adopting draconian legislation. Indeed, some of them such as Rwanda, Zimbabwe and the Democratic Republic of Congo are considered to be having very restrictive and delimiting legal regimes.

# CIVIL SOCIETY AND PRIVATE SECTOR INITIATIVES

Civil Society Organisations (CSOs), the private sector, and the academia play an important role in ensuring checks and balances in governance at the national, sub-regional, regional and international levels. They instrumentally influence transparency and accountability in key political decisions, including legislative, social, political and economic undertakings as well as human rights promotion and protection.

CSOs and the private sector have been instrumental in influencing the privacy and data protection regimes in Africa. For instance, there were numerous concerns raised by CSOs and the private sector about the initial draft of the AU Convention Cyber Security and Personal Data Protection on grounds that it was

too vague and insufficiently addressed privacy related rights. In response, it was deferred for a later time, hence the adoption of 2014 which presents an improved version especially in light of privacy rights. For instance, the right of the individual to object to processing of data was added under article 18; the right to privacy was added under section 25 (3); and the inclusion of CSOs under article 26 (1) (b). The Commission of the AU has also, of May 30, 2017 in joint effort with the Internet Society (a CSO) issued Internet Infrastructure Security Guidelines for Africa to facilitate implementation of the Convention. It is important to note that these guidelines have been a result of concerted effort of regional and global Internet infrastructure security experts, government and CERT representatives, and network and CCTLD Domain Name System (DNS) operators.[124]

At individual states' level, CSOs and the academia in Africa including in Uganda, Kenya, Rwanda, Tanzania, Democratic Republic of Congo and Zimbabwe have been at the forefront of analysing and critiquing proposed privacy and data protection laws. As part of the intervention measures, they have been instrumental in presenting recommendations for improved legislation on privacy and personal data protection.

Despite the contributions by CSOs and private sector, they often labelled and branded as supporters of opposition and saboteurs of government activities. The operating environment and civic space continues to shrink across Africa, thereby affecting their effectiveness in promoting accountability and transparency, specifically in the ICT sector which goes to the core of online privacy and personal data protection.

# LESSONS FROM OTHER REGIONS

The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD Guidelines), the Asia-Pacific Economic Community Privacy Framework (APEC Privacy Framework), the General Data Protection Regulation (GDPR) and the Guidelines on Data Protection in EU Financial Services regulation largely offer important lessons to AU member States and

Africa as a whole in privacy and data protection. For instance, they present the basic concepts, guidance and issues that States need to pay attention to such as data protection principles, the rights of the data subject and the establishment of a data controlling authority/body. These principles are for instance enumerated under the Chapter II of the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS on a data protection authority and chapter VI on the rights of the data subject. Part III of the SADC Model Law on the data protection authority and part VII on the rights of the data subject. These very principles are traceable in the GPDR, Chapter III on the rights of the data subject and Chapter IV on the Data controller and processor. While majority are not binding, they go to the root of privacy and data protection if not followed or adhered to. Africa as a whole has made attempts to emulate instruments from other regions but still lacks exhaustive cover of privacy and data protection rights especially in light of portability and territorial jurisdiction and definition of the functions of the data controller.

On a positive note, all if not majority of privacy and data protection laws and bills for implementation in Africa have imbedded data protection principles laid down in aforementioned instruments. For instance, most of data protection legislation and proposed laws have imbedded, internationally recognised data protection principles, rights of data subjects as well as the establishment of data protection authorities; namely the data protection and privacy related laws of Angola (2016), Equatorial Guinea (2016), Mauritania (2017), South Africa (2013), Burkina Faso, (2004), Mali (2013), Gabon (2011), Benin (2009), Ghana (2012), Ivory Coast (2013), Lesotho, (2012), Madagascar (2014), Morocco (2009), Senegal (2008), Tunisia (2004), Zimbabwe (2003). The bills of Kenya, Niger, Nigeria, Tanzania and Uganda also have similar provisions.

Equally, the rights of the data subject are outrightly evident in Africa's efforts to protect privacy and personal data related rights. Further, in terms of the scope of definition of personal information and data processors presents a commonality across the instruments, and this has been imbedded in individual state laws and proposed laws on privacy and data protection.

Nevertheless, there are unique differences from which major lessons may be drawn for African states. Some of the instruments like the APEC Privacy Framework and the OECD Guidelines offer general protectionist strategies for data and privacy while the GDPR protection is specific and centred on personal data protection as a primary purpose for its adoption in Europe. In terms of territorial scope, the GDPR uniquely extends protection in every jurisdiction and processing of personal data is subject to acceptable permission.

The issue of privacy and data protection as going to the core of fundamental human rights and freedoms. Hence the Guidelines on data protection in EU financial services regulation which is to reinforce data protection in financial markets to ensure privacy is not breached, data is not illegally processed and is only processed for a specific period for a specific purpose, ensure appropriate security measures as well as provision for supervisory and specific procedural measures for data processing. Generally, Europe as seen in the GDPR has a much stronger personal data protection regime when compared with model laws or frameworks in other regions like the EAC, ECOWAS and SADC the rest of the instruments.

The above instruments offer practical guidance to African states on the emerging privacy rights and data protection trends. In the technologically evolving Africa with growing e-commerce, Africa needs to draw practical examples the protection of the African person against misuse and abuse of privacy and personal data.

# EUROPEAN PERSPECTIVES OF DATA PROTECTION THE RIGHT TO DATA PROTECTION

Privacy and data protection are two rights enshrined in the European Union Treaties and in the European Union Charter of Fundamental Rights.

The Charter contains an explicit right to the protection of personal data (Article 8). The entry into force of the Lisbon Treaty in 2009, gave the Charter of

Fundamental Rights the same legal value as the constitutional treaties of the EU. Thus the EU institutions and bodies and the Member States are bound by it.

In addition, article 16 of the Treaty on the Functioning of the European Union (TFEU) obliges the EU to lay down data protection rules for the processing of personal data. The EU is unique in providing for such an obligation in its constitution.

## *Data Protection Law*

For decades, the EU has held high standards of data protection law. The law entitles individuals to exercise specific data protection rights and obliges (public or private sector) organisations that process their data to respect these rights in April 2016, the European Union adopted a new legal framework - the General Data Protection Regulation (GDPR) and the Data Protection Directive for the law enforcement and police area.

Fully applicable across the European Union in May 2018, the General Data Protection Regulation is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age. It applies to organisations or companies not established in the EU who offer goods and services to individuals in the EU or monitor their behaviour. It creates new rights for individuals in the digital environment and several new and detailed obligations for cooperation. Globally, there is an increasing growth in data protection (sometimes referred to as data privacy in non-EU countries) laws. Many of these laws are strongly influenced by the EU rules, which have long been considered the gold standard in data protection law. Over 100 countries around the world now have data protection laws in place: fewer than half of these countries are in Europe (28 EU Member States and others). The majority of data protection laws have been adopted outside of Europe, with the fastest growth seen in African countries.

## *Data Protection in Practice*

In most countries, national Data Protection Authorities (DPAs) or Regulators have been established to be the guardians of data protection. For the enforcement of data protection laws to be effective, DPAs are given the power to investigate, detect and punish violations as well as the responsibility to raise awareness of data protection rights and obligations in general. In the EU, this effectiveness is strengthened by the requirement for DPAs to be independent of any political, governmental or other influence. Furthermore, good cooperation between DPAs (Article 29 Working Party, EDPB) ensures greater consistency of data protection in the EU.

## *Independence*

In the EU the requirement for Data Protection Authorities to be independent is laid down in law: Article 16(2) of the Treaty on the Functioning of the EU (TFEU) and Article 8(3) of the European Union Charter of Fundamental Rights.

The Court of Justice of the European Union, has consistently emphasised that control by an independent authority is an essential component of the right to data protection and has laid down the criteria for such independence. In particular, the supervisory authority must act with complete independence, which implies a decision-making power independent of any direct or indirect external influence. The Court has also emphasised the crucial role of EU independent supervisory authorities in relation to control of international transfers to non-EU countries.

The General Data Protection Regulation (GDPR) also emphasises the importance of independence; Chapter VI of the GDPR provides detailed rules for the establishment and functioning of independent supervisory authorities, including provisions on the resources necessary for the effective performance of their tasks and powers.

The EDPS is an independent supervisory authority responsible for ensuring that EU institutions and bodies comply with data protection law when processing personal data.

### *Cross border Data Protection.*

Data protection laws are national but in the online environment, data does not respect borders. Cross-border cooperation and agreements to deliver effective data protection are essential, particularly if the EU is to maintain its values and uphold its principles. To achieve this, the EDPS regularly interacts with EU and international DPAs and Regulators to influence and develop cross-border enforcement.

## PRIVACY, DATA PROTECTION AND SECURITY

In the European Union, privacy and data protection are not absolute rights and can be limited under certain conditions according to the EU Charter of Fundamental Rights. The rights to privacy and data protection may need to be balanced against other EU values, human rights, or public and private interests such as the fundamental rights to freedom of expression, freedom of press or freedom of access to information.

The rights to privacy and data protection may also need to be weighed up against other public interests, such as national security. EU Member States adopt measures to combat terrorist threats, but more generally to reinforce the judicial and police cooperation in criminal matters in the area of Freedom, Security and Justice (AFSJ). In the EU, national security is the sole responsibility of each Member State and is outlined in the Treaty on the Functioning of the EU (article 4.2 TFEU).

However, the courts by means of the specific legal provision on data retention, are now exploring the boundaries of this competence: according to the Court of Justice of the EU (CJEU), even measures derogating from EU law are subject to the Charter of Fundamental Rights.

In any case, the scale of collection, storage and cross-border exchange of personal data between Member States in crime and terrorism matters is enormous. The increased access to European databases as well as to commercial

data for law enforcement purposes are challenging the balance between privacy and security.

Data protection authorities in general have a pivotal role to play in ensuring this balance between privacy and other interests, including in the sensitive domain of security where their role is expanding; for instance on 1 May 2017, the EDPS took over the data protection supervision of Europol, the EU body actively cooperating with law enforcement authorities to combat international crime and terrorism.

The EDPS' role of independent adviser to the EU institutions relates to all matters concerning the processing of personal data, including initiatives to improve security in the EU and new data- exchange tools for law enforcement agencies.

Indeed, the EDPS has issued numerous Opinions on initiatives to expand information sharing for law enforcement purposes inside the EU including on the Entry/Exit System and EU PNR - but also outside of Europe such as the Umbrella Agreement with the US and PNR agreements with non-EU countries.

# INTRODUCTION TO DATA PROTECTION LAW

Protection of database and associated rights is gaining traction in Uganda. The vast volume and deluge of data available with the Business Processing Offices in Uganda from jurisdictions which have stringent database protection laws have increased the awareness and need for adequate protection of personal data through domestic legislation or international commitments. But the question whether Uganda has adequate measures in place for database right protection still remains to be answered.

A number laws in Uganda attempt to address issues or data base protection while there is a Data Protection and Privacy Act, 2019.

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious

threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment.

Database security covers and enforces security on all aspects and components of databases. This includes:

1. Data stored in database
2. Database server
3. Database management system (DBMS)
4. Other database workflow applications

Database security is generally planned, implemented and maintained by a database administrator and or other information security professional. Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered personal data.

The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights; and to exercise other rights and freedoms - such as free speech or the right to assembly.

Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors.

The protection of personal data (data protection) is recognized by the HR Committee as a fundamental part of privacy as protected by **Article 17 of the ICCPR. The HR** Committee in General Comment 16 stated that:

The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the

hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. (HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 10.)

Some of the ways database security is analyzed and implemented include:

1. Restricting unauthorized access and use by implementing strong and multifactor access and data management controls

2. Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDS) attack or user overload

3. Physical security of the database server and backup equipment from theft and natural disasters

4. Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

Database protection is essential to any company with any online component. Sufficient database security prevents data bring lost or compromised, which may have serious ramifications for the company both in terms of finances and reputation.

Security risks to database systems include, for example:

1. Unauthorized or unintended activity or misuse by authorized database users, database administrators, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations);

2. Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or

damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services;

3. Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence;

4. Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized privilege escalation), data loss/corruption, performance degradation etc.

Databases have been largely secured against hackers through network security measures such as firewalls, and network-based intrusion detection systems. While network security controls remain valuable in this regard, securing the database systems themselves, and the programs/functions and data within them, has arguably become more critical as networks are increasingly opened to wider access, in particular access from the Internet. Furthermore, system, program, function and data access controls, along with the associated user identification, authentication and rights management functions, have always been important to limit and in some cases log the activities of authorized users and administrators. In other words, these are complementary approaches to database security, working from both the outside-in and the inside-out as it were.

Many organizations develop their own "baseline" security standards and designs detailing basic security control measures for their database systems. These may reflect general information security requirements or obligations imposed by corporate information security policies and applicable laws and regulations (e.g. concerning privacy, financial management and reporting systems), along with generally accepted good database security practices (such as appropriate hardening of the underlying systems) and perhaps security recommendations from the relevant database system and software vendors. The security designs for specific database systems typically specify further security administration

and management functions (such as administration and reporting of user access rights, log management and analysis, database replication/synchronization and backups) along with various business-driven information security controls within the database programs and functions (e.g. data entry validation and audit trails). Furthermore, various security-related activities (manual controls) are normally incorporated into the procedures, guidelines etc. relating to the design, development, configuration, use, management and maintenance of databases.

Ross J. Anderson has often said that by their nature large databases will never be free of abuse by breaches of security; if a large system is designed for ease of access it becomes insecure; if made watertight it becomes impossible to use. This is sometimes known as Anderson's Rule.

Multinational companies take pride in the database of the clients they possess. The value of the right in database and its association with the companies' goodwill is increasingly leading to actions by companies for their protection. Recently Golbibo terminated the services of its marketing agency as it had Golbibo's database for sending out promotional emails for another company. In fact some franchising and marketing agreements mandate sharing of data and defines ownership at dissolution of the arrangement. .When such agreements propose to deal with personal data, particularly the physical condition or sexual orientation as most traditional forms filled by customers of marketing companies, restaurants, retail chains require, a duty is enjoined upon them to formulate a privacy policy which should be intimated to the information provider

# DATA PROTECTION PRINCIPLES

Data protection principles are provided for under **section 3 of the Data Protection and Privacy Act, 2019.**

Section 3 provides that a data collector, data processor or data controller or any person who collects, processes, holds or uses personal data shall be accountable to the data subject for data collected, processed held or used;

*(a)* collect and process data fairly and lawfully;

*(b)* collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data;

*(c)* retain personal data for the period authorised by law or for which the data is required;

*(d)* ensure quality of information collected, processed, used or held;

*(e)* ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and

*(f)* Observe security safeguards in respect of the data.

The Authority shall ensure that every data collector, data controller, data processor or any other person collecting or processing data complies with the principles of data protection and this Act.

Under data protection, every organisation (data controller) that processes personal information (personal data) must notify the relevant authority, unless they are exempt in any case where data is or has been processed. Failure to notify is a criminal offence.

Personal Data is defined in the Law as, "Any Data referring to an Identifiable Natural Person" and Sensitive Personal Data is defined as, "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life." Such data includes but is not limited to name, address, email address, phone numbers, geolocations, job title, health and biometric data, religious affiliations or criminal history.

**Section 2 of the Data Protection and Privacy Act, 2019** for Uganda defines personal data as; "Means information about a person from which the person can be identified, that is recorded in any form and includes data that relates to—

*(g)* the nationality, age or marital status of the person;

*(h)* the educational level, or occupation of the person;

*(i)* an identification number, symbol or other particulars assigned to a person;

*(j)* identity data; or

*(k)* other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual."

Personal Data generally can be any information that when viewed together (or in some cases is so unique) it clearly identifies a living individual. It could be data about clients, employees, suppliers, or family members, to name a few categories of Personal Data. Many if not all organizations process Personal Data as a result, and will be required to submit a notification request to the relevant authority.

Data Controllers who Process Personal Data in accordance with the Law provide certain details about their Processing of Personal Data so that the authority may keep a public register describing the Processing.

The principal purpose of notifications and a public register is transparency and openness, to ensure compliance with the principles for ethical, legitimate, fair and limited personal data management. Notification is a resulting function of data protection law and policy so the public knows or should be able to find out who is processing Personal Data and for what reasons

# DETAILS ON DATA PROTECTION PRINCIPLES

**Fair, Lawful, and Transparent**

Personal data undergoing processing should be processed lawful manner and Personal data undergoing processing shall be processed fairly and in a transparent manner.

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

Personal data must be processed in a lawful and fair manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. 'Fairness and transparency' are essential for ensuring that people's data is not used in ways they would not expect. 'Lawful' means that data must be processed in a way that respects of rule of law and that meets a legal ground for processing. A 'legal ground' is a limited justification for processing people's data set out in law (e.g. consent) - discussed in the below section on 'Lawful Grounds for Processing'.

Every individual should be informed and aware of how their data is going to be processed, and by whom. If there is an intention to share the data of an individual with a third party but the data controller is not transparent about this fact and the data subject is not clearly informed, it is likely that their personal data was obtained unfairly, and the process will not be considered transparent.

It is not enough to just be clear about what you are doing with people's data, but the lawful criteria included in this principle means that an entity must be justified in doing so by satisfying a legal ground.

**Purpose Limitation principle.**

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the

fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

Personal data undergoing processing must be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes.

All personal data should be collected for a determined, specific, and legitimate purpose. Any further processing must not be incompatible with the purposes specified at the outset (i.e. the point of collection). This essentially means that it is not acceptable to state that you need a person's data for one purpose, and then use it for something else without notice or justification.

In **Community Charge Registration Offices /CCROs Of Runnymede BC , South North Ampton Shire DC and Harrow BC v Data Protection Registrar**[99], the local finance Act provided that the CCROs were required to compile and maintain community charges and take reasonable steps to come up with that purpose however they instead even obtained information on property yet they were not supposed to do so.

It was held that CCROs were holding far more important information than was in fact necessary for their purposes and so in breach of the purpose limitation principle.

Technological developments (and the mass generation, collection, and analysis of data which accompany them) mean that these principles are ever more important. The purpose of processing and the proposed use of the data must be clearly defined and explained to the data subject. If the data is to be used for a purpose other than the original purpose, then the data subject should be adequately informed of this and a legal condition for this processing identified; this may necessitate obtaining further consent. It is particularly important that

[99]Community Charge Registration Offices Of Runnymede BC , South North Ampton Shire DC and Harrow BC v Data Protection Registrar Case DA /90 24/49/3,4 and 5

sensitive personal data is not processed for purposes other than those originally specified.

This is particularly relevant to big data and other data analysis processes. For example, the data broker industry thrives off the re-purposing of data:2 they amass data from a vast array of sources, then compile, analyse, profile, and share insights with their clients. This means that a lot of data shared for one purpose is re-purposed in ways they might not expect, including targeted advertising.

Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, in accordance with the 'Purpose Limitation Principle'.

There are, however, two common exceptions to this principle: it is acceptable if done:

a. with the consent of the data subject

b. by the authority of law

While these are two widely recognised exceptions to the use limitation principles, they are often abused and misused. In the case of (a), consent must be valid; it must not be conditional, obtained through pre-ticked boxes, or have the details of these other purposes hidden in small print or legalese (inaccessible to the average data subject). In the case of (b), this has been used to allow for wide data-sharing arrangements by state bodies and institutions in the exercise of their functions, for example, using data provided for healthcare or education purposes for immigration purposes. Such blanket exemptions threaten to weaken the protection offered by data protection law, so it is crucial that any provisions providing for exceptions be narrowly constructed, so that the principle of purpose limitation is not made redundant and unenforceable when it comes to the State and its functions, and exchanges of information between state agencies and that there are limits on the reliance on consent, for example where there is an imbalance of power.

Furthermore, in relation to purpose limitation, the text of a law could provide for various purposes which should not be incompatible with this principle.

These could include, but are not restricted to:

- Archiving purposes in the public interest
- Scientific, statistical or historical purposes

It is essential that these purposes be restricted in their scope, and the above terms be further defined to provide clarity as to what each could entail.

If no clear limitations are established at the point of collection as to the uses of the data, there are concerns that the data could be used for other objectives over the data lifecycle, which could have detrimental effects on individuals and lead to abuse. There are an increasing number of cases in which the principle of purpose limitation is being undermined and bypassed. For example, Aadhaar, India's national biometric database, was originally established in 2009 with the aim of standardizing government databases. However, over time, the project has become more ambitious and it is now being used for an array of purposes from school admissions to obtaining death certificate

Eurodac, a biometric database established in 2000 to enable EU Member States to check whether an asylum seeker had previously applied for asylum in another European country or was receiving social benefits from another EU country, is now being used for a new purpose.

The updated Eurodac Regulation, which came into force in July 2015, now allows for the "use of the Eurodac database of asylum-seekers' fingerprints f or preventing, detecting and investigating terrorist offences and other serious crimes."

**Principle of Minimisation**

Personal data should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

Personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed**.**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data minimisation is a key concept in data protection, both from an individual's rights and an information security perspective. The law should clearly stipulate that only the data which is necessary and relevant for the purpose stated should be processed. Any exceptions to this must be very limited and clearly defined.

**The principle of Necessity**

This aims at ensuring that the data collected is not intended to be more far-reaching than is necessary for the purposes for which the data will be used. The test should be that the least intrusive method is used to achieve a legitimate aim.

The "purpose test" - as the OECD has called it - "will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating." The concept of necessity also entails an assessment of whether the same aim could be achieved in a way that is less intrusive i.e. uses less data.

**Principle of Relevancy**

Any data processed must relevant to the purposes established. This principles requires that those processing data to consider what the minimum amount of data necessary to achieve the purpose would be. Processors should hold that and no more - it is not acceptable to collect extra data because it might be useful later on, or simply because no thought has been given to whether it is necessary in a specific scenario.

For example, it would be excessive to process precise and detailed location data for connected cars for a purpose involving technical maintenance or model optimisation.

The principle of data minimisation is even more integral in the age of big data, where advancement in technology has radically improved analytical techniques for searching, aggregating, and cross- referencing large data sets in order to develop intelligence and insights. With the promise and hope that having more data will allow for accurate insights into human behaviour, there is an interest and sustained drive to accumulate vast amounts of data. There is an urgent need to challenge thisnarrative and ensure that only data that is necessary and relevant for a specific purpose should be processed.

**Accuracy**

Personal data should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. Personal data undergoing processing shall be accurate and, where necessary, kept up to date .Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Personal data must be accurate throughout processing and every reasonable step must be taken to ensure this. This includes the following elements:

Accuracy: All data processed must be accurate throughout the data lifecycle;

Complete: Any category of data must be complete to the extent possible that the omission of relevant data may not lead to the inference of different information to the information that could be obtained if the data were complete;

Up-to-date: Any data that is retained and may be further processed in accordance with the provisions provided for in the data protection law must be kept up-to-date; and

Limited: Personal data should only be processed (and retained) for the period of time it is required for the purpose for which it was collected and stored.

The above elements reaffirm the rights of data subjects to access their personal data, and to correct incomplete, inaccurate, or outdated data which should be provided for in a data protection law.

Increasingly, decision- and policy-making processes rely on data. However, there is a high risk that if the data is not accurate and up-to-date, then the outcome of the decision-making process will also be inaccurate. In the most serious scenarios, this could lead to a decision that an individual is not granted access to public services, or to welfare programmes, or given a loan. For example, there have been incidences of individuals wrongly denied a loan or re-mortgage on their house because the company in charge of reviewing their credit score had inaccurate information which brought down their rating from 'Excellent ' to 'Poor', or because inaccurate information was registered by banking institutions which made an individual an undesirable customer

**Storage Limitation**

Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Personal data undergoing processing shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject. (‘Storage limitation')"

Personal data should only be retained for the period of time that the data is required for the purpose for which it was originally collected and stored. This will strengthen and clarify the obligation to delete data at the end of processing, which should be included in another provision.

The law should clearly stipulate that data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be very limited and clearly defined.

Just because the data controller might come across another use of the data does not justify blanket or indefinite retention. How long it is necessary to store data will be context-specific, however, this should be guided by other legislative obligations and regulatory guidance. For individuals to be fairly informed about the processing of their data, they must be informed how long their data will be retained, it is therefore imperative that legislation incentivises data controllers to implement the data minimisation principle by minimising the collection of personal data, and not storing it longer than necessary.

Data controllers should establish retention schedules specifying the retention periods for all the data that they hold. These should be kept under regular review. This is separate to the deletion of personal data on the request of the data subject, which must also be provided for in the legislation. After the necessary time period, personal data should be securely deleted. If data is to be stored beyond the retention period in an anonymised (and not pseudonymised) form, the privacy implications and consequences for the data subjects must be carefully considered.

Even if data has been processed fairly, lawfully, in a transparent manner, and with respect to the principles of purpose limitation, minimisation and accuracy, it is essential to ensure that the data is not stored for longer than required and necessary for the purpose for which it was collected.

Any interference with the right to privacy and data protection requires to be necessary and proportionate. Blanket data retention completely fails to respect this - as confirmed in 2014, when the European Court of Justice struck down the Data Retention Directive, calling mandatory data retention, "an interference with the fundamental rights of practically the entire European population...without such an interference being precisely circumscribed by provisions to ensure that is actually limited to what i s strict ly necessary". This decision represented a

strong authoritative recognition of the safeguards that must be in place to protect our right to privacy.

Indefinite data retention is not only an infringement of the rights of an individual but a risk for those processing it. Failure to limit the period for which data is stored increases security risks and raises concerns that it could be used for new purposes merely because it is still available and accessible

There are risks that, if outdated, it could lead to poor decision-making processes which could have severe implications. In the age of widespread, unregulated state and corporate surveillance, it is essential that strict limitations are placed on data retention to mitigate possible unlawful interferences with the right to privacy.

**Integrity and Confidentiality**

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."

The controller, and, where applicable the processor, take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data."

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Personal data, at rest and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data.

Security safeguards could include the following.

- ❖ Physical measures, i.e. locked doors and identification cards, for instance;
- ❖ Organizational measures, i.e. access controls;
- ❖ Informational measures, i.e. enciphering (converting text into a coded form), and threat-monitoring; and
- ❖ Technical measures, i.e. encryption, pseudonymisation, anonymisation.

Other organisational measures include regular testing of the adequacy of these measures, implementation of data protection and information security policies, training, and adherence to approved codes of conduct.

If security measures are not taken to protect data, and ensure the security and safety of the infrastructure, data is left vulnerable to threats and is at risk of breach and unlawful access. There have been multiple examples of data breaches as a result of weak security.

For example, in March 2016, the personal information of over 55 million Filipino voters were leaked following a breach on the Commission on Elections' (COMELEC's) database. In September 2016, the National Privacy Commission concluded that there had been a security breach that provided access to the COMELEC database that contained both personal and sensitive data, and other information that may be used to enable identity fraud. The personal data included in the compromised database contained passport information, tax identification numbers, names of firearm owners and information about their firearms, and email addresses. A preliminary report identified that one of the indicators of negligence on behalf of COMELEC was vulnerabilities in their website, and failure to monitor regularly for security breaches.

In Duly 2016, due to security failures, a database of the Municipality of Sao Paulo, Brazil, was published exposing personal data of an estimated 650,000 patients and public agents from the public health system (SUS). The data included addresses, phone numbers, and even medical d a t a . Details of pregnancy stages and cases of abortion were also exposed.

**Accountability**

OECD: "A data controller should be accountable for complying with measures which give effect to the principles stated above"

Convention 108: "Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in **Article 15**, that the data processing under their control is in compliance with the provisions of this Convention." [**Article 10 (1)]**

An entity which processes personal data, in their capacity as data controllers or processors, should be accountable for complying with standards, and taking measure which give effect to the provisions provided for in a data protection law. Those with responsibility for data processing must be able to demonstrate how they comply with data protection legislation, including the principles, their obligations, and the rights of individuals.

The accountability principle is key to an effective data protection framework. It brings together all the other principles and puts the onus on those processing people's data (whether a company or a public authority) to be responsible for and to demonstrate compliance with their obligations. In practice, this means that those processing personal data should be more open and proactive about the way they handle data in compliance with their obligations. They must be able to explain, show, and prove that they respect people's privacy - both to regulators and individuals.

The importance of the accountability principle is clearest when considering contexts in which there are no accountability mechanisms in place - i.e. where there is no structure to report breaches of the law.

For example, in South Africa, The Protection of Personal Information (PoPI) Act was adopted in 2013, providing for the establishment of an Information Regulators, though this body was not put in place until April 2017. At present, data breaches in South Africa often go unreported: in 2015, it was reported that only five data breaches were registered in South Africa. This is expected to changesignificantly as PoPI comes into force, as responsible parties will be required by law to disclose information about data breaches if they occur.

Accountability mechanisms play an important role in investigating breaches and holding entities subject to the law to account. In 2017, following revelations of a major leak of data from taxi hire app Uber in 2016, the Mexican National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) asked Uber for information on the number of "Mexican users, drivers and employees" who had been affected. The institute also asked Uber for information on the measures the company is taking to mitigate damage and protect clients' information.

# CONSTRAINTS ON DATA PROCESSING

There are limits to data processing. Any data processing should be done within the established law See for instance **Part III of the Data Protection and Privacy Act, 2019 (Sections 7 – 19).**

**Section 7** Consent to collect or process personal data Section 8 Personal data relating to children

**Section 9** Prohibition on collection and processing of special personal data **Section 10** on the protection of privacy

**Section 11** on Collection of data from data subject.

**Section 12** on Collection of personal data for specific purpose

**Section 13** on Information to be given to data subject before collection of data. **Section 14** on the minimality principle

Section 15 on Quality of information Section 16 on Correction of personal data

**Section 17** on the requirement that further processing should be compatible with the purpose of collection.

**Section 18** on Retention of records of personal data Section 19 on processing personal data outside Uganda

## THE RIGHTS OF THE DATA SUBJECT

Generally, the common rights of data subjects are wide. In Uganda, some of the rights are provided for under sections 24 –28 of the Data Protection and Privacy Act, 2019 but can also be drawn from some provisions across the Act. Right to a remedy.

## CONFLICTING RIGHTS OF DATA SUBJECTS

It is important to bear in mind that the data which is subject to these rights may constitute the personal data of more than one data subject and the rights of data subjects may conflict with one another. The GDPR does not give automatic priority to one data subject's rights over another's and a balancing exercise will have to be undertaken on case by case basis. Opinions recorded by healthcare staff about a patient in that patient's care record constitute personal data of the patient. However, they are also likely to be regarded as the personal data of their author, whose rights will need to be considered in any processing decision.

The controller's responsibility to exercise the subject's rights

From the outset it is worth noting the obligations contained in Article 12, whereby the Controller is required to facilitate the exercise of the Data Subjects' rights. In summary:

**Article 12(3)** requires controllers to advise data subjects within one month of receipt of a request under articles 15 to 22 as to whether any action has been taken. That period may be extended by two further months where necessary.

**Article 12(4)** states that if the controller does not taken action, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and of the possibility of making a complaint to the supervisory authority.

**The right to rectification**

Data subjects have the right to obtain rectification of inaccurate personal data without undue delay and taking into account the purposes of processing, the right to have incomplete personal data completed.

In **Johnson V Medical Defence Union[100],** David Paul Johnson was a member of the Medical Defence Union , a group that provided its members with a range of discretionary benefits in the nature of advice and professional indemnity cover. The union carried out a risk assessment review in relation to him and this paved way for his expulsion from the Union.

Court found that some files had been unfairly processed because Johnson was not aware of the existence of his personal data therein , the purpose for which it was being processed or his right to access it and rectify it.

**The right to portability**

In effect this right is a subject access right. However, it applies only to personal data which the data subject has provided to a controller (and not information generated from that personal data), where the processing is based on the individual's consent or for the performance of a contract and when processing is carried out by automated means. This will include any computer based processing. Data controllers will be required to provide personal data to

[100]Johnson V Medical Defence Union [2006] EWHC 321

individuals, or in some cases other organisations, without hindrance, in a structured machine readable format.

**The right to restrict processing**

Under Article 18 data subjects have the right to restrict processing where accuracy of the data is contested.

The processing is unlawful and the data subject opposes the erasure of data

The controller no longer needs the data, but the subject requires the data for the establishment, exercise or defence of legal claims Or the data subject has objected to the processing pursuant to **Article 21(1**) pending the verification as to whether legitimate grounds of controller override those of subject

Where processing has been restricted, further processing, other than storage, may only go ahead with the consent of the subject or for the establishment, exercise or defence of legal claims or for the protection of another natural or legal person of for reasons of important public interest of the EU or a member state.

**The right to object**

Where the public interests or legitimate interests conditions in **Article 6** are relied upon, data subjects have the right to object to their personal data being processed at any time. The controller is not permitted to carry on processing unless it can demonstrate that there are compelling legitimate grounds which override the interest, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where processing is undertaken in reliance on consent, withdrawal of consent will render further processing unlawful in the absence of another relevant ground.

**Rights relating to automated decision making and profiling**

The GDPR's provisions are similar to those contained within the DPA. Individuals have a right not to be subject to a decision when it is based solely on automated processing, including profiling and where that decision produces a

legal or similarly significant effect on them. This does not apply where it is necessary for entering into a contract, authorised by law or based on explicit consent. The processing of special category personal data for automated decision making is subject to additional restrictions.

As the A29WP notes, 'Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people.'

There is ample scope for automated decision making in the context of health and social care, such as the use of risk rating algorithms. Whilst it is likely that such tools would normally be subject to human intervention in respect of the implementation of any resulting decision, the question of whether the degree of human intervention was adequate in a given case may be the subject of dispute.

Given the growth in the use of AI in healthcare this aspect of the GDPR is likely to become increasingly relevant in this field.

**The right to have data erased**

This principle requires personal data to be accurate. Under the DPA, a data subject may apply to the court to request that the inaccurate data which is being processed is blocked, erased, rectified or destroyed.

**Article 17 GDPR** does not provide an absolute right to be forgotten. It provides data subjects with a right to erasure without undue delay where one of the specified conditions are met. These include:

The personal data are no longer necessary in relation to the purposes for which they were collected Where the consent on which processing is based is withdrawn

The data subject objects to the processing pursuant to **Article 21(1)** and there are no overriding legitimate grounds for the processing, or the data subject objects to processing pursuant to **Article 21(2).**

**Personal data have been unlawfully processed.**

However, there are exemptions. It is likely that service providers in health and social care will be able to decline requests for erasure in many cases as processing (including retention of records) could be considered necessary For compliance with a legal obligation which requires processing by EU member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or the establishment, exercise or defence of legal claims, which includes prospective claims

**The right to a Remedy**

Under **Article 82(1)** Data Subjects have the right to compensation, the provision is as follows:

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Damages will remain available for 'distress only' claims, in line with current UK case law. In terms of liability, processors will only be liable to the extent that they have acted outside of their instructions or failed to comply with aspects of GDPR specific to the obligations of processors.

In **Data Protection Registrar V Amnesty International[101],** the defenadant were held liable for reckless holding and disclosing information about about named individduals.

The recent High Court decision in **Various Claimants v Morrisons** demonstrates the possibility that processors or controllers could be held vicariously liable for the wrongful acts of their employees. That decision is likely to be the subject of an appeal.

**In** light of the overarching obligation contained in Article 12, organisations will have to consider how they will co-ordinate their response to requests from data

[101]Data Protection Registrar V Amnesty International[101],

subjects regarding the exercise of their rights and prepare appropriate policies and procedures for handling such requests.

In the first instance it may be worth setting up designated email addresses to receive such requests where possible and raising staff awareness so that they are able to recognise a request and forward this for action as appropriate. This will be necessary as there is no specified format for such requests.

# DATA PROCESSING IN EMPLOYMENT RELATIONS

Employers always collect data from Employees before offering them jobs. However, Sometimes the way of data collection raises issues and challenges and new risks for workers thus a need on the legal framework.

The history of data collection in the Employment sector was taken by the Council of Europe Convention of 1981 and this convention was followed by a directive 94/46/EEC that required all European Union members to protect fundermental rights and freedoms of natural persons and in particular the right to privacy with respect to processing of data.

In Africa it was in 2014 when the African Union recognized the need to regulate data and introduced the Convention On Cyber Security and Personal Data Protection . Uganda is one of the few countries that have ratified to it.

In Uganda the law regarding data protection is ably discussed above.

In regards to the employment sector, **article 27 of the constitution** recognizes the right to privacy to everyone including employees.

**Section 6 of the Employment Act** does not expressly state that employers are obliged to collect data from their employees concerning their religion , political affliation, ethnicity, HIV Status , national extraction, social status but interestingly it bars employers from discriminating employees on such grounds.

**Section 16 of the Employment Act** makes it an offence for one to record or cause to be recorded wrong, inaccurate or insufficient in the employee's record. This in in line with **article 15 of the DPPA** which is against collecting information and the **QECD principle** on data quality principle and **section 17 and 18 of the Computer Misuse Act** makes it an offence to collect data from employees without their consent.

CHAPTER 11

# CYBER CRIME

## INTRODUCTION

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in the Modern world. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent.2 There are number of illegal activities which are committed over the internet by technically skilled criminals. This study investigated the adequacy of the Cyber crime legal framework in Uganda. Special attention was givén to elements of cyber crime. This chapter presents the background to the study, the statement of the problem, objectives of the study, research question, scope of the study, significance of the study, justification and operational definition of terms and concepts.

The introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s; the first unauthorized access to computer networks occurred shortly afterwards. Similarly, the first software offences appeared soon after

The process of formulating cyber laws in Uganda was initiated in 2003 when a national taskforce led by the Uganda Law Reform Commission was set up to undertake the exercise.

The formulation and development of cyber laws was part of a wider reform of the commercial justice system in Uganda that started in 2000. The process was undertaken largely to make the law responsive to the changing needs of society.

In Uganda, the advent and development of ICT came with new crimes and this provided a platform for the commission of existing crimes such as fraud, terrorism, money laundering, murder and theft. Although these crimes could be prosecuted under the Penal code Act, ICT related crimes such as hacking and theft of computer programmes or software poised a challenge to the legal system, hence the need to enhance cyber security.

While Uganda Communications Act and the Electronic Media Act have been in place since 1996, the two laws regulate the telecommunications and broadcasting subsectors without much emphasis on the cyber world. The Electronic Transactions Act, 2011, the Electronic Signatures Act, 2011 and the Computer Misuse Act, 2011 now form the backbone of the legal framework for e-commerce, electronic transactions and computer- or ICT-related communication in Uganda. The three laws became effective on 15 th April 2011. However, even with such laws in place.

Cyber crime has increased by 14.9% since 2013. The report indicates that cyber crime focuses on mobile money and Automated Teller Machines (ATM) fraud. MTN alone has transacted through its Mobile Money service a total of US$245 million. Cyber crime targeting Mobile money and ATMs accounted for a loss of over $lmillion country wide. Around $100,000 was transferred without the knowledge or authority of telecom service providers between August and November of 2012. Despite the challenges attributed to crime statistics, the figures reported above are a pointer towards the seriousness of the problem of cybercrime and the danger posed to electronic transactions. Therefore this study investigated the adequacy of the Cyber crime legal framework in Uganda.

Electronic evidence: electronic evidence originates from the drives of electronic devices or computers and may be volatile (retrievable) and non- volatile forms of electronic evidence.

Threats: threats include: cyber crime attackers committing economic crimes which affect the population. There is also a potential for the commission of political crimes with serious governance consequences. Cybercrime can cause damage to computer systems thrsough virus attacks (sabotage).

# LEGAL FRAMEWORK ON CYBER CRIME

## *The Anti-Terrorism Act, 2002*

The Anti-Terrorism Act (ATA) was adopted in 2002 and includes provisions that provide for obtaining information in respect of acts of terrorism. This includes the authorizing of the interception of the correspondence and the surveillance of persons suspected to be planning or to be involved in acts of terrorism.

**Section 9(1)** states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism or training or mobilising any group of persons or recruiting persons for carrying out terrorism or mobilising funds for the purpose of terrorism commits an offence and shall be liable on conviction, to suffer death. It is further laid down in Section 9(2) of the ATA that any person who, without establishing or running an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death.

## *The National Information Technology Authority, Uganda Act, 2009.*

This law establishes the National Information Technology Authority in Uganda (NITA-U). It is a government agency under the general supervision of the minister responsible for information technology (Section 3 (3) and Section 2). 18 The goals of the NITA-U listed in Section 4 include diverse ways to promote information technology in Uganda and most of these aims are commendable. The functions of the NITA-U listed in Section 5 are many (18) and rather broadly formulated. **Section 5 (18)** extends the functions of the authority to undertake any other activity necessary for the implementation of the objects of the authority.

## *The Regulation of Interception of Communications Act, 2010.*

The Regulations of Interception of Communications Act (RICA) is probably the most problematic law when it comes to guaranteeing the Internet freedom of Ugandan citizens. **Section 3 of RICA** provides for the establishment of a Monitoring Centre for the interception of communications under the act. The minister responsible for security is mainly responsible for establishing and running the centre.

An application for the lawful interception of any communication may be made by the Chief of Defence Forces, the Director General of the External Security Organisation, the Director General of the Internal Security Organisation, the Inspector General of Police or their nominees (Section 4 (l)), also referred to as authorized persons (Section 1). A warrant to intercept communications shall be issued by a designated judge, by which is understood a judge designated by the Chief Justice to perform the functions of a designated judge for purposes of RICA (Section l).

## *The Electronic Signatures Act, 2011.*

The Electronic Signatures Act (ESA) regulates the use of electronic signatures in Uganda. While promoting the use of electronic signatures can generally be regarded as a positive development, there are some aspects of ESA that can be seen as creating risks in relation to individuals' right to privacy and freedom of expression. ESA for example includes provisions on advanced electronic signature that are uniquely linked to signatory, reliably capable of identifying the signatory and linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable (Section 2). In case the security of these types of signatory systems is not adequate, the anonymity of a person's online behaviour can be threatened due to the possibility to identify the individual through his or her signature. The Electronic Signatures Act 201 1 provides for the use of electronic signatures and their regulation. All the three laws have been published and are now in force.

## *The Computer Misuse Act, 2011.*

The Computer Misuse Act (CMA) prescribes liability for offences related to computers. For example child pornoyaphy, cyber harassment, offensive communications, and cyber stalking are penalized under CMA. The maximum penalties for these offences range from one to five years of prison, with the exception of child pornography, which can generate the maximum prison sentence of 15 years. The conditions required for these offences to be at hand are, however, often rather vaguely defined. This both contravenes the requirement of unambiguous and foreseeable provisions in international law and can have a hampering effect on freedom of expression.

## *The Electronic Transactions Act, 2011*

The Electronic Transactions Act (ETA) provides for the use, security, facilitation and regulation of electronic communications and transactions. As regards possible threats to Internet freedom, ETA contains above all pertinent provisions

concerning the liability of Internet service providers. It is stipulated in Section 29 that a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on the making, publication, dissemination or distribution of the material or a statement made in the material or the infringement of any rights subsisting in or in relation to the material.

## *The Uganda Communications Act, 2013.*

The Uganda Communications Act (UCA) regulates the Ugandan communications services. It provides for the establishment of the Ugandan Communications Commission (UCC) (Section 4).Functions of the UCC include e.g. to monitor, inspect, licence, supervise, control and regulate communications services (b), to receive, investigate and arbitrate complaints relating to communications services and take necessary action (j) and establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators (u) and to set standards, monitor and enforce compliance relating to content (x) (Section 5).The UCC shall exercise its functions independently (Section. 8) while the Minister may, in writing, give policy guidelines to the Commission regarding the performance of its functions and it shall comply with these guidelines (Section 7).

## *The Anti-Pornography Act, 2014.*

The Anti-Pornography Act was adopted in 2014 and criminalizes all forms of pornography. According to Section 13(1), a person shall not produce, traffic in, broadcast, procure, import, export, sell or abet any form of pornography. An offence under this paragraph can result in a prison sentence of maximum ten years (Section 13 Section 14(1) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years. The realization of APA is overseen by the Pornography Control Committee established in Part Il.

# INSTITUTIONAL FRAMEWORK ON CYBER CRIME

The principal player agencies are: the Ministry of Information Communication Technology, the Uganda Communications Commission, the National Information Technology Act-Uganda (NITA-U), the Uganda Police Force; and the Judiciary. Uganda has gone further to set up a Computer Emergency Response Team (CERT) with all the aforementioned Government agencies being represented on the committee. The Uganda Communications Commission (UCC) has set up its own CERT to compliment the national team and this was set up on the 6th of June 2013. This CERT prowls the Internet to monitor and report hi-tech crime including cyber terrorism, computer intrusion, online sexual exploitation and cyber fraud. The team also coordinates all other multi sectoral agencies in this fight against cyber crime; liaises with other law enforcement agencies in the prosecution of cyber related crimes and collaborates with other regional and international agencies with similar remits.

# ELEMENTS OF CYBER CRIME IN UGANDA

The Concept of cyber crime is very different from the traditional crime. Also due to the growth of Internet Technology, this crime has gained serious and unfettered attention as compared to the traditional crime. So it is necessary to examine the peculiar characteristics of cyber crime.

Cyber crimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. The people who have committed cyber crime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cyber crime. In cyberspace the geographical boundaries reduced to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States.

In cyberspace the geographical boundaries reduced to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States. It is very difficult to collect evidence of cyber crime and prove them in court of law due to the nature of cyber crime. The criminal in cyber crime invoke jurisdiction of several countries while committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.

The cyber crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can of the most commonly occurring offences included in this category.

**Illegal access (hacking, cracking)**

The offence described as "hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Govemment. Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to entera computer system setting up "spoofing" websites to make users disclose their passwords and installing hardware and software-based keylogging methods (e.g. "keyloggers") that record every keystroke — and consequently any passwords used on the computer and/or device.

**Illegal data acquisition (data espionage)**

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a 40 different country.

**Illegal interception**

Offenders can intercept communications between users41 (such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VolP communications). Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept. However, offenders search for weak points in the system.

Wireless technologies are enjoying greater popularity and have in the past proved vulnerable. Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres. Offenders who wish to intercept a dataexchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.

**Data interference**

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can

result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data. One common example of the deletion of data is the computer vilus. Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection. Since then, the number of computer viruses has risen significantly. Not only has the number of virus attacks increased, but also the techniques and functions of viruses (payload) have changed.

**System interference**

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.

Attacks can be can•ied out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware.

**Erotic or pornographic material**

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping; worldwide access, reaching a significantly larger number of customers than retail shops; the Internet is often viewed as an anonymous medium (often erroneously); an aspect that consumers of pornography appreciate, in view of prevailing social opinions. Recent research has identified as many as 4.2 million pornographic websites

that may be available on the Internet at any time. Besides websites, pornographic material can be distributed through file-sharing systems and instant messaging systems. Different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material, seeking to protect minors.

**Illegal gambling and online games.**

Internet games and gambling are one of the fastest-growing areas in the Internet. Linden Labs, the developer of the online game Second Life, reports that some ten million accounts have been registered. Reports show that some such games have been used to commit crimes, including the exchange and presentation of child pornography, fraud, gambling in virtual online casinos and libel (e.g. leaving slanderous or libellous messages). Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling (although compared with revenues from traditional gambling, these estimates are still relatively small).

**Fraud and computer-related fraud.**

Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities. Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes. One example of such a scam is the Nigeria Advanced Fee Fraud.

Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud. The main distinction between computer related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud.

Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences. The most common fraud offences include online auction fraud and advanced fee fraud.

**Misuse of devices**

Cybercrime can be committed using only fairly basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools. The tools needed to commit complex offences are widely available over the Internet, often without charge. More sophisticated tools cost several thousand dollars. these software tools, offenders can attack other computer systems at the press of a button. Standard •attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets. Software tools are available that enable the offender to carry out DOS attacks, design computer viruses, decrypt encrypted communication or illegally access computer systems.

**Elements of cyber crime in Uganda**

Illegal access or hacking is one of the leading cyber crimes in the Uganda. Respondents indicated that this crime is rampant on social media accounts especially Facebook and emails such as yahoo and Google personal accounts.

Data interference is a cyber crime that is common in Uganda, majority of respondents said that offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data through the use of computer viruses which has affected them through the losses of data and financial losses.

Distribution of pornographic material is a very serious cyber crime occurring especially among the young youthful population of Uganda. One key informant

interviewed said "After the distribution of internet and the advance of computers and smart phones, access to pornographic material has become easy even for minors." This implies erotic material is a common cyber crime in the country.

Computer-related fraud is one of the most popular crimes on the Internet in Uganda, respondents indicated that offender to use automation and software tools to mask criminals identities and cheat un suspecting members of the public colossal sums of money through trickery activities such as promising delivery of goods after effecting payments online.

Additionally among the forms of cyber crime that were found to have a high prevalence rate within Ugandan organisations include Fraud Committed by the Consumer, Business Misconduct, Asset Misappropriation, Cybercrime and Bribery and Corruption. Business Conduct/Misconduct refers to frauds or deception by companies upon the market or general public. It involves deceptive practices associated with the manufacturing, sales, marketing or delivery of a company's products or services to its clients, consumers or the general public. It is the second most prevalent form of economic crime in Uganda. Whereas Cybercrime has only the third highest incidence rate in Uganda at 31% (tying with Asset Misappropriation), it continues to be one of the biggest potential threats to organizations in the future. At 30%, Cybercrime scored the highest among Uganda's respondents as the form of economic crime likely to be most disruptive to their organizations in the next 24 months, both monetarily and otherwise.

# WEAKNESS OF UGANDA'S CYBER LAW IN CURBING CYBER CRIME

Uganda has a number of legislations in place, which address Internet misuse (the Computer Misuse Act, the Electronic Signatures Act, The Electronic Transactions Act, Electronic Misuse Act, the Access to Information Act, and the Regulation of Interception of Communications Act). Different stakeholders were involved in drafting these legislations for example the Ministry of Information and Communications Technology (MolCT) in conjunction with Ministry of

Justice and Constitutional Affairs (MoJCA), Uganda Communications Commission and National Information Technology Authority (NITA-U) of Uganda jointly coordinated the drafting of the Data Protection and Privacy Bill"

Some of these prosecution cases have been based on the Computer Misuse Act, the Electronic Signature Act, and the Electronic Misuse Act, and applied as cyber Laws.

Cyber criminals in Uganda take advantage of weaknesses in cybercrime legislation and the nascent systems of law enforcement leading to a proliferation of illicit activities. On this respondents noted that mainly cross- border prosecutions of Cybercrime are still a challenge for law enforcement agencies major limitation. This therefore implies gaps in the laws on cyber crime in Uganda.

**Section 5 (3) of the National Information Technology Authority, Uganda Act, 2009**, mandates NITA-Uganda to co-ordinate, supewise and monitor the utilization of information technology in the public and private sectors, however this provision can be interpreted to threaten privacy and freedom of expression by allowing supervising and monitoring, the scope of which is not clearly and unambiguously defined. Moreover, it is unclear if by "utilization" of information technology is understood access to Internet on a more general level or a more content-specific use of the Internet. The latter interpretation would open up considerable powers to supervise and monitor e.g. individuals' Internet traffic.

**Section 5 (4) of the National Information Technology Authority, Uganda Act, 2009**, mandates NITA-Uganda to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals, however this provision opens up for the NITAU to stipulate standards for hardware and software in public computers that can restrict freedom of expression and privacy. It could for example be interpreted to allow for regulations requiring installation of filters, blocking mechanisms or spyware in public computers. The judicial officer added that Section 22 of the National Information Technology Authority,

Uganda Act, 2009 stipulates that confidentiality is the main rule as regards for example data set or part of data stored in a computer or any other electronic media. However, this does not affect the fact that the NITA-U as a public authority has a possibility to get access to personal data concerning individuals.

The Electronic Transactions Act provides for the use, security, facilitation and regulation of electronic communications and transactions as a functional equivalent to the already existing forms of communication. The Act gives legal certainty in respect of validity, legal effect and enforceability of information in electronic form with respect to relations between parties especially establishing contractual obligations. In 2007, prior to the enactment of this Act, the High Court in Hansa, Emmanuel Onyango vs Aya Investments Ltd, Mohammed Hamid relied on the exchange of emails between the parties to determine the contractual relations.

In regard to procuring surveillance equipment and criminalizing gadgets (computers) as well as Internet content. Their powers range from illegally ordering Internet service providers to block certain social platforms to signing secret memorandum of understanding among government agencies to share information about Internet users and published content in order to enforce the Ugandan cyber legislation. Harassment of online activists by police has also been reported.

There is no statutory framework governing the transactions. The mobile network operators have no obligations to report or disclose info on mobile money services to Bank of Uganda (BOU) as a regulator. All these are gaps that are clearly visible in the Ugandan legal framework on cyber crime.

There is a general lack of capacity among the police and other law enforcement agencies to detect ,investigate and assist in prosecution under the Computer Misuse Act 2011. This has been a challenge in the prosecution of some high profile cases in the country like **Uganda Vs Kato Kajubi and Uganda Vs Dr. Aggrey Kiyingi cases** that relied on electronic evidence. In Kato Kajubi following a retrial, the accused was convicted. Following the terrorist attack on

Kampala on 1Ith July 2010, the police with the help of the FBI were able to uncover emails linking the bombings to the suspects.

There is lack of capacity and funding to enable special skills training required to counter the ever evolving and increasing cyber crime nationally and globally. Uganda does not have adequate data protection laws. Across the East African sub region and the African continent, there is a lack of a harmonized legislative regime to tackle cybercrime. Finally, there is insufficient knowledge about the law and inadequate sensitization of the public and other potential victims of cybercrime.

Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

On enforcement and implementation of laws, there is no centralized budget for cyber security. Every Ministry allocates its budget separately and depends on previous experience and future plans to allocate budget for cyber security. In agreement, an advocate interviewed said

There is limited capacity by the law enforcement agencies to investigate computer-related crimes, in-line with known global best practices. This has been attributed largely due to lack of sufficient technical expertise in digital forensic in Cybercrime cases."

A key informant said that the National Information Security Strategy (NISS) does not provide specific actionable directives that relate to cyber security. He added "Risks may exist but the strategies are not aligned with national goals; at the moment evay Agency has their own list of incidents and have different priorities. Different institutions place different levels of importance to technology, depending on their priorities."

Uganda does not have an official list of Critical National Infrastructure (CNI) sectors in Uganda. This is mainly attributed to the lack of clear understanding of what constitutes a CNI sector list and the difficulty in recognizing what needs to be protected. Experts believe they generally have the ability to recognize what is important for Uganda and will take the appropriate & necessary measures to protect Uganda's CNI. Thé National Information Security (NIS) Policy defines the concept of critical information infrastructure (Cll), but does not clear address the CNI issue in detail. According to the National Information Security policy"theinformation and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services". This is an areas that needs to be developed further.

Overall, cyber security capacity in Uganda lies between an initial and formative stage of maturity. This expresses a state of maturity where some features have begun to grow and be formulated, but may be ad-hoc, while these can be clearly evidenced.

# SOLUTIONS TO THE PROBLEMS

The debate about necessary measures should include the whole range of instruments such as awareness raising, making available and promoting free of charge protection technology (such as anti-virus software) and the implementation of solutions that enable parents to restrict the access to certain content. Such measures should ideally be available at the time of an introduction of a service/technology and maintained through out it's operation.

To ensure a wider reach of such measure a broad range of stakeholders should be involved that range from Internet Service Provider to governments and regional bodies and explore various sources for funding.

It there is need for Uganda to have a National Cyber security Strategy in order to identify and include other national risks and priorities areas of Cyber security. For example, the current rick register needs to be enhanced so that it can include

all critical sectors in Uganda. It was suggested that NITA-U could coordinate the update, review and collation of all sectors registered in the country. There are general risks, which can be listed as internal and external at national level and their respective impacts needs to be considered.

In regard to Substantive and Procedural law the parliament of Uganda should amend the Evidence Act to expressly provide for the admissibility of electronic evidence; amend the Computer Misuse Act to impose an obligation on citizens/persons to report any incidents of cyber crime; amend **Section 9 Computer Misuse Act** on preservation orders, to fit within the confines of the relevant provisions in the Budapest Convention. The section should be broadened to cover content data as data that may be subject to preservation orders.

# CYBERCRIME AND CYBERSECURITY

Areas that are related to cyber law include cybercrime and cybersecurity. With the right cybersecurity, businesses and people can protect themselves from cybercrime. Cybersecurity looks to address weaknesses in computers and networks. The International Cybersecurity Standard is known as ISO 27001.179

Cybersecurity policy is focused on providing guidance to anyone that might be vulnerable to cybercrime. This includes businesses, individuals, and even the government. Many countries are looking for ways to promote cybersecurity and prevent cybercrime. For instance, the Indian government passed the Information Technology Act in 2000. The main goal of this law is to improve transmission of data over the internet while keeping it safe.

Information is another important way to improve cybersecurity. Businesses, for example, can improve cybersecurity by implementing the following practices:

- Offering training programs to employees.
- Hiring employees who are certified in cybersecurity.
- Being aware of new security threats.

- Cybercrimes can be committed against governments, property, and people.

**What is computer Misuse and Crime?**

**Section 2 of the Computer Misuse Act (CMA)** defines key terms and as such "computer" means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices;

Cybercrime is unlawful act wherein the computer is either a tool or a target or both Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subjects to the Indian Penal Code. The abuse of computers has also given birth to a range of modern crimes that are addressed by the Computer Misuse Act, 2011.

## *Scale and nature of computer crime*

Computerization significantly eases the performance of many tasks. For example, the speed and ability to communicate with people is fostered by the Internet, a worldwide network that is used to send communiqués and provide access to the world-wide web. But this same speed and ability to communicate also opens the door to criminal conduct. Computer crime plays a significant role in the criminal law of the information age. Accompanying the influx of computers is an increase in criminal acts and, as a result, an increase in the number of statutes to punish those who abuse and misuse this technology.

Computer crime, sometimes known as cyber-crime, is a serious concern. The crime can be perpetrated instantaneously and its effects can spread with incredible quickness. Furthermore, the ever-increasing use of computers, especially in serving critical infrastructure, makes computer criminality increasingly important.

There is an endless list of possible crimes that can occur through use of the Internet. For example, the Internet can be a medium used for committing hate crimes, pornography, consumer fraud, stalking, terrorism, theft of security or trade secrets, software piracy, economic espionage, and financial institution fraud. The threat of computer crime is underlined by the fact that a security organization such as the Federal Bureau of Investigation was forced to temporarily take down its Internet site in 1991 after an attack by hackers. Companies have been equally vulnerable and have incurred millions of dollars in damage due to the effect of certain viruses.

Misuse of the computer threatens individual and business privacy, public safety, and national security. There have been considerable efforts made by state, federal, and international governments to curb computer crime.

## *Categories of Cyber Crime*

A precise definition of computer crime is problematic. This is because of the array of different forms and forums in which the crime may appear. A single category cannot accommodate the wide divergence of conduct, perpetrators, victims, and motives found in examining computer crimes. Adding to this confusion is the fact that computer crimes also can vary depending upon the jurisdiction criminalizing the conduct. The criminal conduct can be the subject of punishment under a state statute. There is also an odd mixture of federal offenses that can be used to prosecute computer crimes. But computer crimes are not just domestic. Because computers operate internationally, the definition of computer crime can be influenced by the law of other countries as well. Despite debate among leading experts, there is no internationally recognized definition of computer crime.

At the core of the definition of computer crime is activity specifically related to computer technologies. Thus, stealing a computer or throwing a computer at another person would not fall within the scope of the definition of computer crime in that these activities do not use the technology as the means or object of the criminal act. Computers serve in several different roles related to criminal

activity. The three generally accepted categories speak in terms of computers as communication tools, as targets, and as storage devices.

The computer as a communication tool presents the computer as the object used to commit the crime. This category includes traditional offenses such as fraud committed through the use of a computer. For example, the purchase of counterfeit artwork at an auction held on the Internet uses the computer as the tool for committing the crime. While the activity could easily occur offline at an auction house, the fact that a computer is used for the purchase of this artwork may cause a delay in the detection of it being a fraud. The use of the Internet may also make it difficult to find the perpetrator of the crime.

A computer can also be the target of criminal activity, as seen when hackers obtain unauthorized access to Department of Defense sites. Theft of information stored on a computer also falls within this category. The unauthorized procuring of trade secrets for economic gain from a computer system places the computer in the role of being a target of the criminal activity.

A computer can also be tangential to crime when, for example, it is used as a storage place for criminal records. For example, a business engaged in illegal activity may be using a computer to store its records. The seizure of computer hard drives by law enforcement demonstrates the importance of this function to the evidence gathering process.

In some instances, computers serve in a dual capacity, as both the tool and target of criminal conduct. For example, a computer is the object or tool of the criminal conduct when an individual uses it to insert a computer virus into the Internet. In this same scenario, computers also serve in the role of targets in that the computer virus may be intended to cripple the computers of businesses throughout the world.

The role of the computer in the crime can also vary depending upon the motive of the individual using the computer. For example, a juvenile hacker may be attempting to obtain access to a secured facility for the purpose of demonstrating computer skills. On the other hand, a terrorist may seek access to this same site

for the purpose of compromising material at this location. Other individuals may be infiltrating the site for the economic purpose of stealing a trade secret. Finally, unauthorized computer access may be a display of revenge by a terminated or disgruntled employee.

In addition to computer crimes having several roles, the individuals who commit the crimes do not fit one description. The only common characteristic of the individuals committing these crimes is their association with a computer. The perpetrator of a computer crime could easily be a juvenile hacker, sophisticated business person, or terrorist. Likewise, the victims of computer crimes do not fit a specific category in that the spectrum of possible victims includes individuals, financial institutions, government agencies, corporations, and foreign governments.

Cyber crimes often fit within traditional criminal law categories in that computers can be used to commit crimes such as theft, fraud, copyright infringement, espionage, pornography, or terrorism. In some instances, existing criminal categories adapt new terminology to reflect the computer nature of the crime. For example, cyber terrorism is used when the terrorist activity involves computers, and cyber laundering relates to money laundering via computer. Trespass crimes take on a new dimension when the unauthorized access occurs in cyberspace. For example, in 2000, the website for the American Israel Public Affairs Committee was defaced by intruders who downloaded e-mail addresses and credit card numbers from the site.

Criminal conduct that may appear to have no connection with computers can, in fact, be affected by technology. For example, stalking presents itself as a serious concern growing from increased use of the Internet. Cyber stalking generally involves the stalking of a person via the Internet or other electronic communication. Access to personal information on the Internet makes cyber stalking particularly problematic. Recognizing the need to consider the effect of technology on crimes such as stalking, the Attorney General issued the "1999 Report on Cyber stalking: A New Challenge for Law Enforcement and Industry" that describes the efforts that law enforcement can take to deter this criminal

activity. First Amendment concerns factor into whether these and other legal initiatives regarding computer crimes will withstand constitutional challenges.

Computer crimes do not always correlate with traditional descriptions of illegality. Some activities present unique forms of criminal conduct that bear no resemblance to common law or existing crimes. For example, computerization allows for new types of crimes, such as trafficking in passwords.

Other computer crimes may have a resemblance to traditional crimes but the conduct may not fit neatly into an existing category. For example, a "page-jacker" who misappropriates material from another individual's website may face criminal liability for a copyright violation. If the "page- jacker," however, manipulates a website to redirect individuals to his or her own website, it remains uncertain whether this fraudulent conduct fits within classic theft or fraud offenses. Specific computer crime statutes are tailored to meet these new forms of criminal conduct. The ability the Internet provides in accessing information with a degree of anonymity makes some crimes, such as identity theft, important priorities for the criminal justice system.

The technical and changing nature of computer technology can make it difficult for those who are drafting criminal statutes. The array of new terms and new meanings given to existing terms requires a certain level of expertise in order to understand the computer activity. Examples of simple words used in the context of computer activity are the terms "virus" and "worm." A federal court explained, "A 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.'" This differs from a computer "virus," which does attach to the computer operating system that it enters (United States v. Morris, 928 F.2d 504, 505n.1 (2d Cir. 1991)) Generally, there are three major categories of cybercrimes that you need to know about.

## *The categories of crime*

**Crimes Against People**. While these crimes occur online, they affect the lives of actual people. Some of these crimes include transmission of child-pornography, cyber harassment, cyber stalking, cyber bullying, cyber defamation, revenge porn, email spoofing, cracking, carding, sms spoofing, pornography, credit card frauds, online libel / slander, cyber smearing, trafficking, financial frauds, identity theft, etc.200

**Crimes Against Property**. Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, IPR violations. cyber trespass and transmitting viruses.

**Crimes Against Government**. When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

## *State of Cyber Crime in Uganda*

Cybercrime is largely regulated by the 2011 Computer Misuse Act. The act comes after the first known case of a person (a blogger in 2010) reportedly being charged for offences relating to free expression on the internet.

The Computer Misuse Act makes provisions for the safety and security of electronic transactions and information systems. The act creates several computer misuse offences, for example, unauthorized modification of computer material, unauthorised access, access with intent to commit or facilitate commission of further offence. It also outlines mechanisms for investigation and prosecution of the offences, as well as appropriate sentences for each offence.

## *Encryption*

There does not appear to be any restriction on the use of encryption in Uganda. The use of end-to- end encrypted messaging applications, particularly WhatsApp, is popular.

## *Licensing of Industry*

Uganda's telecommunications industry is governed by the Uganda Communications Commission (UCC). The Commission's mandate is to develop "a modern communications sub-sector and Infrastucture in Uganda, in conformity with the operationalization of the Telecommunications Policy."

The National Information Technology Authority is an autonomous statutory body established under the NITA-U Act (2009), to coordinate and regulate Information Technology services in Uganda. It is supervised by the the Ministry of Information and Communication Technology (MoICT).

Uganda's main mobile network providers are a mixed group of Ugandan, African, and international providers. These include:

- MTN Uganda (a subsidiary of South African company MTN);
- Airtel Uganda (a subsidiary of Indian company Bharti Airtel);
- Uganda Telecom (partially government-owned and partially owned by a subsidiary of the Libya Africa Investment Portfolio);
- Africell Uganda (formerly Orange, Africell is an African company founded in The Gambia);
- Smile Telecom (an African provider incorporated in Mauritius);
- Sure Telecom (a subsidiary of Time turns Holding Ltd, Cyprus);
- K2 Telecom (a private Ugandan company);
- Smart Telecom (owned by the Industrial Promotion Services (IPS) Kenya, which is part of the Aga Khan Fund for Economic Development); and

- Vodafone Uganda (a subsidiary of the British Vodafone group).

## *Different Cyber Crimes*

**Hacking – Unauthorized Access to Computer Material**

**Section 12 (1) of the Computer Misuse Act provides that a** person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence. Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another person's website called as web hijacking.201

**Unauthorized Modification of Computer Programs or Data**

**Section 14** of the requisite intent and the requisite knowledge at the time when he or she does the act,

This is an offence whereby a person knowingly and without authority does an act which causes the contents of a computer to be changed, erased, added to or impairs the normal operations of the computer. It also includes the introduction of viruses etc., where these result in the modification or destruction of data.

This type of offence usually refers to the hacking into of computer server systems vandalising it or leaving malicious computer viruses.

## *Piracy and Related Offences*

The internet and online peer-to-peer sharing software has made piracy more popular than ever. Whether you're being accused of illegally downloading a song or movie or using an unlicensed copy of Photoshop, a piracy charge is nothing to make light of. In fact, piracy is a federal crime. These felony charges can land you in prison for a year or longer, depending upon the circumstances of your individual case. Although at first glance, piracy might seem like a victimless crime, it's still considered theft. When you're downloading music without paying for it, it's illegal. If you're facing any type of piracy charges or related charges, you top priority needs to be speaking with a criminal defense attorney about your case.[202]

## *Elements of a Piracy Charge*

Piracy is essentially illegally stealing or sharing files that you haven't paid for. In the parlance of our times, we think of piracy as involving music and video files online. When it comes to piracy charges and convictions, two separate elements have to be satisfied. First, the prosecutor must prove that piracy (the theft) was willful and intentional. Did you intend to illegally steal the music? Second, did you, yourself, personally download or share the files? If you have a computer that more than one person uses, it might be difficult to prove that you were actually the one that committed the piracy.

## *Piracy and Cyber Crimes*

Piracy is one of the most common types of cyber crimes. Cyber crimes can include just about any crime or criminal activity that takes place online. This type of cyber crime deals with theft of certain types of intellectual property. Illegally downloading music is probably the most popular form of piracy and cyber crime. Illegal file sharing can also occur with games, movies, television

shows and a variety of different types of software. Any time a file is shared or downloaded illegally online, that's piracy and a cyber crime.

**Downloading Music**

In its heyday, illegal downloading and sharing of music was out of control. Initially, Napster was the preferred file sharing, peer-to-peer software of choice. A variety of other peer-to-peer file sharing websites and pieces of software followed. As soon as one was shut down, another one popped up. Limewire, and other programs filled the space that Napster left behind. If you or somebody you love has been accused of illegally downloading or sharing music, you need to speak with an skilled criminal defense attorney with cyber crimes case experience immediately.[205]

**Digitally Bootlegging Movies**

Digitally bootlegging movies is also a huge crime associated with piracy. The Motion Picture Association of America (MPAA) estimates a loss of nearly $3.5 billion each year due to digital piracy. This multi-billion dollar criminal enterprise can also land you in hot legal water. It might seem innocent enough, but illegally downloading or bootlegging a movie online can mean serious trouble if charged or convicted.[206]

## *Piracy, a Crime*

Piracy is a federal crime. This means that you can go to prison for more than a year, if convicted. It also means you could be facing hefty financial fines. If you're facing any kind of felony charges related to piracy or other cyber crimes, you need to speak with an experienced criminal defense attorney immediately about your case. It might feel like a seemingly victimless crime to you, but the federal government takes these charges and investigations very seriously.[207]

In Uganda, section 14 (6); A person who commits an offence under this section is liable on conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

**Penalties Associated With Piracy.**

They might seem draconian in nature, but penalties associated with digital piracy of copyrighted works can get you hard time in a federal prison facility. In fact, if you're convicted of video taping a move, you can get sentenced to three to six years in a federal correctional facility. Additionally, people who use peer-to-peer networks in violation of the No Electronic Theft (NET) Act of 1997 can also face harsh penalties if convicted. It's possible to get a five to 10 year sentence if you're found guilty of illegally trafficking recordings of lie events or performances for financial gain.[208]

**Computer Pornography**

The Internet has given rise to a new industry for the online publication and consumption of obscene materials. Millions of people around the world are visiting web-sites catering to this product. These Internet sites represent the largest growth sector of the digital economy.

An obscene publication is generally understood to be any publication whose dominant characteristic is the undue exploitation of sex, or of sex together with crime, horror, cruelty or violence. Whether a publication's dominant theme is the undue exploitation of sex is determined by reference to a "community standards" test. Obscene article contains an image or a description of sexual behaviour which is, arguably, an exceptional practice or a minority taste, or something which is beyond the pale and carry the risk that viewers of the material may be encouraged or corrupted into such practices.

A work is indecent if it, taken as a whole, appeals to the prurient interest in nudity, sex, or excretion; depicts, represents or describes in patently offensive ways, ultimate sexual acts, normal or perverted, actual or simulated sadomasochistic acts or abuse; or lewd exhibition of the genitals, pubic area, buttocks, or post-pubertal female breasts .

Obscenity is calculated to promote the violation of the law and the general corruption of morals. The exhibition of an obscene picture is an indictable

offence in law, if it be averred that the picture was exhibited to sundry persons for money.

However, for something to be obscene it must be shown that the average person, applying contemporary community standards and viewing the material as a whole, would find:

i. that the work appeals predominantly to prurient interest;

ii. that it depicts sexual conduct in a patently offensive way; and

iii. That it lacks serious literary, artistic, political or scientific value.

An appeal to prurient interest is an appeal to a morbid, degrading and unhealthy interest in sex, as distinguished from a mere candid interest in sex. The first test to be applied, therefore, in determining whether the given material si obscene, is whether the predominant theme or purpose of the material, when viewed as a whole and not part by part, and when considered in relation to the intended and probable recipients, is an appeal to the prurient interest of the average person of the community as a whole, or the prurient interest of members of a deviant sexual group, as the case might be.

The predominant theme or purpose of the material, when viewed as a whole, means the main or principal thrust of the material when assessed in its entirety and on the basis of its total effect, and not on the basis of incidental themes or isolated passages or sequences.

**Pornography as a Crime in Uganda**

Pornography is provided for by the Anti-Pornography Act, 2014 which creates the offence of pornography, prohibits pornography and establishes the Pornography Control Committee and prescribes its functions.

**Section 13** prohibits pornography

(1) A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography.

(2) A person who produces or participates in the production of, or traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography contrary to subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding ten years or both.

The literal mining of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc."

This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Adult entertainment is largest industry on internet. There are more than 420 million individual pornographic web pages today.

Research shows that 50% of the web-sites containing potentially illegal contents relating to child abuse were 'Pay-Per-View'. This indicates that abusive images of children over Internet have been highly commercialized.

Pornography delivered over mobile phones is now a burgeoning business, "driven by the increase in sophisticated services that deliver video clips and streaming video, in addition to text and images."

**Child Pornography**

Child Pornography is provided for by section **23 of the CMA, 2011** and the **Anti Pornography Act, 2014, section 14.**

**Section 23 of the CMA, 2011 provides that**:

**(1) A person who**

(a) produces child pornography for the purposes of its distribution through a computer;

(b) offers or makes available child pornography through a computer;

(c) distributes or transmits child pornography through a computer;

(d) procures child pornography through a computer for himself or herself or another person; or

(e) unlawfully possesses child pornography on a computer, commits an offence.

(2) A person who makes available pornographic materials to a child commits an offence.

**(3) For the purposes of this section "child pornography" includes pornographic material that depicts**

(a) a child engaged in sexually suggestive or explicit conduct;

(b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or

(c) realistic images representing children engaged in sexually suggestive or explicit conduct.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

A child under **section 2 of the Computer Misuse Acts, 2011** refers to a person under the age of eighteen years; **Section 14 of the Anti Pornography Act, 2014** provides that:

(1) A person who produces, participates in the production of, traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography depicting images of children, commits an offence and is

liable on conviction to a fine not exceeding seven hundred and fifty currency points or imprisonment not exceeding fifteen years or both.

(2) For the avoidance of doubt, the definition of pornography in section 2 applies in determining the commission of the offence of child pornography.

Child pornography has typically been one of those subjects that are difficult to quantify or determine. Especially, with our ever changing and evolving digital age, understanding what can and cannot get you in legal hot water is critical. Child pornography is just about any image or depiction of a minor in a sexual explicit way. This includes computer-generated images, photos, videos and cell phone pictures. In the digital age, we're seeing more and more child pornography charges involving computers and the internet. Downloading child pornography is illegal.[209]

**Paedophiles**

Also there are persons who intentionally prey upon children. Especially with a teen they will let the teen know that fully understand the feelings towards adult and in particular teen parents.

They earn teens trust and gradually seduce them into sexual or indecent acts.

Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.

Pedophilia is a sexual attraction to pre-pubescent children, relatively stable and defined. It is not the same as an attraction to teenagers, known as hephebophilia. A pedophile is not necessarily a hephebophile too, just as a hephebophile is not necessarily a pedophile too.

The vast majority of pedophiles are male, but the amount of female pedophiles is still much harder to evaluate given that their deviancy can find outlets that are far more discrete. Pedophiles can be found in all social classes and stratas.

Some are only attracted to boys (boy-lovers), others only to girls, others to both with or without some degree of preference for one. Some pedophiles have specific preferences for children of a certain age span, or possessing particular physical traits (hair, face, constitution, voice, etc), while others are less specific if at all.

There are exclusive pedophiles (only attracted to children), preferential pedophiles (who prefer children but are also attracted to adults or teenagers) and non preferential pedophiles (who prefer adults or teenagers but are also attracted to children).

# THE LOOPHOLES IN OBSCENE PUBLICATIONS

Very little information is available about the Internet porn industry. Many online pornographers operate under an ineffective regulatory regime that permits virtual anonymity. Accordingly, it is difficult to ascertain the extent and popularity of the Internet porn business. What is known is that pornography is comprised of legal as well as illegal elements. Many national governments are focused on preventing the production, distribution and consumption of pornographic materials involving children. State resources are being committed to the Herculean task of monitoring and surfing the Internet for child porn. Government efforts to combat child pornography involve interaction with various aspects of the adult Internet porn sector, much of which is legal in several states.

The anonymous and paperless nature of the internet serves as an incentive for the electronic transmission and purchase of pornographic goods and services. Government authorities encounter difficulties because the whole process of marketing, distribution, payment and delivery of obscenities can be completed electronically without the need for physical delivery or legal identification of either the consumer or the e-commerce vendor. The intangible nature of internet porn eliminates the paper trail that is a fundamental component of criminal investigations and international tax audit and verification practices.

The popularity of the unregulated Internet is now causing difficulties. Porn sites are notorious for their annoying pop-up and pop-under advertising windows. Huge amounts of unsolicited e-mail are widely sent with much of it attributable to adult web sites. The proliferation of offensive materials is deterring the use of the internet as an educational tool for youth. Recent studies indicate that children continue to be regularly exposed to lawful, sexually explicit materials on the internet. Internet pornography detracts from the social and economic benefits of e-commerce, and national governments are being driven to regulate the internet to control these harmful practices.

Many governments around the world have been slow in extending the application of their criminal laws to address the proliferation of illegal porn and obscene materials on the internet. Enforcement difficulties abound because internet markets are global while criminal laws differ from country to country. Nonetheless, national governments and international police have increased the amount of economic resources dedicated to the monitoring of the Internet and the enforcement of child pornography laws.

Due to the lure of huge profits and the lack of effective criminal sanctions, pornographers are expending economic resources to promote the production and consumption of Internet porn. The inequity of this economic shift of resources becomes more pronounced when consumers forego purchasing from local outlets in favour of shopping online to avoid paying sales and other transaction taxes. National governments should take immediate steps to remove the tax loopholes exploited by porn vendors and consumers.

## *The suggested solution to obscene publications*

If the illegal and harmful content on the Internet needs to be regulated then the question is: how should this be achieved? Despite the popular perception, the Internet is not a lawless place. The Internet is a complex, anarchic, and multi-national environment where old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily applicable or enforceable. This is why a wider concept of governance may be more suitable.

There appears to be no single solution to the regulation of illegal and harmful content on the internet because the exact definition of offences related to obscene publications and what is considered harmful varies from one country to another. What is obscene in one country may be highly protected speech in another. A recent European Commission Communication Paper stated that each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. A multi-layered governance system should be a mixture of national and international legislation, and self-imposed regulation by the ISPs and on-line users. This should include codes of conduct by the ISPs, software filters to be used by parents, advice to parents and school teachers, hotlines and special organizations to report illegal content on the internet. But the base of the pyramid must be the universal legal framework that needs to criminalize the publication, distribution and selling of obscene materials over the internet and to prosecute them accordingly. Needless to say, without full international cooperation, the implementation of the above recommendation on a global level would be totally ineffective.

# CYBER HARASSMENT

Cyber harassment refers to any intentional, substantial and unreasonable intrusion into the private life of a person that causes the person to suffer mental distress.[210] Generally it is the use of Information and Communications Technology (ICT) to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm. Unlike physical harassment involving face-to-face contact, cyber harassment requires the use of ICT and is verbal, sexual, emotional or social abuse of a person, group or organization. The cyber harasser's primary goal is to exert power and control over the targeted victim(s).

**Section 24 of the Computer Misuse Act, 2011** provides that:

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

According to the same section, Cyber harassment arises under the following circumstances. Use of the computer for the following purposes

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.

# CYBER STALKING

Cyberstalking: Cyberstalking is the use of Information and Communications Technology (ICT) to stalk, control, manipulate or habitually threaten a child, adult, business or group. Cyberstalking is both an online assailant tactic and typology of psychopathological ICT user. Cyberstalking includes direct or implied threats of physical harm, habitual surveillance and gathering information to manipulate and control a target. Cyberstalking requires a direct or implied threat of physical harm by the assailant.[212]

It is the use of images, signs, language, or other similar means for the willful purpose of systematically threatening, harassing, intimidating, tormenting or embarrassing directly or indirectly another person, either through electronic devices or by e -mail or over the Internet.[213]

**Section 26 of the Computer Misuse Act, 2011** provides that: Any person who wilfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine

not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

With the popularity of the Web increasing each day, the act of stalking has now moved into the virtual realm of the Internet, and has come to be known as cyber –stalking. Today, cyber -stalking is easier than ever, considering the anonymity provided by electronic communication. On the Web, it is not difficult to conceal one's identity or to provide incorrect personal information. Websites, e -mail, chat rooms, and discussion forums provide stalkers with a variety of opportunities to harass others. They also offer stalkers access to the private information of their victims.[214]

Cyber-stalking can be divided into direct and indirect aspects.

Direct cyber-stalking include: threats, bullying, or intimidating messages sent directly to the victim via e -mail or other Internet communications mediums, and/or the use of technological means to interfere with a victim's use of the Internet, such as hacking or denial of services attacks.

Indirect cyber-stalking includes, but is not limited to, spreading rumours about the victim in various Internet discussion forums, subscribing the victim to unwanted online services, posting information about the victim in online dating or sex services, or sending messages to others in the victim's name.

## *The Existing Texts on Cyber Stalking*

Though stalking has existed for centuries, the legal system has only codified its presence in the statutes in recent decades. As a result, cyber- stalking could truly be identified as a crime of the 21st century owing to its reliance on computer and communications technology.

In legal terms, the manifestation of this misconduct is most likely to be charged as per the statutes in place in the respective jurisdictions. The incrimination of cyber-stalking varies greatly from misdemeanour to serious crime. The penalties

also are very different, starting from fines, peace bonds, restraining orders, protection orders up to 10 years imprisonment.

A number of countries have undertaken measures including; USA, Canada, Switzerland, New Zealand, Australia.

## *The Loopholes in Cyber Stalking*

There is a definite gap between the legal statutes and the actual situation in the electronic world. Investigating and prosecuting cyber-stalking presents unique challenges. Establishing a pattern of harassment is critical to an investigation as well as to identifying the stalker's true identity, which may be unknown to the victim due to the anonymous nature of the Internet. Victims must maintain copies of all online correspondence from the stalker, such as e¬mails, chat room conversations, and websites, as evidence which law enforcement agencies can investigate. Victims should notify law enforcement agencies when online communications become threatening or cyber-stalkers approach their targets in the real world.

When identifying cyber-stalking in the field, particularly when considering whether to report it to any kind of legal authority, the following features or combinations of features can be considered to characterize a true stalking situation:

The manifest desire and intention to terrorize and hurt somebody, Much cyber-stalking is malicious in nature due to the presence and communication of clear and direct threats. Not all cyber-stalking however is malicious. In cases of love-oriented obsessive cyber-stalking for example, the stalker has no visible intent to harm, and while their behaviour may cause great distress, they do not necessarily realize that this is happening. Other forms of online harassment are also not necessarily malicious. Some online harassment takes the forms of practical jokes, and while this may be unpleasant and cause great inconvenience, annoyance, fear or distress, the harasser may not have intended to cause harm.

Not all harassment is premeditated either. Sometimes it may be the result of a sudden emotional outburst, where someone loses his temper and lashes out electronically. This may indeed cause distress but could not be called premeditated, since the attack was sudden and not planned.

Repetition is a key feature of online stalking. A one-off attack online, while it may cause distress, could not be described as cyber-stalking. Cyber-stalking is a course of conduct that takes place over a period of time and involves repeated attempts to causing distress. Some laws even define it as involving two or more incidents and following a repetitive pattern.

One could not claim cyber-stalking or even online harassment if distress is not felt in some way. Distress can take many forms, from annoyance, offense, inconvenience and humiliation, to worry and fear for safety. The presence of fear is an important characteristic of cyber-stalking.

One also needs to be careful that is not over-reacting. In legal terms, stalking is usually defined as a course of conduct that causes a reasonable person to be in distress. Proving distress as a result of online stalking might be difficult. It needs the testimony of expert witnesses, or proof that the victim went to a doctor for help or medication concerning the incident.

The anonymity of electronic communications could also pose a difficulty. Though a victim may know the identity of his or her aggressor, the prosecutors have few chances to prove a connection between the sender and the accused. It is important that more expertise is acquired about (local and virtual) stalking, and that special units are established to deal effectively with these offences. Most police and juridical institutions still have insufficient experience to recognize the serious nature of cyber-stalking and to investigate these crimes.

The disparity in the activity level among law enforcement agencies can be attributed to a number of factors.[2] First, it appears that the majority of cyber-stalking victims do not report the conduct to law enforcement, either because they feel that the conduct has not reached the point of being a criminal offense, or that law enforcement will not take them seriously. Second, most law

enforcement agencies have not had the training to recognize the serious nature of cyber-stalking and to investigate such offenses. Unfortunately, some victims have reported that rather than open an investigation, a law enforcement agency has advised them to come back if the cyber-stalkers confront or threaten them off-line. In several instances, victims have been told by law enforcement simply to turn off their computers.

## *The Suggested Solution*

Jurisdictions around the world are now only starting to recognize cyber- stalking as a criminal offense. The fear of victims of cyber-stalking is just as real as with any other crime. It is therefore important to develop a comprehensive and effective plan for dealing with cyber-stalking. Only when this is done will the Internet be a safer place for web users. Until the law on cyber-stalking has been fully developed, victims should educate themselves on the methods of effectively handling on-line harassment.

Self-protection, while essential, is not sufficient to make cyber-space a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber-crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether these are sufficient to combat the cyber crimes.

Effective law enforcement is complicated by the transnational nature of cyber-space. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber- criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber-crimes like cyber- stalking.

A future international law statute should criminalize the use of images, signs, language for the willful purpose of systematically threatening, harassing, intimidating, tormenting or embarrassing, directly or indirectly, another person through electronic devices, e-mail or over the Internet. Upon conviction, cyber-stalking should then be punished with fines and imprisonment.

**Example of a case on Cyber Stalking: Cyber Stalking Case Conviction | State Vs Yogesh Prabhu**

# OFFENSIVE COMMUNICATION

**Section 25 of the Computer Misuse Act, 201**1 provides "any person who willfully and repeatedly uses communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both".

The word 'willful' according to Webster's Universal English Dictionary means stubborn; or done intentionally. The word repeatedly means 'many times, over and over again. Thus a person who stubbornly and intentionally uses communication over and over again is said to disturb or attempt to disturb the peace, quiet or right of privacy of any person especially where there is no purpose of legitimate communication.[220]

## *Legitimate Communication*

Legitimate communication occurs where the purpose of a particular electronic communication is genuine and lawful and occurs between genuinely existing individuals or entities. Where a person poses as a legitimate or trusted entity or individual and yet seeks to convince another to handover their personal details or information or any valuable thing, that act is called phishing; it is a form of electronic fraud. That communication is not legitimate. Where there is no purpose of a legitimate communication between the sender and receiver of

electronic communication; there is practically nothing in common between the sender and receiver warranting the communication, such communication is illegitimate.

To test the legitimacy of any communication, the persons must genuinely exist; there must be a genuine purpose necessitating the communication.

In summary, to prove offensive communication, the prosecution must show the following:

1. The communication was willfully or stubbornly sent to the complainant
2. The communication was repeatedly sent to the complainant
3. The communication had no legitimate purpose
4. The communication disturbed or attempted to disturb the peace, quiet or right to privacy of the complainant
5. The accused was responsible for the said offensive communication. Examples of Cases involving offensive communication in Uganda:

Access with intent to commit or facilitate the commission of a further offence

The Computer Misuse Act 2011, Section 13 is to the effect that

(1) A person who commits any acts specified under section 12 with intent to—

(a) commit any other offence; or

(b) facilitate the commission of any other offence, commits an offence

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

**Unauthorised Use or Interception Of Computer Service**

**Section 15 CMA, 2011** is to the effect that Subject to subsection (2), a person who knowingly—

(a) secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device whether similar or not; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) Damage caused by the offence attracts a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both.

Unauthorised Obstruction of Use Of Computer.

**Section 16 of the Computer Misuse Act, 2011** is to the effect that A person who, knowingly and without authority or lawful excuse

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer, commits an offence and is liable on conviction to a fine not

exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

# UNAUTHORISED DISCLOSURE OF ACCESS CODE

**Section 17 of the CMA, 2011** is to the effect that

(1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

# ELECTRONIC FRAUD

**Section 18 of the CMA, 2011 is** to the effect that:(1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

Abetment and Attempts.

Section 21 of the CMA, 2011 is to the effect that

(1) A person who abets another person in committing an offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

Attempt is defined **by section 22 of the CMA, 2011** as; (1) When a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some

overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

It has been held that attempt to commit is indeed an offence in R v Heyne and others 1956 (3) SA 604 (A) at 622:

# UNAUTHORISED DISCLOSURE OF INFORMATION

**Section 18 of the Computer Misuse Act, 2011**, provides that;

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

# CYBER-HOOLIGANISM

Computer network related mischief, such as defacing websites or releasing a virus or a worm, without necessarily causing any serious disruption or widespread panic or terror for the general population.[222]

The Internet has evolved from a scientific and military network to a crime scene. The network is used by scientists, spies and terrorists alike. Even though the cost of attacks in cyber-space is rising at a fast rate, the network is so widely used that it cannot be possibly shut down. This opens the door then to a group of individuals described as cyber-hooligans.

Cyber-hooliganism is defined as a computer network related mischief such as defacing websites or releasing a virus or worm, without causing serious disruptions for the general population, or without creating widespread panic or

terror. In addition to using computers for digital vandalism and low- level destruction. Another aspect is hacktivism, or using those tools to get a political message across.

Cyber-vandalism, or cyber-hooliganism, might include the knocking out of an e-mail system, defacing a Web site, or performing some other disruptive or annoying activity. Hackers seek to infiltrate secure computer systems in order to steal confidential information, such as the credit card data of customers.

Cyber-hooliganism is essentially non-violent, but can cause financial losses. For example, the creation of the I Love You virus or the destruction of the NASA web page were both cyber- hooliganism acts.[223]

## *The Existing Texts on Cyber-hooliganism*

The Council of Europe Convention on Cyber-crime is the only attempt to regulate this kind of computer related crime. It defined the cyber-hooliganism as an offence against the confidentiality, integrity and availability of computer data and systems. The penalty for this kind of offence is left to different national legislations.

The provision aims at criminalizing the intentional hindering of the lawful use of computer systems including telecommunications facilities by influencing computer data. The term hindering refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data. The hindering must furthermore be serious in order to give rise to criminal sanctions.

The definition of "serious" is understood to cover the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems, for example, by means of programs that generate denial of service attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge

quantities of electronic mail to a recipient in order to block the communications functions of the system.

The "hindering" must be unauthorised. Common activities inherent in the design of networks, or common operational or commercial practices are considered as authorised. These include, for example, the testing of the security of a computer system, or its protection, as authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized even if it causes serious hindering.

Nevertheless, Parties may have different approaches to. The text leaves it to the parties to determine the extent to which the functioning of the system should be hindered, partially or totally, temporarily or permanently, before it reaches the threshold of harm that justifies sanction under law.

The most important aspect is that the offence must be committed intentionally, that is to say, the perpetrator must have the deliberate intent to seriously hinder.

## *The Loopholes in Cyber-hooliganism*

The open and defiant manner in which attackers currently operate reflects the weakness of the legal, defensive, and investigative capacities of the current system. Some attackers are snared after long, expensive investigations, but most go unpunished. This stems ultimately from the fact that the information infrastructure is transnational in nature. Attackers deliberately fashion their efforts to exploit the absence of internationally agreed standards of behaviour and cooperation. For example, attackers can avoid prosecution or greatly complicate investigations simply by initiating attack packets from countries with inadequate laws, and routing them through countries that with different laws and practices, and no structures for cooperation.

The measures thus far adopted by the private and public sectors have not provided an adequate level of security. While new methods of attack have been

accurately predicted by experts, and some large attacks have been detected in early stages, the efforts to prevent or deter them have been largely unsuccessful, with increasingly damaging consequences. Intelligence exchanges have been slow, and investigations even slower. Some attacks are from states that lack adequate laws governing deliberate destructive conduct. A significant enhancement of defensive capabilities seems essential.

Cyber-crimes are often committed quietly, and remain unpublicised. According to the FBI, between 85% and 97% of crimes are not even reported or revealed.

## *The Suggested Solution to Cyber-hooliganism*

International laws must be drafted with the goal of securing speedy agreement among nations to adopt uniform definitions of offenses and commitments, despite having different network capabilities and different political interests.

The international community must encourage a universal recognition of basic offenses in cyber- space and the need for universal agreements to cooperate in investigating, extraditing, and prosecuting perpetrators. The law should describe the conduct it covers, including: interfering with the function of a cyber-system, cyber-trespass, tampering with authentication systems, interfering with data, trafficking in illegal cyber-tools, using cyber-systems to further offenses specified in certain other treaties, and targeting critical infrastructures.

The lack of an adequate international response to these weaknesses is puzzling, given the huge and growing financial impact of cyber-attacks and crimes. Even if some estimates of damages are inflated, the problem is becoming undeniably expensive to businesses, governments, and individual users around the world. Multilateral action is therefore required to build security into the underlying technical and social architecture. History has shown that when nations agree upon a common malicious threat, be it piracy on the high seas centuries ago, or aviation terrorism in the 20th century, a cooperative treaty mediated regime can contribute substantially to addressing the problem.

It is through such a treaty that Cyber-hooliganism must be criminalized, because it presents a real threat in its ability to disrupt and to produce serious damages to computer networks. Such criminalisation would not be effective unless it is punished with fines and imprisonment; hence the need for punitive measures to complete the chain of the global legal system of regulation and implementation.

# HACKING

Hacking is one of the most well-known types of computer crime. In this context, the term refers to the unauthorized access of another's computer system. These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan Horses that can shut down or destroy an entire computer network. Hacking is also carried out as a way to take credit card numbers, internet passwords, and other personal information. By accessing commercial databases, hackers are able to steal these types of items from millions of internet users all at once.

The New Hacker's Dictionary, a resource used to elucidate upon the art of computer hacking, has defined the practice through an assortment of definitions:

A hacker may be defined as any person who enjoys exploring the intricacies of programmable systems and how to stretch their capabilities. This definition is held in contrast to a generic computer user, who prefers to access a computer's minimal functions;

One who programs or who enjoys programming, as opposed to those individuals who simply theorize about programming.

An individual who possesses exceptional skill regarding computer programming;

A malicious meddler who attempts to discover and subsequently tamper with sensitive information through poking around computer-based technologies. These individuals are commonly referred to as "network hackers" or "password hackers."

Regardless of the definition, there are unwritten rules or principles that a hacker will ultimately live by. The belief that information sharing is a powerful exercise and that is the ethical duty of hackers to share their expertise through the creation of free software and through facilitating access to information and to computing resources is a fundamental code for which the majority of hackers follow. In addition, computer hacking as a practice revolves around the belief that system-cracking as a hobby or for fun is ethically okay so long as the hacker commits no vandalism, theft, or a breach of confidentiality.

# ISSUES OF COMPUTER HACKING.

Computer hacking possesses a mixed perception. Due to our reliance on computer technologies and the critical information shared on networks, the art of computer hacking has been skeptically viewed. That being said, there is also a "Robin Hood" mentality attached to the practice, where free programs or facilitated measures have been awarded to the average computer user.

The primary issue attached to computer hacking stems from an individual's ability to access crucial or personal information that is found on a computer network. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts.

## *Ways to Prevent Computer Hacking.*

Educational institutions must clearly establish use policies and delineate appropriate and inappropriate actions to all individuals who access information via a computer. The use of filters or firewalls may be considered to reduce access to unauthorized software serial numbers and other hacking-related materials.

# IDENTITY THEFT

Identity Theft is a truly modern crime, being crafted out of the sight of, and often beyond the effective reach of, the victim. It is carried out by compromising electronic data systems, obtaining false primary documents, directing mail to new addresses, obtaining new credit accounts and improperly charging existing ones. It can be accomplished by a neighbour next door or by criminals hunting from thousands of miles away. It relies on the facility of modern technology and superficial consumer security.

Identity theft is the unauthorized collection and fraudulent use of key pieces of information, such as social security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, thus creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen. Victims of identity theft suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names.

Identity theft is categorized in two ways: True Name and Account Takeover.

**True Name Identity** Theft means that the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain blank checks.

**Account Takeover Identity Theft** means the imposter uses personal information to gain access to an existing account. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes that there is a problem.

A new form of identity theft is phishing, which occurs when scammers send mass e-mails posing as banks, credit card companies, or popular commercial

web-sites, asking recipients to confirm or update personal and financial information in a hyperlink to a look-alike web-site for the spoofed company, and usually threaten suspension or deactivation of accounts for non¬compliance. Many of the emails claim to be anti-fraud departments at the institutions alerting the recipients to non-existent suspicious transactions.

The Internet has made it easier for identity thieves to use the information they have stolen because transactions can be made without any personal interaction. Computers make it possible to reduce therisk of personal harm to the criminal by decreasing the probability of detection, and therefore punishment, while at the same time significantly increasing the expected return.

Example of a scam case is: Nigerian Email Scam Case Conviction | State Vs Opara chilezien Joseph & Ors

## *The Existing Texts on Identity Theft*

Combating identity theft is difficult because each state or group of states has a different idea about how to combat the issue, about how much privacy invasion is allowed under a crime-fighting or civil litigation plan, and about what system would be useful for regulating and granting jurisdiction .

As a consequence, laws regulating identity theft differ in content in different countries. On the one hand, European States do not expressly criminalize the identity theft, while on the other hand, United States legislation sets up the toughest penalties. In 1998, the US Congress passed the Identity Theft and Assumption Deterrence Act, making identity theft a crime punishable by up to 15 years of imprisonment. In July 2004, the Identity Theft Penalty Enhancement Act stiffened penalties for the crime of identity theft even further, and established a new federal crime of aggravated identity theft for such serious offenses as bank fraud or defrauding employee benefit plans. Under the new law, those convicted of aggravated identity theft must serve an additional mandatory two-year prison term and enhanced five-year consecutive penalties if a terrorist-related offense occurs.

# CYBER-TERRORISM

Attacks and threats of attack against computers, networks, and the information stored therein, with the objective of intimidating or coercing a government or its people in furtherance of political or social objectives.

With the increased exposure to and dependence on Internet connectivity and dependent services, government, media and the public have also increasingly given more attention to the potential threat of cyber-terrorism to these Internet-connected systems, particularly for the critical information infrastructures of nation states

While a definition of terrorism has eluded the international community for decades, it is generally agreed that a terrorist act implies the use of violence for political objectives and for the purpose of sowing fear within a target population.

**Cyber-terrorism** is but one form of cyber-attack. Too often the terms cyber-terrorism and cyber- attack are used interchangeably and may result in a misunderstanding of the cyber-threat in general, and the threat of cyber-terrorism in particular. Politically motivated cyber-attacks that lead to death or bodily injury, explosions, or severe economic loss would be clear examples of cyber-terrorism.

Terrorism in cyber-space is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. To qualify as cyber- terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyber-terrorism is indeed a grave crime considering the substantial losses that even a single successful operation can generate. Cyber-space is constantly under assault from cyber-spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies. These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of web- sites on the Internet. Therefore we should also categorize as cyber-terrorism those attacks that cause less than total or partial destruction, like slowing down the performance of a machine or a server system, and thus produce financial consequences.

In contrast, cyber-terrorism has been used improperly to refer to the use of:

i. encryption technologies for secure electronic storage of data and communication by and between supporters/members of known terrorist groups;

ii. various forms of electronic communications (web sites, email etc) for the purposes of recruiting supporters, organizing and communicating the messages (propaganda) of known terrorist groups;

iii. the occasional use by known terrorist groups of cyber-attack techniques which are incapable of causing bodily harm, fear or serious economic damage; and

iv. the occurrence of port scans from countries considered to sponsor terrorism or which harbour known terrorist groups.

There is a major difference between cyber-crime and cyber-terrorism. Cyber-terrorism aims to wreak casualties and destruction through cyber-space, allowing attackers to remain far from the target. In contrast, cyber-criminals seek profits, and could focus on illegal transfer of funds, money laundering, Internet fraud, tax evasion, and communications between criminal organizations.

It is therefore prudent to distinguish between cyber-crime (an unlawful act wherein the computer is either a tool or a target or both), and cyber- terrorism. Cyber-terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber-space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives.

There are a number of reasons why cyber-terrorism is a very attractive option for terrorists. Firstly, it is cheaper than traditional terrorism methods. All that the terrorist needs is a personal computer and a simple telephone connection. Terrorists do not need to buy traditional offensive weapons such as guns and bombs; instead they can create and deliver computer viruses through a telephone line. Also, terrorists do not need to rent vehicles or to pay someone to deliver their explosives; they can deliver their terror from their home computer.

Secondly, cyber-terrorism is more anonymous than traditional terrorist methods. It is simply difficult to track a cyber-terrorist. There are no physical barriers such as checkpoints, customs agents, or borders which are crossed. Criminals in the physical world have long employed the tactics of masking their true identity with disguises and aliases. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ similar techniques. "IP spoofing" is one of the most common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine. It should not be difficult to detect this maneuver because there are very feasible technologies available to counter this spoofing now.

Thirdly, there are an exponentially large number of targets. These could be government computers, corporation computers, individual computers, public works, private airline computers, etc. within each of these categories of computers there are sub-categories of systems and networks that can be hacked into. Another appealing factor is that the law of averages dictates that with this

many computers and networks, there will be a large number of weaknesses and vulnerabilities that the terrorists can exploit.

Fourthly, cyber-terrorism can be conducted remotely. This feature of cyber-terrorism is especially appealing to cyber-terrorists. Typically, terrorists using traditional methods, such as suicide bombing, spend a great deal of time and money recruiting and training terrorists who eventually die carrying out their attacks. Cyber-terrorism would result in terrorist groups retaining a larger number of followers in relative safety.

Finally, cyber-terrorism has the potential to affect a larger number of people than traditional terrorist methods. For example, it was estimated that the I Love You virus affected more than twenty million Internet users and cost billions of dollars in damage. Because cyber-terrorism can affect more people, there is the potential for a greater degree of media coverage, which is ultimately what a terrorist wants.

It seems that the presence of firewalls and advanced encryption technology has not prevented intrusions, the theft of trade secrets, and the wreaking of havoc in government bodies. Many experts continue to warn of the persistence of a number of terrorist organizations attempting to develop new generations of viruses to launch wide-scale cyber-attacks.

Fears of cyber-terrorism attacks cover a number of scenarios including, developing a virus that enables the control of telephones throughout a community and prompts them to all simultaneously dial the emergency number in order to paralyze the emergency service. Losses would be heavier should this paralysis be accompanied by a bomb explosion in a market or building.

The rise of terrorism, as one type of asymmetric and distributed warfare, has not only threatened the gains derived from cyber-space, but has threatened the activities that now come to depend on communication through cyber-space infrastructure. Individuals and governments wish to ensure that they will continue to reap the benefits of cyber-space, and that cyber-space controls will not be turned against them. Their enemies see cyber-space as a high-value target.

It is legimately feared that terrorists may have developed an academy of cyber-terrorism, seeking means to attack the cyber- space infrastructure of the West.

Public opinion and dramatic attacks on computer networks could provide a means to do this with only small teams and minimal funds. Moreover, virtual attacks over the Internet or other networks allow attackers to be far away, making borders, X-ray machines, and other physical barriers irrelevant. Cyber-terrorists would not need a complicit or weak government to host them as they train and plot. On-line attackers could also cloak their true identities and locations, choosing to remain anonymous or pretending to be someone else.

Terrorists might also try to use cyber-attacks to amplify the effect of other attacks. For example, they might try to block emergency communications or cut off electricity or water in the wake of a conventional bombing or a biological, chemical, or radiation attack. Many experts believe that this kind of coordinated attack might be the most effective use of cyber-terrorism.

Cyber-terrorism could also involve the destruction of the actual machinery of the information infrastructure; remotely disrupting government computer networks, or critical civilian systems such as financial networks; or using computer networks to take over machines that control traffic lights, power plants, or dams in order to wreak havoc.

Attacks could also involve remotely hijacking control systems, with potentially dire consequences: breaching dams, colliding airplanes, shutting down the power grid, etc.

Uganda has in place the Anti-Terrorism Act, 2002 as amended 2015 and 2017 which is intended to fight all forms of terrorism.

# CYBER-WAR

The deliberate use of information warfare by a state, using weapons such as electro-magnetic pulse waves, viruses, worms, Trojan horses, etc., which target the electronic devices and networks of an enemy state.

Cyber-War, or information warfare waged over the Internet, basically involves the infiltration and disruption of an enemy's computer networks and databases, often with the use of weapons such as viruses, worms, trojan horses and the new electro-magnetic pulse wave weapon. The latter is particularly worrisome as the capability now exists to generate an instantaneous electromagnetic pulse that will overload and destroy the sensitive circuitry in advanced electronics and computer systems without any detonation of weapons in the upper atmosphere. Any system that is within the limited range of these weapons will be disrupted or have its electronic components destroyed. An electromagnetic weapon does not leave a crater like a conventional bomb, nor does it modify the operating system of a computer, and as a result the detection of an attack becomes more difficult.

Military doctrine, organization and strategy have continually undergone profound, technology-driven changes throughout history. Industrialization led to attrition warfare by massive armies in World WarI. Mechanization led to manoeuvre predominated by tanks in World War II. The information revolution implies the rise of a new mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that has greater technological knowledge will enjoy decisive advantages. The information revolution sets in motion forces that challenge the design of many traditional institutions. It diffuses and redistributes power, often to the benefit of smaller actors. It crosses borders, redraws boundaries, and generally compels closed systems to open up. The information revolution caused shifts, both in how societies may come into conflict, and how their armed forces may wage war.

In previous wars, critical infrastructure components such as airports, power plants, water systems, railroads, oil and gas pipelines, and communication centers were targeted by the military because their destruction could help cripple

a nation. These same components no longer have to be physically destroyed because most are dependent on computer-based systems that could be more easily disabled in a cyber-attack.

Cyber-war comes under what military theorists increasingly refer to as asymmetric warfare, whereby unconventional tactics are used by smaller players to offset their military weaknesses. Like a classic guerrilla struggle, which is a conflict of the weak against the strong, cyber-war can enable an individual to damage the computer system of a government or down the website of a multinational corporation. The weapon of choice can be nothing more than a laptop computer wired to the Internet.

In cyber-war, one single individual can target the chink in the armour of modern technology: that no computer system is totally invulnerable to attack from a talented and determined hacker. It is a form of warfare that can be conducted remotely and anonymously. Cyber-war may be less bloody but it is potentially highly destructive with far-reaching effects. Other possible scenarios include cyber- attacks on the websites and databases of businesses, on the Internet route-server infrastructure itself, as well as on public utility networks involving, for example, the tampering with electrical grids, the shutting down of telephone systems, the paralyzing of banking systems, and of rendering air traffic control systems inoperable. Whether the hackers on either side are labeled as terrorists or freedom fighters, or whether cyber-war is practiced as deliberate state policy, online warfare looks set to become a key part of today's era of connectivity and globalization.

Cyber-war can thus take various forms. It may occur between the governments of rival nation-states. It may arise between governments and non- state actors, but financed nevertheless by states. It may be waged against the policies of specific governments by advocacy groups, involving, for example, environmental, human rights, cultural, or religious issues. Non-state actors may or may not be associated with nations, and in some cases they may be organized into vast transnational decentralised coalitions.

In the case of cyber-risks, almost everything is new. The weapons are not kinetic, but software and knowledge; the environment in which he attacks occur is not only physical, but virtual; the possible attacker, even if it is a government, is able to hide effectively even during an attack. This form of warfare may involve diverse technologies, notably for command and control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend- or-foe, and for smart weapons systems. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits.

Decisive changes are occurring in how information is collected, stored, processed, communicated and presented, and in how organizations and governments are designing themselves to take advantage of this change. Information is now a strategic resource.

Cyber-war thus has broad ramifications for military organizations. Cyber- war now implies the development of new doctrines about the kinds of forces needed, where and how they are to be deployed, and how to strike the enemy. How and where to position what kinds of computers, sensors, networks and databases may become as important as the question once was for the deployment of bombers and their support functions.

As an innovation in warfare, cyber-war may be to the 21st century what blitzkrieg was to the 20th century. At a minimum, cyber-war represents an extension of the traditional importance of obtaining information in war: having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the enemy before he does the same to you.

The premise behind cyber-war is how to subjugate the enemy without fighting. It is designed to disable an enemy's armed forces and civilian infrastructure without the use of a single bullet. The computer will be the weapon of the 21st century.

The attractiveness of wartime use of information rests on the application of the theory that it may be more efficient to attack an enemy infrastructure than to

confront military forces on the battlefield. The strategy of attacking the civilian sector of a nation as a way to defeat its armed forces in the field is not a new one. In the late nineteenth century, military forces began to rely on industry for sustenance. This dependence has progressed to the point where wars are no longer aimed at defeating the enemy on the battlefield; they are wars of attrition, in which victory can be attained only through the destruction of the state itself, and the morale of its civilian population.

Current military theory suggests therefore that attacking a nation's centers of gravity, in addition to its armed forces, is the most effective way to destroy the state. In today's societies centers of gravity include telecommunications networks, energy and power sources, transportation systems, and financial centers and networks. Thus, the destruction of these systems becomes just as important as destroying an adversary's military forces.

Not only will cyber-war be a force in future warfare, it may also turn out to be the great equalizer for nations attacking adversaries with superior conventional military power. Most nations lack the resources to build a military machine and may use information technologies to overcome their battlefield inferiority.

The seriousness of the growing threat is magnified by the fact that cyber- war technology is inexpensive and widely available to both nations and individuals. Even individuals or hackers acting in small groups can do serious damage. The tools and techniques for doing so are widely available on the Internet. Individuals no longer need be inordinately familiar with the intricacies of computer technology to be a threat.

The incentive to use technology is greatly enhanced by the fact that it may be very difficult, if not impossible, to trace the attack back to its source. Cyber- war may also be quite easily dissimulated as "accidents" within the infrastructure of the target country itself.

While the law regarding cyber-war is likely to rely on UN Charter principles to define the legal boundaries of cyber-space, there is nevertheless a need for modern international law to define more precisely the criteria used to distinguish

which state actions are permissible. Technological change may even reveal contradictions among existing legal principles.

There are many challenges posed by cyber-war that existing international law does not cover.

Firstly, the type of damage that such attacks may cause may be rationally different from the kind of physical damage caused by traditional warfare. Bombs and bullets are visually destructive; however, the disruption of information systems may cause intangible damage, such as disruption of civil society or government services.

Secondly, the sovereignty of states is disrupted by the ability of technology to cross borders without hindrances. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each nation has exclusive authority over events within its borders. Radio waves or satellite signals, and the Internet, now allow individuals or groups to cross borders, while national legal authority generally stops at those same borders. The intangible violation of borders, that these signals may cause are not understood as traditional violations of sovereignty.

Thirdly, it will be harder to define the targets of cyber-war as military or civilian. The intangible damage the attacks cause may not be the sort of injuries against which the humanitarian law of war is designed in its protection of non-combatants.

Existing international law regarding cyber-war is sparse to non-existent. According to the Report of the International Law Commission to the General Assembly, the UN Charter normally prohibits international intervention through the use of armed force, but withholds comments on other, more subtle forms of coercion that do not involve a perceived threat of force. As force is too loosely defined, there is a great need to devise legal restrictions on the use of cyber-force.

## *The Loopholes*

Future international law must adapt to the fast changing nature of transnational communications systems . The United Nations has an opportunity to focus on not only creating international law regarding cyber-war but also an organization that focuses on the issues, threats and problems cyber- war poses to the global community.

The great shortcoming of international law is that it lacks the power of domestic law. Not only is there no real legislature, there is also no compulsory jurisdiction, or enforcement system. International law is created by means similar to entering into a contract where the parties to the agreement, whether countries, organizations, or a combination of the two, consent to be bound by specific terms. As a result, the parties to an agreement will commit violations where they feel their state interests in taking a proscribed action outweigh the political and diplomatic consequences of breaking the law.

The problem in many cases, cyber-war included, is that it is unclear whether conduct is prohibited under the present framework. Often the legality of issues remains unresolved until one nation acts and the United Nations General Assembly or the Security Council responds to that act. Such asystem is simply insufficient to regulate the use of information technology. A convention convened for the purpose of drafting a set of rules governing cyber-war is most likely the only way that a binding international doctrine on the subject will be enacted.

The question for such a convention is whether a nation's sovereignty is violated when an individual or a country accesses computer networks in another jurisdiction.

**Article 2, Section 4 of the U.N. Charter** prohibits, "the threat or use of force against the territorial integrity or political independence of any state. . . Article 39: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to

maintain or restore international peace and security. Article 41: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions……..Article 42: Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by land, sea or air forces of the United Nations". These articles describe the conditions under which the Security Council may authorize the use of armed force.

**Article 51 of the Charter** describes the condition under which individual members, individually or collectively, may use armed force in self-defense, and stipulates that, Nothing in this Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures to secure international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

The question is whether cyber-war qualifies as either a use of force or an armed attack. Neither the Charter nor the International Court of Justice defines these terms. Hence, it is unclear what exactly constitutes an armed attack. The term has been construed to require the use of armed forces, force, or violence, as well as interference with a nation's sovereignty. Without clarification from the U.N., a member state cannot know whether it is legally justified in responding to a cyber-war attack. It would certainly be problematic for a nation under siege from a cyber-attack to wait for the U.N. to decide whether it can or cannot respond.

The United Nations Declaration on the Definition of Aggression is equally unhelpful. It provides that the U.N. Security Council can address acts of aggression, which are characterized as, 'the use of armed force by a State against

the sovereignty, territorial integrity or political independence of another State". The declaration enumerates a non-exclusive list of acts that qualify as aggression, including, "invasion or attack by armed forces, military occupation, annexation by the use of force" on a foreign state, "the use of any weapon" against a foreign state, and an attack on the armed forces of another state. It is difficult to say whether cyber-war constitutes aggression. Although the results of cyber-war are tangible in a physical sense, the act of indulging in cyber-war itself is non-physical.

The **United Nations Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States (Non- intervention Treaty)** prohibits direct or indirect intervention in the, "internal or external affairs of any state. It also provides that armed intervention and all other forms of interference or attemptedthreats against the personality of the State or against its political, economic and cultural elements, is condemned". The major problem with the treaty is that it does not define intervention. It also gives no indication about which forms of interference constitute aggression warranting a response in self defense under **Article 51 of the Charter**.

International law regulates war on two fronts: the conduct of warring parties toward each other, and the conduct of belligerents in relation to neutral states. Whether cyber-war can be characterized as an act of war is essential to determining the constraints that the international community will place on its wartime use. If cyber-war is an act of war, then the following principles will govern its use.

The fundamental principle of humanitarian law is that there are limits to the methods that can be used against adversaries during warfare. Warring nations must avoid inflicting even collateral civilian injuries on a belligerent's civilian population. This concept was originally codified in the St. Petersburg Declaration of 1868 which, "recognized that the only legitimate object of war was to weaken an enemy's military forces". Civilians are not legitimate targets. Only military objectives may be targeted. They include those, 'which by their nature, location, purpose, or use make an effective contribution to military action

and whose total or partial destruction, capture or neutralization, . . . offers a definite military advantage".

Because of the concern over attacking proper objectives, humanitarian law91 requires that nations use weapons that allow aggressors to distinguish between military and civilian targets. The problem is that both the military and civilians use many of the same information systems. Thus it is unclear whether these dual-use systems may legally be attacked.

For example, according to customary international law, it is legal for warring parties to cut off lines of communication. As such, action taken to destroy or inhibit the lines of communication between military systems would most likely be permissible because they are a major military objective; but weighed against the potential harms that civilians might incur, this proposition becomes debatable. For example, a virus that is unleashed on a dual-use system might inhibit both its military and civilian functions, causing great hardship to civilians.

Humanitarian law also requires the aggressor to abide to the principle of proportionality in considering whether its attack is justifiable. The principle mandates that attackers weigh the potential civilian damage that might result against the benefits to be derived from attaining the military objective. The principle requires that parties responding to attacks consider whether their use of force in response is proportional to the wrong. Whether this principle applies to cyber-war is important for two reasons.

Firstly, it creates difficult issues for information warriors who seek to attack dual-use targets. If the principle does not apply to cyber-war, attackers do not have to be concerned with civilian losses. Secondly, if cyber-war is covered, it will be difficult to weigh whether the type of response is appropriate. Can a nation use physical means to respond to a cyber-war attack? What are the implications of using cyber-war to respond to attacks that occur in the physical plane? These dilemmas must be resolved in light of the proliferation of cyber-war technology.

During times of war, belligerents may not pass through or use the territory of neutral states. Thus, if cyber-war is construed as an instrument of force, it is arguable that information warriors would be prohibited from channelling attacks through the networks of neutral states. Given the ephemeral and uncontrolled nature of the Internet, it is difficult to see how that interdiction can be exercised.

In the past, such use of a neutral's territory was confined to the physical realm. Cyber-war attacks take place in another dimension, however, and once again there is no indication that the current law will cover these attacks.

## *The Suggested Solution*

It can be argued that the use of cyber-war is an armed use of force and therefore invokes **Article 2, Section** 4 and **Article 51 of the U.N. Charter, the Definition of Aggression, and the Non-Intervention Treaty**. International law theorists have been reluctant to characterize cyber-war as such, but their hesitance is unfounded. As technology has advanced, we have used machines as a more efficient means to carry out tasks that previously required use of human force in the tangible, physical sense. These innovations symbolize humanity's ongoing progression away from reliance on a physical means of carrying out force towards reliance on technology to achieve the same effect.

If a logic bomb can be detonated at a given time to severely damage computer systems, leading to subsequent physical damage, this is hardly different from an actual bomb on its way to a target. Each of these types of bombs is capable of causing the same amount of damage, may be detected before it blows, and should therefore be treated similarly.

A nation should not have to wait until a dormant threat comes to life as an attack in order to respond to it. No army officer would argue that he must wait for detected enemy forces lying in the tall grass of an open battlefield to attack before they can be eradicated. The same concept applies to dormant cyber-war threats. Thus, even attacks that have not yet manifested themselves should be

considered armed uses of force. Once more, it is the intended result that is critical.

It is imperative that the new international paradigm characterize acts as either war, terrorism, espionage, or something not prohibited by international law, so that nations under siege can know whether, and to what extent, retaliation is justified. Only by focusing on the result, rather than on the means by which that result is effectuated, can such clarity be achieved.

The most challenging aspect of regulating cyber-war will be the difficulty that victims will have in tracing the attack back to its source. Lack of accountability will encourage increased and reckless use of cyber-war. Thus, a new legal paradigm will effectively prevent, or at least limit, the use of cyber- war only if the repercussions of doing so are a sufficient deterrent when balanced against the gain sought by potential attackers. The seriousness of this threat indicates that the deterrents must be great indeed.

Terrorists might shut down an airport's control tower, causing many planes to crash, with resulting deaths in the hundreds or thousands. Such an act, though traditionally considered terrorism, must, in consideration of the potential extent of the harm, also be considered an act of war when sponsored by nation-states.

The same reasoning applies to state-sponsored espionage. Nations have been willing to tolerate a certain amount of such activity. The law frequently takes a results-based approach and distinguishes between, for example attempted wire fraud aimed at a single bank, and an attempt to shut down the New York Stock Exchange.

In fact, because the damage that cyber-war can cause is comparable in many ways to the damage that may result from traditional physical means; the law must also agree to hold parties accountable for the negligent use of cyber- war. For example, if a nation's information warriors plant a virus that causes a navy plane of another nation to accidentally crash into its carrier, the responsible nation should not be able to claim it was an accident. The consequences of cyber-war technology are grave, and its negligent use should not be excused.

The law must create severe penalties, including a possible damage repayment system, to deter nations from claiming ignorance.

The law should also require nations to cooperate in investigations, by allowing victim-states access to computer networks that may have been used to disguise the source of an attack. Refusal to cooperate with a reasonable investigation might be met with sanctions against that nation. In extreme situations, where there is strong evidence that the nation is shielding individuals who acted on its behalf, that evidence, combined with the refusal to cooperate, should be interpreted as an act of war.

As cited by World Federation of Scientists Permanent Monitoring Panel on Information Security in August 2003 in its Recommendation 3 ? : *"Cyber¬crime, cyber-terrorism, and cyber-wafare activities that may constitute a breach of international peace and security should be dealt with by the competent organs of the UN system under international law. We recommend that the UN and the international scientific community examine scenarios and criteria and international legal sanctions that may apply"*

Cyber activities that constitute deliberately hostile actions by nation states may threaten international peace and security, and yet elude penal sanctions under current legal frameworks or a future Law of Cyber-Space. One consideration is that, under certain circumstances, the international doctrine of sovereign immunity protects nation states against legal actions. This protection could conceivably extend to offensive cyber actions taken by nation states. Other concerns relate to the lack of international cooperation on a global scale, and technical considerations regarding the inability to effectively track and trace Internet communications.

The nations of the world must come together in a convention to confront the threat that cyber-war presents. The conclusion that must be reached is that cyber-war is eqivalent to the use of force as defined by United Nations documents.

# BANKING/CREDIT CARD RELATED CRIMES.

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information.

Use of stolen card information or fake credit/ debit cards are common.

Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami slicing.

E-commerce/ Investment Frauds.

Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

Merchandise or services that were purchased or contracted by individuals online are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

# SALE OF ILLEGAL ARTICLES

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.

## ONLINE GAMBLING.

There are millions of websites hosted on servers abroad that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

## DEFAMATION.

Defamation can be understood as the intentional infringement of another person's right to his good name.

Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. e.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone.

Cyber defamation is also called as Cyber smearing

Defamation is defined as "an intentional false communication, either published or publicly spoken, that injures another's reputation or good name."(Black's Law Dictionary (6th Edition, 1990)) Defamation includes the common law torts of libel (involving written or printed statements) and slander (involving oral statements). Significantly both libel as well as slander could be committed via internet medium

### *Ingredients of Defamation*

Defamation is an intrinsically personal wrong. The gist of defamation is actual or presumed damage to reputation flowing from publication. In other words,

defamation flows from publication or communication of information. In traditional libel case "publication" is generally referred to as "the date on which the libelous work was placed on sale or became generally available to the public."( Kenneth Love v. William Morrow & Co, 193 A.D.2d 586, 597 N.Y.S.2d 424 (2d Dep't 1993)) It has following ingredients:

1. Publication of a statement;
2. Statement makes reference to the plaintiff;
3. Statement is communicated to some person or persons other than the plaintiff himself;
4. Statement reaches the plaintiff; and
5. Statement causes actual or presumed damage to the plaintiff.

The question is does one encounter similar 'ingredients' when defamation occurs in internet medium? Here, the only difference is that the tort of defamation occurs when the defamatory imputation is published in electronic form, everything else remains the same.

**Various Legal Issues in Online Defamation Time of Occurrence of Publication.**

Publication occurs when the contents of the publication, oral, spoken or written are seen and heard,

and comprehended by the reader or hearer. From the point of view of plaintiff, the process of publication is complete, when the communication reaches him.

In **Godfrey v. Demon Internet Ltd. 4 All ER 342 (1999) the** defendant ISP carried the newsgroup 'soc.culture.thai' and stored postings within that hierarchy for about a fortnight during which time the posting was available to be read by its customers. On 13 January, 1997 someone unknown made a posting in the US in the newsgroup. This posting was squalid, obscene and defamatory of the

plaintiff who was resident in England. On 17 January, 1997 the plaintiff sent a letter by fax to the defendants, requesting them to remove the posting from their

Usenet news server. The defendants could have obliterated the posting after receiving the plaintiff's request, but it remained available until its expiry on or about 27 January, 1997. The plaintiff claimed damages for libel in respect of the posting after 17 January, 1997-the time when he affirmed to the ISP that the communication had indeed reached him. Morland, J. ruled: "In my judgment, the defendant, whenever it transmits and whenever there is transmitted from the storage of its news server a defamatory posting, publish that posting to any subscriber to its ISP who accesses the newsgroup containing that posting. Thus, every time one of the defendant's customers accesses 'social culture that and sees that posting defamatory of the plaintiff, there is a publication to that customer."

**Mode of Publication**

It looks into the mode of publication or transmission whether audio, video, textual or multimedia. Internet publishing is in 'electronic form'. Instances of defamation in 'electronic form' include generating, sending or receiving 'defamatory' e-mails, online bulletin board messages, chat room messages, music downloads, audio files, screaming videos, digital photographs, etc. on the internet.

**Forensic Issues/Evidential Issues**

Computer forensics mainly started with the first period a system administrator decided to find out what unauthorized changes had occurred and by whom in his system. Although, the concept is reasonably new, computer forensics can be considered as a branch of forensics. It was first limited to law enforcement divisions and investigators. Sambidge (2012) stated that antigovernment group manages to hack the Gulf Air official Facebook page by replacing the company’s logo with positing activist photo. The instance was immediately taken care of by Gulf Air and worked with law enforcement agencies to prosecute those involved.

However, in today's growing advancements, computer forensics tools are available for the public use. Organizations and individuals can conduct cases to investigate any suspected situations of computer crime and thus apply auditing standards and principles.

A clear-cut definition of computer forensics basically includes recovering data from floppy disks, hard drives, or removable disks such as flash memories. Forensic difficulties of compression, encryption, password protection and Steganography have been combined to the overall investigation process. On the hardware side recent additions include up-to-date technological innovations such as smart cards. Handheld devices such as electronic organizers and personal digital assistants can also be considered as possible evidence.

Another place evidential data can be located in and recovered are printers. Some have big stores of memory from which documents have the potential of being retrievable. The printer head, toner cartridge, or ink cartridge may also prove useful as physical evidence to locate specific printouts that were produced from specific printers. A branch of computer hardware which grew out of the requirement to share data faster and the want for centralized servers to store data, is the computer network. As these networks developed and interconnected, the Internet evolved.

There are two general techniques in visualization environments that analysts in forensic cases might use. The first is Non-hierarchal Visualization Techniques: non-hierarchal “views of file statistics display every files in a directory and its subdirectories without any consideration given to the relationship” among “said files and directories”. The second is “Hierarchical Visualization Techniques: hierarchical views of file statistics” display “the relationship of files as they exist in the directory structure (Teelink and Erbacher, 2006).

When dealing with computer forensics, the main type of evidence beside the physical type is the digital. Digital evidence is evidence that is kept on or transmitted by computers. It can play a major or a minor role in a wide range of crimes, including homicide, rape, abduction, child abuse, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, spying

and last but not least terrorism. However, an increasing amount of criminals are using computers and computer networks, few investigators are knowledgeable in the technical and legal matters associated to digital evidence. As an outcome, digital evidence is frequently overlooked, collected incorrectly and analyzed ineffectively.

According to an interview with the Head of Cybercrime Unit in the MOI with TradeArabia (2013), stated, Bahrain Cyber Police draft law which could enforce a maximum penalty of up to US$263,762.00 on hackers. He added that social media misuses are increasing "as hackers seduce young women into sharing private pictures and then post them on pornographic or matrimonial websites" and they argue for the need for more public awareness programs while the governmentalteam "of forensic investigators are qualified to deal with new threats and are constantly monitoring any new trends". Hence, he confirmed that, 80% of victims are women. Cybercrime rise 10 fold since the Unit was introduced during 2006 with above 200 cases being registered each year since 2010. During 2010 the Unit registered 223 cases but in 2011 they were 249 cases were reported. Unfortunately, the missuses of social media such Twitter and Facebook has increases the percentages of cybercrimes in Bahrain by creating phony accounts and begin for example, circulating and posting females' information and photos in pornographic websites, use in the wrong way and threating the victims.

Data types: Morris (2003) illustrated three types of data that users might use to hide evidence; nonetheless these data can be used in forensic examinations. The first type is "deleted data", this is basically the data that users delete and believe that it is removed from the system.

This is not true. Even if the user delete files from the recycle bin in the window operating environment, the data is not deleted from the system permanently.

The second type is "hidden data". This is data that the user wishes to store but hide from others. The simplest way to do so is by changing the name or file path

by of the file. Another way is by using encryption techniques that will hide the content and sometimes the nature of the designated file.

The third and last type is "system data" which is data stored by the operating system or other software related to operations and transactions occurring within a single computer or even a network. An example of such data is the Cookies folder that is used by internet sites to store information regarding site visits by the user. Examining files containing such data help retrieve and reveal information related to files that existed previously and logging activities to the system. Morris (2003) also describes a specific type of files which are the temporarily files that exist when a process is running or when installation is at progress. These files usually are removed once the application is closed or the system is shut down. Based on his experience, the most significant information related to a user's surfing activities over the Internet is generated by the combination of temporary files developed by the Internet Explorer Web browser and the Cookies file.

**Approaches and Methodologies**

Many researchers and computer forensic investigators argued different steps and approaches taken when conducting a computer crime investigation. Nevertheless, the majority agrees that the bold steps included in such an investigation include: securing the suspected computer, securing the potential evidence, collecting evidence, analyzing evidence and lastly preparing and presenting the evidence. May (2002), suggests some preliminary steps that must be considered before conducting an investigation. These steps include:

1. Documenting facts and clues that relate to any useful information for further referencing

2. Researching the background and history of computer and suspect

3. Establishing a well prepared chronological order of the main players who are involved in the case.

4. Establishing the level of damage caused by the incident to other computers or networks

5. Assess the degree of importance the involved systems are to running the business. If the system is vital to running the business the investigation has to occur outside working hours

6. Considering legal positions as well as the option of coordinating with the police

7. Allocating a team of expertise to conduct accordingly the investigation and asses the analytical techniques and tools use

May (2002) also noted that "one mistake which businesses often make is that subsequent to an IT crime they make every effort to get systems up and running as quickly as possible, destroying vital evidence in the process". This highlights the importance of the factor of time and how it can affect and question the process of data collection and the integrity of services provided by the business alongside.

A clear objective of the investigation: forensic or non-forensic and the main differences of each choice is important

After the preliminary actions have been taken once a crime is suspected, the next step in the forensic investigation is conducted: securing the suspect computer. It is important to make sure that evidence allocated on the computer are not tampered with or altered by anyone. Pictures of the alleged crime scene must be taken and descriptive precise notes must be noted as well. Pictures and notes provide a good reflection of the hardware and the connection methods situated. If the computer is a part of the network it has to be removed and the shutdown procedure must be documented.

The next step in the examination process is: securing potential evidence. This is a delicate and a critical issue. The investigator must ensure that the evidence is not contaminated while moving related hardware of the crime or isolating the

computer itself. Data stored on the suspected computer must be secured because they are easily targeted by offenders who might destroy the evidence by viruses or such. No one should be allowed to do anything to the suspected computer without the consent of the investigator who should do backups to make sure no data is changed or deleted throughout the investigation process.

The third step involves collecting the evidence. At this stage, deleted files are recovered and encrypted files are decrypted. This is done on copies of the original computer system to avoid updating the changes to the original system and thus losing potential evidences. Next is the step where analyzing of evidences collected is done. The investigator needs to have a keen eye supported with solid evidence to analyze hidden aspects of the collected data.

To finish the investigation the last step is reached: preparing and presenting the evidence. It is important to that the investigator validates and examines the integrity of the collected evidences before submitting them to the court. A solid case must be built on concrete allegations. Documentation plays a major role in this stage. The court will take into consideration all aspects of the investigation to check the reliability and effects forensic evidences hold against the offender.

Forensic Tools

The scope and exposure of computer forensics cover a wide range as noted earlier. It includes organizations and individuals. Auditing software related to computer forensics range from commercial to free applications. Cost does add efficiency and a more concrete presentation of data and reliability aspects, yet many free tools offer the basic needs to individuals and small cases. The aspect of finding forensic tools free on the Internet, for instance, supporting the idea that the concept of computer forensics is becoming more common than before. The collection of tools available nowadays is continuing to expand and developers are updating them with the latest technologies to support investigations. The investigator must keep in mind the diverse collection of tools available and the most suitable for the case at hand.

# THE ECONOMIC IMPACT OF CYBERCRIMES IN BUSINESS

According to **Savona (2012)** in the Global Council on Organized Crime report stated that, organized crimes suffer the loss of a multibillion cost on legal business, damages markets and affects extensive outcome on community. Accelerated through the equivalent strength of worldwide that involve extended business, global information and communications, criminal groups nowadays have extraordinary reach into the lives of normal citizens and into the boundary of international corporations and public organizations globally.

The estimation cost of cybercrimes are very difficult to authenticate, nevertheless a study by Norton Cybercrime (2011) reported that cybercrime cost 24 countries (UAE was the only Arab country among these selected countries for survey) Internet users US$388 billion worldwide. The amount encompasses US$274 billion in the time lost and US$114 billion for recovery. About 30% of surveys participants consider to a greater extend to be a target of cybercrime than physical globe crime.

Nevertheless it is estimated the cost of the global cyber activity to be between $300 billion to $1 trillion and in the USA alone between $24 billion to $120 billion.

It necessitate us all to work harder toward raising awareness, to enhanced security, to be further alert and to dedicate more in our cyber smarts and protection.

According to Gartner's latest report, news 24/7 sheds light on how the financial impact of cybercrime will increase 10 percent per year because of the continuing discovery of new vulnerabilities.

The report also articulated that new software vulnerabilities might arise and innovative attack paths would be developed by financially motivated attackers, as IT delivery method continues to meet the demand for the use of cloud services and devices owned by the employees. The combination of new vulnerabilities

and more targeted attacks will lead to continued growth in bottom-line financial impact because of successful cyber-attacks. Gartner, Inc. has also revealed its top predictions for IT organizations and users for 2012 and beyond.

A warning came out from a leading financial security expert who believed that small Bahraini banks could face attack from international criminals.

Tony Tesar, a Bahrain based financial security specialist Chief executive, stated that these recent events are continued proof that the crimes in banking sector are moving away from physical attacks to a harmless more financially profitable tactics of doing it remotely. Further to which he also mentioned that the ability to secure data on participant has never been more relevant and the use of effective firewalls has never been more critical. The need to on a regular basis tryout online orderliness and servers will be requirement in conflict these cases of pick apart and smaller banks with less effective make up one's mind will always be more prone to attack. These types of attacks are very unmanageable to foreclose and discover due to continuous advances in technology and the speed at which an attack can take social rank. Regular penetration testing (Pentesting) is essential and using a variety of organizations and individuals to assist with this will greatly help in staying ahead of advances in technology and in identifying loopholes and gaps in a bank's existing online and internal IT systems.

Mr Tesar said an alternate thought is the monetary and reputational effect it will have on the banks that are casualties of this sort of strike. Having adequate security methods set up and complete emergency administration and fiasco recuperation plans, will extraordinarily support in managing these sorts of assaults and the fallout that will accompany.

Meanwhile, Union of Arab Banks chairman Adnan Yousif said Bahrain-based banks are well protected from any cyber-crimes, reports our sister paper Akhbar Al Khaleej. They are sheltered from such ambushes in light of the fact that they utilize European advances starting from major worldwide organizations, including the sound supervisory approaches actualized by the Central Bank of Bahrain have helped raise a protected keeping nature’s domain.

Impact of cyber-crimes in business on a global scale: The 2011 Norton Cybercrime showed that over 74 million people in the United States were preys of cyber rimes in 2010. The direct financial losses caused by these types of criminal acts were $32 billion. About 69 percent of adults online have been victims of cybercrime resulting in 1 million cybercrime victims a day. Many people have the attitude that cybercrime is a fact of doing business online.

“Gary Warner, director of computer forensics research at the University of Alabama at Birmingham, has been quoted as saying that the fight against financial cyber-crimes is that the criminal complaint has almost disappeared. Even when a police report is filed it is often “so the bank will give you your money back.”

The cyber Intelligence identified that a decently huge and composed that is said to be utilized false wire exchanges as the method of strike. This digital security strike is said to influence session capturing in a man-in-the-middle cyber assault. Subsequently, Man-in-the-middle cyber-attack is characterized as a bargain where the assailant has the capacity to embed themselves between its target and the framework or administration in which the target is attempting to enter or utilization. An attacker finishes this by mimicking the framework or administration that the target is endeavoring to interface with by erroneously rerouting the movement to and from the administration or by commandeering session information. Different cyber intelligence sources have cautioned that an expected 30, U.S. based financial services institutions may be the focuses of an arranged cyber- criminal gangs that is said to be the element behind this strike.

As of late, the FBI issued a cautioning about dangers occurring as to cyber-crimes. Their cautioning expressed that the hoodlums behind this cyber-strike were utilizing numerous strategies to acquire client log-in accreditations. When the offenders have these qualifications, they start universal wire exchanges.

Reports being distributed in 2012 showed that cybercrimes have had a twofold digit development and are around the four greatest wrongdoing risks everywhere throughout the world, inside stake robbery unlawful acts, misrepresentation and

debasement. These patterns are the same everywhere throughout the world. Cybercrime industry has been gathering a ton of triumph throughout the previous five years. This sector of crime doesn't realize the word "crisis". Actually the cybercrime's financial and geographic development demonstrates no slowdown despite the global economic difficulty.

The lack of awareness have played an important role in the favor of cybercrimes therefore, no organization or company is immune to such crime. Another reason that was found was the inadequate protection measures against crimes as such, taken by organizations which are the leading cause of cybercrime.

There are three sorts of cybercrimes utilized by the criminals; they are Intrusive, silent and dangerous. Regularly the organizations/companies don't understand that they have been casualties of fraud or assaults until long after the crime has taken place. This sort of crime is called silent crime which turns into a major issue while battling such dangers. The outcomes are incapacitating and recover the circumstances is now and then unimaginable, precisely due to the time crevice between the criminal event and it revelation gives favorable element to the individuals who carry out law violations are often unbridgeable that makes it inconceivable for any actions of persecution. Numerous organizations are indeed throughout the years casualties of cybercrime yet are not familiar with it its a tumor that wrecks from inside.

According to the report "Second Annual Cost of Cyber Crime Study-Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of cybercrime has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of cybercrime for 50 organizations is $5.9 million per year with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year.

Greater part of cyber-attacks are generally alluded to a criminal activity led through the web that incorporate cyber espionage that is seizing bank accounts,

making and disseminating viruses to infect the exploited people, posting confidential business information on the internet and disrupting a country's critical national infrastructure.

In this market segment cybercrime is exceptionally furious and every day it tries to evade defenseless organizations that regularly neglect to meet the cyber threat, the related damages are destroying causing in many situations the end of the business. In this sector is desirable for governments to support small businesses in harmony with a cyber-strategy defined at the national level. Leave powerless the social fabric made up of small organizations has doubtlessly an immediate affect also on the business of large firms.

## CYBER SECURITY STRATEGIES

Besides understanding cyber law, organizations must build cybersecurity strategies. Cybersecurity strategies must cover the following areas:

**Ecosystem.** A strong ecosystem helps prevent cybercrime. Your ecosystem includes three areas automation, interoperability, and authentication. A strong system can prevent cyberattacks like malware, attrition, hacking, insider attacks, and equipment theft.

**Framework.** An assurance framework is a strategy for complying with security standards. This allows updates to infrastructure. It also allows governments and businesses to work together in what's known as "enabling and endorsing'.

**Open Standards**. Open standards lead to improved security against cybercrime. They allow business and individuals to easily use proper security. Open standards can also improve economic growth and new technology development.

**Strengthening Regulation**. This speaks directly to cyber law. Governments can work to improve this legal area. They can also found agencies to handle cyber law and cybercrime. Other parts of this strategy include promoting cybersecurity, proving education and training, working with private and public organizations, and implementing new security technology.

**IT Mechanisms**. There are many useful IT mechanisms/measures. Promoting these mechanisms is a great way to fight cybercrime. These measures include end-to-end, association-oriented, link- oriented, and data **encryption.**

**E-Governance.** E-governance is the ability to provide services over the internet. Unfortunately, e- governance is overlooked in many countries. Developing this technology is an important part of cyber law.

**Infrastructure. Protecting** infrastructure is one of the most important parts of cybersecurity. This includes the electrical grid and data transmission lines. Outdated infrastructure is vulnerable to cybercrime.

CHAPTER 12

# INTERMEDIARY LIABILITY

## INTRODUCTION

Intermediary liability refers to when internet intermediaries involved in the transmission processing or storage of electronic data across on the internet are held liable for unlawful content transmitted or stored on their networks. According to the OECD "internet intermediaries bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet based services to third parties."[102] It is inevitable due to the openness of the internet that "some users will post content or engage in activity that is unlawful or otherwise offensive."[103] Sometimes intermediaries may find themselves legally liable for content on their networks created by third parties, including content which they did not even know was on their networks.

102 OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives (OECD, 2011) 21 http://www.oecdilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policyobjectives_9789264115644-en

103 Center for Democracy and Technology, Intermediary Liability: Protecting Internet Platforms for Expression and Innovation, (Center for Democracy and Technology, April 2010) p1, https://www.cdt.org/paper/intermediary-liabilityprotecting-internet-platforms-expression-and-innovation.

It is important to institute proceedings against the intermediary than the user himself. It is easier to identify an intermediary than a user, and thus easier to bring them before a court for a criminal or civil offence. Intermediaries also have bigger pockets than the average internet user and can sued in court for damages more easily, and for more money. Intermediaries can be quite vulnerable to governments and corporations. Many governments seeking to use intermediaries to control certain content, also have control over the granting of telecommunications licenses.

Depending on relevant national law, liability for online content of third parties "can arise in a number of situations, both legitimate and politicized, including for defamation, obscenity, invasion of privacy, intellectual property infringement, or because the content is critical of the government."[104]

For governments, intermediaries "represents a potential point of control over content or unlawful behaviour." Private actors may "also threaten expression and innovation online if they can bring civil lawsuits against the intermediaries that host or disseminate expression that the private parties seek to suppress. [105] Intermediary liability has been argued to be an increasing trend globally in which responsibilities of law enforcement, as well as of copyright enforcement are transferred to intermediaries. Internet intermediaries are increasingly used to "police and enforce the law on the internet and even to mete out punishments.[106]

*Internet intermediaries* comprise the pipes through which internet content is transmitted and the storage spaces in which it is stored. Intermediaries are essential to the functioning of the internet. They act as intermediaries between two or more nodes on a network: as mere conduits for the transmission (sending or receiving) of information/data, as online storage spaces for online data, as

104 Ibid.

105 Ibid.

106 Joe McNamee, "Internet intermediaries – The new cyberpolice?" in GISWatch 2011 – Internet Rights and Globalisation, ed Alan Finlay, (Johannesburg: APC & HIVOS, 2011), 27.

platforms for storage and sharing of user generated content (UGC), or as platforms that provides links to other internet content. Intermediaries perform a passive and automatic role in the storage and transmission of electronic data, information or content – they are not actively involved in, and do not actively initiate the transmission or storage of data; this is done automatic manner and as a component of a service that is provided by the intermediary.

An internet service provider (ISP), that provides services like email or FTP is an intermediary. So is an internet access provider (IAP), which provides access to the internet. When using ISPs and IAPs users simply request a web page or a file, or send an email, and the data is transmitted by an intermediary (most often through a number of intermediaries) to its location. A network operator is also an intermediary; its business is the transmission of data between points on the network as well as other networks. Using the example of a mobile network operator; a user request information from a website or online service data is transmitted to the mobile device without active intervention or participation of the network operator.

Similarly internet cafes, or cybercafes can also be considered intermediaries, as they offer other users access to the internet A web host, or web hosting company, which stores web sites, or data or information on the internet for its users, is also an intermediary. The information on its servers, is uploaded and downloaded by the users.

Hereafter, the terms “Internet intermediaries” and “intermediaries” are used interchangeably.

In common usage IAPs are called ISPs, as most ISPs offer services (like email and hosting in addition to access) users by means of automated processes without direct intervention by the hosting company.

## *Examples of Internet intermediaries*

Social networking platforms like Facebook, Linked In, Orkut and Pinterest are also intermediaries. They play an automated role in the storage of and sharing of content between different users of the platforms.

UGC platforms like the blogging site Tumblr, or the microblogging site Twitter are intermediaries.

YouTube, image picture sharing sites like FlickR, and blogging platforms like Wordpress.com, provide platforms for users to upload, share and access content. Search engines also perform the role of internet intermediaries – providing links to websites that are searched for and retrieved automatically with computer algorithms. Content aggregators which automatically compile content from different online sources can also be intermediaries.

If an online entity performs a service that is automatic, and in which they are not actively involved in creating and selecting data, then they may function as an intermediary. Thus a news site, or even a blog may under certain conditions be an intermediary. Although they may publish their own content, if there is a comments section, forum, or some kind of hosted discussion, then the site acts as an intermediary for an automatically facilitated hosted discussion. A blog or news site that does not have comments, discussion, or mechanisms hosting UGC, is not an intermediary. Sites are not intermediaries for content they have actively commissioned or created.[107]

107 For example a news site is not an intermediary for transmission of content that it has paid for or commissioned for publication on the site, a blog is not an intermediary for content posted by the blog owners, in this case the blog or news site is a publisher.

## *When does intermediary liability occur?*

Intermediary liability occurs "where governments or private litigants can hold technological intermediaries such as ISPs and websites liable for unlawful or harmful content created by users of those services."[108] Intermediary liability can thus occur in a vast array of circumstances, around a multitude of issues including: copy right infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.[109]

Often intermediary liability can also occur in the context of laws that have not adequately taken account of the internet; especially the role of intermediaries. This is the case in Kenya and Nigeria. In these cases, understanding where intermediaries are liable, and where intermediaries are not liable, would entail a comprehensive review of all relevant legislation, criminal law, civil law and common law . Here intermediary liability is generally assessed on a case-by case basis, by reviewing legislation, and by looking at legal precedents.

Intermediary liability can also occur as a result of a conscious effort of governments and other actors to control certain aspects on the internet by holding intermediaries responsible for users. It can be a government or corporate (or combined) strategy for controlling illegal, unlawful, or undesirable content on the internet. This is a strategy adopted by the Chinese government to control aspects of the internet there.[110] In these cases intermediary liability is determined

108 Center for Democracy and Technology, op cit.

109LaQuadratureDuNetWiki,"IntermediaryLiability". http://www.laquadrature.net/wiki/Intermediary_Liabilityaccessed 29 September 2012.

110 Rebecca MacKinnon, "Are China's demands for self-discipline spreading to the West?"(McClatchy,18,January,2010), http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html. See also: Qian Tao, "The knowledge standard for intermediary

by investigating specific laws that mandate intermediaries to be liable in certain circumstances. There is little evidence to point towards intermediary liability currently being used as an effective cohesive strategy by governments to censor the internet in any of the countries in the study. However, this is always a risk in any society, especially where there is no legislated protection for intermediaries to mitigate for this (like for example in Kenya and Nigeria).

In many countries, there are legislated limitations on liability for intermediaries, often termed "safe harbour". This protection is provided under certain conditions; usually that intermediaries do not actively initiate or consciously modify the transmission, are unaware of unlawful content on their networks, and that they conform with certain laws and practices – like for example responding to take-down requests. In cases where there are limitations on liability, liability can only occur when intermediaries are not protected under existing legislation. This is the case under the **South African Electronic Communications and Transactions (ECT) Act (25 of 2002)[111], and the Ugandan Electronic Transactions (ET) Act (8 of 2011).[112]**

## *Assessing intermediary liability*

### The human rights consequences of intermediary liability

When intermediaries are exposed to risk for criminal or civil liability for content on their networks, they are incentized to control or police this content. Globally internet intermediaries are increasingly used to "police and enforce the law on the internet."[113] Intermediary liability can be argued to be a set of strategies for dealing with certain real problems of unlawful content on the internet – for

liability in China", International Journal of Law and Information Technology 20(1), 1-18.

111http://www.internet.org.za/ect_act.html

112http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=59&Itemid=61

113 Joe McNamee, "Internet intermediaries – The new cyberpolice?" op cit.

example to curb and control child pornography, hate speech or piracy of copyrighted material. Some of these strategies may however be unfair on intermediaries who did not create the content, where not actively involved in storing, transmitting or referencing it, are unaware of the content. Furthermore, such strategies can also have negative consequences on the functioning and usefulness of the internet.

The most obvious negative consequences are economic. If intermediaries are liable for content transmitted over their networks, then the expense and risk of building and maintaining these networks increases. If network operators were held liable for all criminal acts conducted over their networks, if ISPs were held liable for all unlawful content sent over emails, if hosting providers were liable for all content on their networks, and there were no limitations on this liability, then e-commerce and the information society would grind to a halt.

If user-generated content platforms and social networks are too scared to provide these platforms out of fear of liability, then these services would not be offered, resulting in adverse effects on freedom of speech and freedom of association. When policing roles are transferred to intermediaries this can also have chilling effects. If intermediaries, rather than the courts become responsible for determining what content is lawful and what content is not, this may undermine the right to a fair trial or due process, it can also cause intermediaries to be overzealous in policing content, so as to avoid liability. Intermediary liability may thus "create borders in the online world, undermining the very openness that gives the internet its value for democracy, and indeed, or the economy."[114]

At the extreme end of the potential negative consequences is that governments could use intermediary liability as a means of censorship. For a government seeking to control the internet in a way that undermines human rights, outsourcing control to third parties by mechanisms of intermediary liability can look better than, as well as be more efficient than technical mechanisms such as a web filter would, as Evgeny Morozov has pointed out:

114 Ibid.

"One way for governments to avoid direct blame for exercising more Internet control is to delegate the task to intermediaries. At a minimum, this will involve making Internet companies that offer social networking sites, blogging platforms, or search engines take on a larger self-policing role by holding them accountable that their users post or (in the case of search engines) index and make available.

Being able to force companies to police the Web according to state-dictated guidelines is a dream come true for any government. The companies must bear all the costs, do all the dirty work, and absorb the user's ire. Companies are also more likely to catch unruly content, as they are more decentralized and know their own online communities better than the state's censors."[115]

## *The need for limitations on liability*

According to the **Center for Democracy and Technology,** the history of the Internet to date shows that providing broad protections for intermediaries against liability is vital to the future of the Internet."[116] Every society needs limitations on intermediary liability in order for an information economy and information society to function effectively. Thus "protecting intermediaries from liability for the actions of third parties expands the space for online expression, encourages innovation in the development of new services, and creates more opportunities for local content, thereby supporting development of the information society." [117]

During the 1990s – first decade of the popular spread of the internet – it was realised that limitations on the liability of internet intermediaries needed to be legislated for in order to ensure the effective functioning of the internet. Thus many countries have introduced limitations of liability for internet

115 Evgeny Morozov, "Whither Internet Control?" in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. Larry Diamond and Marc F. Plattner, (Baltimore: Johns Hopkins University Press, 2012).

116 Center for Democracy and Technology, Op cit, p2

117 Center for Democacy and Technology, op cit, p1.

intermediaries. In **Ezeemoney Uganda Limited V MTN (U) limited**, the plainitiff successfully sued MTN for causing loss by unlawful means and inducing a breach of contract

In **Al Hajji Nasser Ntege Sebagala V MTN**[118], the plaintiff sued mtn for using his voice recording as a caller tune . However he was not successful because he had not copy righted the recording.

In **Byte Legion Technologies V MTN Uganda Limited**, [119]the plaintiff developed a soft ware programme and shared it with MTN company in making proposals for the two to work together. However to the shock of the plaintiff the company launched another similar product called GOOGLE SMS TRADER that was similar to that of the plaintiff.

The court dismissed the suit and held that the defendant was not obliged to inform the plaintiff about its simultaneous negotiations with Google. Court further held that the plaintiff was unable to prove copyright for his product.

In **Bassajjabaka Yakub V MTN**[120] , the plaintiff successfully sued the defendant for violation of his right to privacy when the company used his photo on abillboard without his permission.

**Limitations on liability under the European Union E-commerce directive.**

Under the European Union (EU) E-commerce directive, internet intermediaries[121] are afforded protection from intermediary liability for being a mere conduit for information, for caching information, or for hosting information.[122] Provided that these activities are "of a mere technical, automatic

[118]Al Hajji Nasser Ntege Sebagala V MTN Highcourt Commercial division Civil suit 283 of 2012

[119]Byte Legion Technologies V MTN Uganda Limited, High court commercial division 395 of 2009 .

[120] Bassajjabaka Yakub V MTN, high court Civil Division 100 of 2012.

121 Termed "information society services".

122 This does not include liability for the protection of individuals with regard to the processing of personal data which "is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of

and passive nature" and the intermediary "has neither knowledge of nor control over the information which is transmitted or stored. "[123] In the case of being a mere conduit, or of caching, in order to be protected from liability; the intermediary must not modify transmitted information, and not collaborate with recipients of its services in order to undertake illegal activity.[33] Protection from liability for hosting[124] is conditional on the service provider having been unaware of content on its networks, and once becoming aware of illegal activity on its network, acting expediously to remove it.[125]

**Intermediary liability in Nigeria, Kenya, South Africa and Uganda**

A report was carried out in on Internet Intermediary in Nigeria, Kenya, South Africa and Uganda are then explored. Finally important conclusions from the research are summaries, and a set of recommendations for all stakeholders affected by intermediary liability is provided.

Although addressed explicitly in South African legislation since 2002, and in Ugandan legislation since 2011, intermediary liability, termed as such, is a relatively new debate in Kenya, Nigeria and Uganda. While there is quite a substantial amount of literature on intermediary liability in Europe the United States of America (USA) and other countries. There is little existing literature comparing intermediary liability in African countries, and there are few developed African case studies. Considering that intermediary liability research is driven by policy and legal debates, and that policy discussion expressed as "intermediary liability" has been absent in the countries in the study until

individuals with regard to the processing of personal data and on the free movement of such data (2) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (3)"

123 Directive 2000/31/EC of the European Parliament and the Council, of June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Article 42. integrity of the data 33 Directive 2000/31/EC, Op cit, 43, 44.

124 Termed "storing information".

125 Directive 2000/31/EC, Op cit, 46.

recently, this situation not surprising. Thus this study is an exploratory study; it does not provide an exhaustive overview of intermediary liability in all the respective countries, it rather investigates important issues and themes framing the discussion in contemporary debate, and points towards strategic points for further research, advocacy and capacity building Issues relating to intermediary liability vary among the countries in the study but there are many common issues among the countries including the limitations on liability, the role of intermediaries with regards to terrorism and violence, hate speech, cybercrime, copyright infringement, digital piracy, and obligations to assist with lawful interception of communications.

Other than in South Africa policy debates around intermediary liability are relatively new. Limitations on liability were legislated in South Africa in the Electronic Communications and Transaction Act (25 of 2002)[126], almost five years before they were first contemplated in Kenya[127] and almost ten years before they were legislated in Uganda[128]. This is perhaps due to the relatively higher internet penetration in South Africa in the 1990s and 2000s – it had one of the highest rates of internet penetration in Africa and ranked higher than other countries with similar levels of economic development[129]. The absence of mention of intermediary liability in legislation in Kenya, Nigeria and Uganda is perhaps explained by the lower levels of internet access in these countries in the 1990s and 2000s. Now other African countries have overtaken South Africa, which is reported by some studies to have lower levels of internet penetration than Nigeria, Kenya and Uganda.[130] As all countries have in recent years

126http://www.internet.org.za/ect_act.html

127 Safe harbour like provisions for liabilities were proposed in the Now Defunct Electronic Transactions Bill of 2007.

128 In the Electronic Transactions Act of 20011, op cit.

129 "South Africa" in Freedom House, Freedom on the Net 2011, http://www.freedomhouse.org/report/freedomnet/2012/south-africa)

130 One study reports South African internet penetration at 17%, "it lags significantly behind the biggest Internet user bases of Africa." Nigeria has 29% penetration ,

experienced increased internet access, increased bandwidth and increased access through mobile phones, intermediary liability has emerged in legislative and policy debates.

Nonetheless issues concerning intermediary liability are neither new nor have they arisen out of a vacuum they have been discussed earlier in issue-based contexts using different terminology. In Nigeria the role of cyber cafes with regards to cybercrime was discussed in the mid-2000s. As mobile internet access has increased and relative rates of access from cyber cafes have decreased the discussion has now moved center around mobile phone operators. In Kenya, after the election violence following the 2007 elections, an ongoing debate about the role of communications intermediaries with regards to hate speech along with their role in peacebuilding began. The debate initially focused on the role of mobile operators and particularly focused on SMS/text messages. The debate continues as Kenya streamlines the writ and interpretation of its legal system to accord with its new constitution. Debate around the role of intermediaries in hate speech and in political messaging has regained momentum as the Kenyan General election approaches on the 4th of March 2013.

## *Protection for intermediaries*

In all countries in the study, excluding South Africa there is a significant degree of legislative and regulatory uncertainty with regards to issues around intermediary liability. Regarding limitations on liability for internet intermediaries, or "safe harbour"; only in South Africa and Uganda are there clear pieces of legislation limiting the liability of certain intermediaries for unlawful content under certain circumstances. In **Chapter XI of the ECT** Act provides internet service providers with protection from liability: service

Egypt has 26%, Morocco has 49% and Kenya has 25% (Arthur Goldstuck, *Internet Matters in South Africa*, Johannesburg: Word Wide Works, 2012,

http://www.internetmatters.co.za/report/ZA_Internet_Matters.pdf). Another study says that in South Africa 48% of people have "ever used the internet" this is compared to 57% in Senegal, 52% for Nigeria and 49% in Ghana, Kenya

providers are not liable for hosting, being a mere conduit or caching, provided that they conduct their operations in a specific manner, are a member of a recognised industry representative body, and adhere to its code of conduct, and respond to take down notices. The legislation has existed since 2002 but only recently has it come into effect when the minister recognised the Internet Service Providers Association (ISPA) as an industry representative body in 2009. Therefore only the 160 current members of ISPA are provided with limitations on liability. Many cyber cafes, individual blog owners, news sites, and other intermediaries that are not members of the ISPA are not afforded the limitations on liability afforded by **Chapter XI of the ECT Act**.

In Uganda under **Section 29 of the Electronic Transactions Act (2011**) a service provider is not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access. This is provided that the intermediary is not directly involved in the making, publication, dissemination or distribution of the material or a statement made in the material; or the infringement of any rights subsisting in or in relation to the material. **Section 30** states that service providers are not liable for infringement for referring or linking to a "data message or infringing activity" if the service provider, is unaware of the infringement, does not receive financial benefit from the infringement, and "removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of another.

In Nigeria and Kenya there are no pieces of legislation affording explicit protection for intermediaries. In Nigeria the copyright bill, which is currently under discussion may limit liability for intermediaries for copyrights content, should they be unaware of this content, as well as according to a number of other conditions. In Kenya the now defunct Electronic Transactions Bill of 2007, borrowing extensively from the EU Commerce Directive would have provided limitation on criminal and civil liability for third parties, where they acted as mere conduits, in caching processes, and when used as information location

tools. It also had a license and take down procedure, and provided immunity from liability for any actions taken once notified of the infringing activity. It is suggested in the report that this bill may need to be revisited in efforts to ensure that legislation provides for safe harbour for intermediaries.

## *Hate speech.*

Hate speech is an important area possibly affecting the liability of intermediaries in all countries. Nigeria, South Africa, Uganda and Kenya all have histories that include violent political conflicts in which hate speech, based on discrimination or ethnicity over mass media and/or ICTs have at some point played a role.

In South Africa, knowingly distributing films that advocate hatred based on race or ethnicity, gender or religion and constitutes and incitement to cause harm is an offence under Section 29 (1-2) of the Film and Publications Act (65 of 1996)[131] punishable by a fine or no more than five years of imprisonment. ISPs can thus be liable if they knowingly distribute hate speech (subject to limitations on liability in the ECT Act). The South Africa Promotion of Equality and Prevention of Unfair Discrimination Act (Act 4 of 2000) makes it a crime to publish speech that could demonstrate a clear intention to be hurtful, harmful, incite harm or promote or propagate hatred. It is also an offence to broadcast or distribute content that amounts clearly intends to unfairly discriminate against any person.

In Kenya the new constitution states that publishers can be held liable for publishing hate speech. Whether this clause in the constitution exposes intermediaries to liability has not been tested yet in courts. Online publishers and media groups are greatly aware of the problem of hate speech, and have made efforts at attempting to control it. For the Nation Media has issues guidelines on blogging and moderating comments.

131http://www.info.gov.za/view/DownloadFileAction?id=70901

In **September 2012 the Communications Commission of Kenya** released "Guidelines for the prevention of Transmission of Undesirable Bulk Political Content Messages via Electronic Communications Networks". The Guidelines which apply to Mobile Network Operators (MNOs) and Content Service Providers (CSPs) which provide content or content services.[132] They regulate the sending of "political messages" defined as "the transmission of political content by Political Parties and other individuals to the general public by SMS or MMS or any other similar medium that is capable of transmitting bulk.[133] Political messages are not to contain "inciting, threatening, abusive, misleading, confusing, obscene or profane language" or "inciting, threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule based on the basis of ethnicity, tribe, race, colour, religion, gender, disability or otherwise." Political messages must also not contain "attacks on individual persons, their families, their ethnic background, race, religion or their associations."

Political messages are only to be delivered by licensed Content Service Providers (CSPs)[134] with inter-operability agreements with mobile operators (MNOs). " MNOs are exempt liability for bulk content sent by third parties but CSPs are required to indemnify themselves (presumably through contractual agreements with the third parties), although it is not specified how. [135] Whilst

132 Under Kenya's Universal Licensing regime, "Licensees under this category shall provide contents services material, information services and data processing services." "Market Structure" Kenyan Communications Commission/ http://www.cck.go.ke/licensing/telecoms/market.html45 Multi Media Message.

133 Communications Commission of Kenya, Guidelines for the Prevention of Transmission of Undesireable Bulk Political Content Messages via Electronic Communications Networks. September 2012. http://www.cck.go.ke/regulations/downloads/Guidelines_for_the_prevention_of_transmission_of_undesirable_bulk_polit ical_content_via_sms.pdf Section 2.1.6

134 Under Kenya's Unified Licensing Framework,

135 Op cit, Sections 8.1 and 8.2: The guidelines state that "CSPs shall take legal responsibility for the content of political messages and must indemnify and keep indemnified MNOs. against claims that may arise out of those Political Messages" and that "CSPs shall endeavour to indemnify themselves against any claims that may

MNOs are exempt from legal liability, they are presented with responsibility of approving political messages. CSPs need to send an application to an MNO, before sending a bulk political message.[136] MNOs are effectively given the responsibility determining whether political messages approve or conform to the guidelines, and must come to a decision within 18 hours. If the MNO is unable to reach a decision, they may refer the matter to the National Cohesion and Integration Commission.

While many CSPs are not internet intermediaries because they sell content, and are actively involved in selecting the content, many others listed as CSPs perform intermediary functions and could be considered intermediaries.[137] The guidelines would impose possibly liability on CSPs for bulk messages sent by third parties. They would also impose liabilities on internet intermediaries to make censorship decisions, as well as onerous administrative costs. Imposing responsibility to moderate content on private corporations (MNOs) rather than industry bodies may have negative effects on transparency, or freedom of expression should MNOs be overly zealous in their new censorship responsibilities, or use these new powers to advance private or political interests.

## *Terrorism national security and lawful interception*

The role of intermediaries in the planning and coordination of violent acts such as terrorism is an issue that may expose intermediaries to liability. In Uganda the Anti-Terrorism Act (14 of 2002), states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news and materials that promote terrorism may be liable for the death penalty

arise out of Political Messages from the Political Party or individual sponsoring the Political Message."

136 This application must include the message and signed authorisation by the sponsor of the message, political party or identity documentation, and the timing of the message. Op cit, Section 4.1.

137 For a complete list of 83 listed CSPs, see "Content Service Providers", Communications,Commission.of.Kenya http://cck.go.ke/mobile/licensing/register/csp.html.

when convicted. Under the same act, any person that obstructs terrorism investigations, or interception and surveillance of communications under the act is liable to conviction and/or a fine not exceeding two years. **The Regulation of Interception of Communications Act of 2010,** introduces obligations to intermediaries to collect customer information (names, addresses, ID numbers), install surveillance equipment, and disclose information to authorities (when presented with a warrant or a demand from the minister). Intermediaries are obliged to assist "the monitoring centre" and ensure that their services can render real-time interception. Failure to assist the monitoring centre is an offence, that upon conviction may result in a fine, imprisonment for up to five years, or cancellation of the intermediaries license.

In Nigeria following coordinated bomb explosions in Abuja, discussions around the role of intermediaries in being used to plan violence and terrorism begun, after for the first time in Nigerian telecom history an intermediary came under the spotlight for being used to plan violent acts of terrorism. Following this the Telecom Facilities (Lawful Interception of Information) Bill was proposed, which is currently under discussion by the House of Representatives in the Nigerian National Assembly. This bill may introduce obligations for intermediaries to cooperate with lawful interception, as well as possibly introduce liability for failure to do so.

## *Copyright and digital piracy*

Law enforcement and public debate around digital piracy in the countries of the study, as well as in many other developing countries originally focused not on the internet or intermediaries, but rather on the distribution and sale of pirated material on CDs and DVDs. Perhaps due to increased levels of internet access in all countries, increased bandwidth and falling prices for access, digital piracy over the internet is now emerging as an issue policy and legislative debate.

In **South Africa** although the application of copyright law to the digital terrain is a very uncertain area.[138] In 2008, the **Recording Industry of South Africa (RISA**), has sent notices to the Internet Service Providers Association of South Africa regarding three South African hosted file sharing sites, which were then removed or disabled.[139] It has been argued that "Sites that collect, index and host so-called torrents are legal in South Africa [and] protected by the constitutional right to free speech."[140] In 2009, RISA requested that ISPA block access to block two Russian music sites that sold unlicensed/infringing mp3s. ISPA argued that it was not its responsibility to block sites.[141] Under the ECT Act intermediaries are not liable in South Africa for the transmission, storage, caching and referencing of copyright infringing content on their networks, provided that they did not create the data or initiate or modify the transmission. However this applies only to members of a recognised industry representative body. Intermediaries are have no obligation to monitor their networks for copyright infringements or police users in any way for copyright infringement (except at the request of a court). The Copyright Review Commission of the Department of Trade and Industry has recently made suggestions that a termination policy for

138 See Natasha Primo and Libby Lloyd, "South Africa" In *Media Piracy in Emerging Economies* (ed. Joe Karaganis) (Social Science Research Council, 2011), 99 – 148 http://piracy.americanassembly.org/the-report/., and Department of Trade and Industry, Copyright Review Commission Report (2011), http://www.info.gov.za/view/DownloadFileAction? id=173384.

139 These sites did not provide files but rather provided links to files, much like the pirate bay. They provided links to torrents files and NBZ files (used for downloading files from Usenet). Bit Farm and NinjaCentral were both bittorrent trackers, Newshost indexed NZB files, which are files that assist computers to download multiple files from Usenet Servers.

140 enigmax, Recording Industry Takes Down BitTorrent & NZB sites, (TorrentFreak, 6 November 2008), http://torrentfreak.com/recording-industry-takes-down-bittorrent-nzb-sites-081106/; enigmax, "Recording Industry Negotiates with Bittorrent and NBZ Sites" (TorrentFreak, 24 November 2008) http://torrentfreak.com/recordingindustry-negotiates-with-bittorrent-and-nzb-sites-081124/; and Rudolph Muller, "Risa and Torrent Website Truce?" (MyBroadband 24 November 2008) http://mybroadband.co.za/news/internet/6101-risa-and-torrent-website-truce.html.

141 enigmax, "ISPs refuse to block cheap russian music sites" (TorrentFreak 11 August 2009) http://torrentfreak.com/ispsrefuse-to-block-cheap-russian-music-sites-090811/

repeat offenders should be investigated and possibly implemented.[142] This would require however amending the ECT Act as such a policy would not be legal under the current act.

In Nigeria major concerns include the increasing amount of websites on which pirated Nigerian Music and Nollywood movies are available. Digital piracy has been brought onto the legislative agenda by means of discussions around various versions of the proposed Copyright Amendment Bill. The Copyright Amendment Bill could possibly give intermediaries obligations to disconnect repeated copyright infringer, and liability if they fail to do so. Disconnection of one's internet connect for repeated copyright infringement, as well as having human right implications, could also potentially have implications on cybercafes; meaning that they would be exposed to liability in the form of potential disconnections of their internet connection, if their users download pirated material. There are no limitations on liability for copyright infringements by third parties on their networks, although one of the versions of the proposed copyright amendment bill would have safe harbour clauses covering transmission, hosting, caching and referencing.

In Kenya during the time of the writing there was a court case concerning a mobile website WAPKid, that provides free pirated Kenyan music for mobile download.[143] Although the site is hosted in Turkey, and the domain registered with the US registrar GoDaddy[144] so the infringing site is outside of Kenyan jurisdiction, it has been alleged that mobile operators sent an SMS, encouraging

142 Department of Trade and Industry, Copyright Review Commission Report (2011), Op cit.

143 The court case involves copyright holders as the plaintiffs and mobile operators as the defendants and involves the case of a mobile website based in Turkey, WAPKid.com which is offering free MP3 downloads of Kenyan music. It is alleged that certain mobile operators sent out an SMS to customers encouraging them to download from this site. For a discussion on the matter see the KICTAnet discussion thread, Music Piracy in Kenya – Government Can Help, KICTAnet mailing list 26 September 2012, http://www.kictanet.or.ke/?p=12377.

144 http://whois.domaintools.com/wapkid.com, last accessed

users to download content from this site.[145] If this is true, then the operator(s) who sent these messages, would cease to be intermediaries, as they were actively encouraging users to download content, thus applying principles of safe harbour (if they existed in Kenyan law) would be irrelevant.

In Kenya, intermediaries have an ambiguous role with regards to copyright infringements, they are not required to monitor for copyright infringement, nor implement punitive action. They are however not protected from liability for copyright infringements.

Digital piracy and digital copyright infringement do not seem to be policy issues in Uganda, nor have their been many court cases in this regard. Uganda's safe harbour laws under the Electronic Transactions act would however possibly protect intermediaries from liability for infringing content or actions of third parties.

It is important to note that many artists are not aware of their rights as content creators or copyright holders, and the avenues of recourse available to them for infringements. For example in Nigeria where the Nollywood and the local industry experiences much online copyright infringements, artists do not however for example file DMCA take-down requests with YouTube, even though it would be very easy to do so.[146] In South Africa, South African Music Rights Organisation (SAMRO) and the Recording Industry of South Africa where provided by ISPA with their own specialised take-down notice form,[147] RiSA has not sent any take-down notices since 2008, and SAMRO has never sent any take-down notices.[148]

145 The author has no source for this, other than the discussion on the KICTAnet list, op cit.

146http://www.youtube.com/t/copyright_noticehas instructions on how to file a copyright infringement notification with YouTube.

147 Loge a RiSA Specific Takedown, http://ispa.org.za/code-of-conduct/lodge-a-risa-specific-takedown/

148 Copyright Review Commission Report (2011), Op cit. P37, Interview with Ant Brooks, former General Manager of the Internet Service Providers Association and

Emerging in all of these countries is a digital divide in legitimate distribution channels. For example the Music Streaming Service Spotify, and the movie streaming service Netflix are not available in any of the countries in the study.[65] Apples I-Tunes store has at the time of writing also yet to launch in South Africa. Local digital distribution channels are growing but also struggling to take traction. This is no doubt reinforced by the legislative and regulatory uncertainty with regards to content in the digital age in all countries of the study.

In Nigeria the debates have gradually shifted from cybercafes and crime to telecom operators and ISPs and the issues of terrorism, copyright infringement, and digital piracy. In Kenya during the election violence hate speech particularly over mobile phones have remained central to the debate since the election violence in 2007 and in the run up to the general election in 2013.

SMS has been a focus and often the issue that often starts the debate. While SMSs are not internet content, it would make sense to include telecommunications intermediaries who bear SMSs into these debates. As content moves between SMSs and the internet, and SMSs are sent by network operators that are also internet intermediaries. Similarly, when adopting a human rights based or legal based approach, human rights and laws are the same online as they are on mobile networks, and offline

Common to all the countries in the study is that intermediaries operate in an uncertain environment with regards to the liabilities that they may possibly be exposed to. While there is some protection for intermediaries from liability in South Africa and Uganda, intermediaries in all countries in the study operate under an uncertain environment, and could be exposed to undue liability that could hamper the development of the information society and economy. This points to a need for clearer legislation in all countries regarding intermediary liability, as well as to a need for clearly legislated protection from liability for intermediaries in all countries. This can only be achieved by informing and

current member of the ISPA Secretariat. 65 Although the streaming service simfy has recently launched in South Africa.

building the capacity of all relevant stakeholders to engage in debates and advocacy around intermediary liability.

All stakeholders in information and communication technology and web users in these countries and the rest of the content should take advantage of this opportunity of increasing debate around this topic to involve themselves in discussions about intermediary liability, in order to shape its future on the continent.

All countries require legislated limited liability (safe harbour) for internet intermediaries. Intermediaries must be given safe harbour under the conditions that they do not initiate or modify communications (other than in an automatic manner), that they respond to take down notices in a fair and transparent manner, that they comply with lawful requests by means of warrant or court order. While indigenous solutions are preferable to "one size fits all" approaches adopted from other legislations, a lot could be learned from CDA 230 and the DMCA safe harbour provisions in the USA, the EU E-commerce Directive, and chapter 11 of the South African ECT Act. These lessons relate both to how intermediaries are protected from liability but also how take down systems in these countries are abused. All stakeholders need to inform themselves and get involved in legislative processes. Safe harbour provisions should include all internet intermediaries and should not exclude legitimate intermediaries due to technicalities or institutional requirements. In South Africa for example limitations on liability needs to be extended beyond only members of the ISPA.

Protection from liability should also be extended to smaller intermediaries like cybercafes and even to individual intermediaries like blog and website owners.

All countries need fair and transparent take-down procedures that are legislated and regulated. These procedures should provide all affected parties with reasonable recourse and due process. Take-down procedures are often unduly skewed towards the complainant. Intermediaries, seeking to avoid liability are not incentivised to defend the interests of third parties (the original creators of the alleged infringing or unlawful content). Take down procedures must include mechanisms for recourse for third parties.

Multi stake holderism needs to be a central principle in policy and legislative debates around intermediary liability. These debates must not just be between governments, the internet industry and copyright holders/intellectual property holders. Civil society, and content creators as well as all affected users of the internet need to get involved.

Termination of internet connections for repeat copyright infringements represent a human rights dilemma, access to the internet is a human right, and denying this right can have consequences on other rights like the right to free expression. Furthermore given the importance of cybercafes and internet sharing and the fact that many cybercafes are small to medium enterprises, and often informal businesses, this imposes challenges on cybercafes, as well as an incentive or a sanction to monitor communications in order to avoid liability. Which can have implications on the right to privacy and free expression, as well as cost implications for cybercafes. Termination policies must have a punishment that fits the crime, and must balance concerns with copyright enforcement with concerns about the rights of individual users, must be sensitive to cybercafes and small businesses.

The mobile phone will always be important to discussions on intermediary liability in Africa. SMS operators and SMS platforms must also be considered intermediaries, and should possibly be dealt with the same way in legislation as internet intermediaries are, and must be offered similar protections.

## *The Fall and Rise of Intermediary Liability Online.*

As the scale and scope of the Internet has grown to permeate all aspects of the economy and society, so too has the role of Internet intermediaries who provide the Internet's basic infrastructure and platforms by enabling communications and transactions between third parties as well as applications and services. 'Internet intermediaries' give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties. They offer access to a host of activities through both wired and wireless technologies. Most 'Internet intermediaries' are from the business sector and they span a wide range

of online economic activities including: Internet access and service providers (ISPs), data processing and web hosting providers, Internet search engines and portals, e-commerce intermediaries, Internet payment systems, and participative networked platforms.

Intermediation is the process by which a firm, acting as the agent of an individual or another firm, leverages its middleman position to foster communication with other agents in the marketplace that will lead to transactions and exchanges that create economic and/or social value. The main functions of Internet intermediaries are i) to provide infrastructure; ii) to collect, organise and evaluate dispersed information; iii) to facilitate social communication and information exchange; iv) to aggregate supply and demand; v) to facilitate market processes; vi) to provide trust; and vii) to take into account the needs of both buyers/users and sellers/advertisers. There is sometimes tension between various functions of Internet intermediaries; for example, tension between preserving identity and privacy while personalising products and services in ways that benefit users or between infrastructure provision and usage.

The pace of change of Internet services and their technical complexity means that reaching stable, established business practices is difficult. It should be re-emphasised that business models are currently in flux and are likely to remain so for most identified intermediaries. In parallel, the blurring of boundaries between what national statisticians classified as separate activities and the creation of new areas of activity that are not necessarily based on transactions make measurement challenging. Nonetheless, available data provides some insight:

Internet access and service providers (ISPs) in several OECD countries operate in consolidating markets. Broadband subscriptions and mobile Internet access services are the main growth segments although business models for mobile Internet access are still in flux. The evolution to mobile broadband is becoming increasingly pronounced.

Data processing and web hosting providers also face strong competition and this competition may originate from anywhere in the world. Growth areas include

shared web hosting and software as a service, offered on subscription basis, that are also known as 'cloud computing', i.e. scalable and often virtualised resources provided over the Internet.

Internet search engines and portals are now highly concentrated, with advertising as the primary source of revenue. They continue to experience very high growth resulting from demand for more efficient search functions and for the expanding array of services they offer on one side, and from demand for online advertising, on the other. Competition continues apace, particularly in developing markets.

The emergence of participative networked platforms, including virtual worlds, is a comparatively recent development and online advertising is seen as a main future source of revenue for this sector. In addition, ancillary linked products - in particular mobile - drive traffic, revenue, engagement, and overall value.

Against the broadening base of users worldwide and rapid convergence to IP networks for voice, data, and video, 'Internet intermediaries' provide increasing social and economic benefits; whether it be through information, e-commerce, communication/social networks, participative networks, or web services. 'Internet intermediaries' provide economic growth with new businesses and productivity gains through their contribution to the wider ICT sector as well as through their key role within the Internet ecosystem.[141] They operate and maintain most of the Internet infrastructure, which now underpins economic and social activity at a global level, and are needed to help ensure there is continued sufficient investment in both physical and logical infrastructure to meet the network capacity demands of new applications and of an expanding base of users.

'Internet intermediaries' also stimulate employment and entrepreneurship by lowering the barriers to starting and operating small businesses and by creating opportunities for 'long-tail' economic transactions to occur that were not previously possible, whereby businesses can sell a large number of unique items, each in relatively small quantities. Internet intermediaries enable creativity and collaboration to flourish among individuals and enterprises and generate

innovation. User empowerment and choice are considered to be very important and positive social side effects of the access to information that Internet intermediaries provide, as well as improving purchasing power with downward pressure on prices. A critical role of Internet intermediaries is to establish trust including through protection of user privacy. By enabling individuality and self-expression, they also offer potential improvements to the quality of societies in terms of fundamental values such as freedom and democracy.

Several caveats warrant stressing. First of all, it is important to note the differences between the categories of actors being clustered under the concept of 'Internet intermediaries'. Additionally, in practice, categories are often not clear-cut as Internet intermediaries may play more than one role. Moreover, statistical definitions tend to focus on Internet information and service sectors in general and do not necessarily distinguish those with an intermediation role.

In considering the role(s) of Internet intermediaries, it is important to appreciate that Internet intermediaries may have different and potentially competing simultaneous roles as intermediaries, end- users and content/service providers. For example, some Internet service providers deliver their own content. Some e-commerce platforms sell goods that they take title to.

# INTERNET ACCESS AND SERVICE PROVIDERS

Although the terms Internet service provider and ISP are in universal usage, they are potentially confusing because they do not necessarily distinguish between the underlying roles of access provider, host, and others. In this document Internet service providers are generally meant to signify Internet access providers, which provide subscribers with a data connection allowing access to the Internet through physical transport infrastructure. This access is necessary for Internet users to access content and services on the Internet and for content providers to publish or distribute material online.

ISPs may provide local, regional, and/or national coverage for clients or provide backbone services for other Internet service providers. They include 'pure-play'

ISPs as well as wired and wireless telecommunications providers, and cable providers that provide Internet access in addition to network infrastructure. Internet service providers have the equipment and telecommunication network access required for a point-of-presence on the Internet. They may also provide related services beyond Internet access, such as web hosting, web page design, and consulting services related to networking software and hardware.

ISPs are typically commercial organisations that generally charge their users - whether households, businesses or governments - a monthly fee on a contractual basis. Sometimes the fee is bundled with other services, as in the "triple play" offered by cable and telephone companies for television, telephone, and Internet access. Laptop users in Internet cafes or wireless "hot spots" may pay an ISP (directly or indirectly) for daily access or even hourly access. ISPs range from large organisations, with their own geographically dispersed networks, local points of presence and numerous connections to other such networks (Tier 1 providers - usually large telecommunications companies), to small providers with a single connection into another organisation's network.

## *Data Processing and Web Hosting Providers, Including Domain Name Registrars*

Today, many providers of data processing and web hosting services are better known as "cloud computing" platforms that enable their clients to use the Internet to access services, such as software as a service or hardware as a service. The 'Data Processing, Hosting, and Related Services' industry group consists of firms that provide infrastructure for hosting or data processing services. They are involved primarily in handling large amounts of data for businesses, organisations, and individuals. Most data hosting companies, including domain name registrars, sell subscription services, while data processing services companies often sell services on a per-unit basis.

'Data processing' firms transform data, prepare data for dissemination, or place data or content on the Internet for others. 'Web hosting' service providers supply web server space and Internet connectivity that enable content providers to

'serve' content to the Internet. They may provide specialised hosting activities, such as web hosting, streaming services or application hosting, provide application service provisioning, or may provide general time-share mainframe facilities to clients. Many hosting providers also provide domain name registration services (acting as registrars) and increasingly, additional tools to enable their customers to create websites, manage their sales or sell on-line.

## *Internet Search Engines and Portals*

Internet search engines and portals operate websites that use a search engine to generate and maintain extensive databases of Internet addresses and content in an easily searchable format. Content may consist of web pages, images or other types of digital files. Search engines index information and content in an automated fashion, based on sophisticated algorithms. Web search portals often provide additional Internet services, such as e-mail, connections to other websites, auctions, news, and other limited content.[145] It should be noted that many portals do not rely on automated search engines alone, but also include human editors whose function is similar to that of a magazine editor.

Search engines and portals generally provide free services to their users even though these services involve significant investment in technical development and infrastructure to meet simultaneous demand of a growing number of users. Investments and operating costs are most often funded through advertising. For example, Google, Naver in Korea and Baidu in China, use auction-based advertising programs that let advertisers deliver ads targeted to search queries or web content across the search-engines' sites and through affiliated third party websites. Advertisers are increasingly charged per user that clicks on the ad versus per user that sees the ad. Revenue-sharing mechanisms with affiliated websites are often used.

## *What are the main models of internet intermediary liability?*

**There are two main models**:

"**Generalist":** In this model, intermediary liability is judged according to the general rules of civil and criminal law. Under this model, which applies in most countries, intermediaries can be liable for content either because they directly contributed to the illegal activity (contributory liability) or because they indirectly contributed since they had the ability to control it and derived a direct financial benefit from not doing so (vicarious liability). This generalist model applies in many African countries, as well as in some areas of South-America (including Argentina and Peru).

"**Safe harbour":** In this model, a legally safe place (a safe harbour) is given to intermediaries – provided their actions stay within this safe harbour, they will not be liable for user actions. This immunity from liability is subject to conditions, which can be very detailed and stringent (referred to as a "vertical" safe harbour, which is limited to one specific area, e.g. copyright or trademark law) or designed to deal with different types of activities and liability under different areas of law (referred to as a "horizontal" safe harbour, which applies across different domains).

The existence of strong safe harbours is considered a strategic factor supporting the emergence of innovative services: it provides intermediaries with the sufficient legal certainty to conduct a wide range of activities, free from the threat of potential liability and the effect of potential litigation. However, there are also concerns that overly broad safe harbours make it more difficult for others to uphold their human rights online.

## *How Intermediaries Regulate Online Content.*

There are five main ways that internet intermediaries are involved in regulating content online:

1. "Notice and takedown": This requires intermediaries to remove content that is deemed illegal, once they have notice of it.

2. "Notice and notice": This requires intermediaries to notify the creator of content which is deemed illegal, before proceeding to any takedown.

3. "Notice and disconnection" (or if no disconnection is foreseen, "graduated response"): This requires intermediaries (so far, only ISPs) to impose on repeated infringers a series of sanctions, which escalate progressively in accordance with the repetition of alleged infringements and may, in extreme cases, culminate in the termination or degradation of services for those particular users.

4. "Filtering and monitoring": This requires intermediaries to take measures to prevent the repetition of violations, including facilitating the identification of users, and identifying, removing or blocking illegal material.

5. "Contract regulation": This enables intermediaries to regulate content through their own contractual terms and conditions (commonly known as "**Terms of Service" or "ToS").** ToS create private regimes of content regulation that are self-enforceable, operating independently from the applicable public law framework. In the field of copyright, ToS are increasingly used to implement agreements between the content industry and ISPs, whereby ISPs adopt so-called "voluntary measures" to deter infringements. These are often an integral part of graduated response regimes.

### *How are users affected by internet intermediary liability?*

Internet users may be affected by internet intermediary liability in both positive and negative ways. On one hand, the quality and variety of products or services that are available to them may be restricted or more expensive if there is a lack of competition and innovation in the intermediary market because intermediaries are unwilling to risk liability for service innovation. On the other hand, extending a law enforcement role to intermediaries poses risks to the rights to freedom of speech, privacy and due process, especially if intermediaries adopt restrictive terms and conditions on content and more human rights-intrusive procedures for the management of content in their spaces. In addition, users' human rights are also at risk if intermediaries will not take down human rights-violating content, but the legal system is not able to offer prompt and effective remedies against the violation of individual rights. This is especially so where the private contractual regimes established by the intermediaries are inadequate.

## INTERMEDIARY LIABILITY IN UGANDA

This is provided for under **sections 29-34 of the Electronic Transactions Act, 2011** as seen below.

### *Liability of a service provider*

(1) A service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on—

(a) The making, publication, dissemination or distribution of the material or a statement made in the material; or

(b) The infringement of any rights subsisting in or in relation to the material.

(2) This section shall not affect—

(a) An obligation in a contract;

(b) The obligation of a network service provider under a licencing or regulatory framework which is established by law; or

(c) An obligation which is imposed by law or a court to remove, block or deny access to any material.

(3) For the purposes of this section, provides access, in relation to third-party material, means providing the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access.

## *Information location tools.*

Where a service provider refers or links users to a data message containing an infringing data message or infringing activity, the service provider is not liable for damage incurred by the user if the service provider—

(a) Does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;

(b) Is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) Does not receive a financial benefit directly attributable to the infringing activity; or

(d) Removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

## *Notification of infringing data message or activity*

(1) A person who complains that a data message or an activity relating to the data message is unlawful shall notify the service provider or his or her designated agent in writing and the notification shall include—

(a) The full name and address of the person complaining;

(b) The written or electronic signature of the person complaining;

(c) The right that has allegedly been infringed;

(d) A description of the material or activity which is alleged to be the subject of infringing activity;

(e) The remedial action required to be taken by the service provider in respect of the complaint;

(f) Telephone and electronic contact details of the person complaining;

(g) A declaration that the person complaining is acting in good faith; and

(h) A declaration that the information in the notification is correct to his or her knowledge.

(2) A person who knowingly makes a false statement on the notification in subsection (1) is liable to the service provider for the loss or damage suffered by the service provider.

## *Service provider not obliged to monitor data.*

(1) For the purposes of complying with this Part, a service provider is not obliged to—

(a) Monitor the data which the service provider transmits or stores; or

(b) Actively seek for facts or circumstances indicating an unlawful activity,

(2) The Minister in consultation with the National Information Technology Authority—Uganda may by statutory instrument, prescribe the procedure for service providers to—

(a) Inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service; and

(b) Communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority

## *Territorial Jurisdiction*

Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is outside or within Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

## *Jurisdiction of courts*

A court presided over by the Chief Magistrate or Magistrate Grade 1 has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the penalty or punishment in respect of any offence under this Act.

## *Evidential Status of Electronic Documents*

**Article 9 of the UNCITRAL Model Law on Electronic Commerce** 1996, amended 1998, states that nothing in the application of the rules of evidence shall apply to prevent the admissibility of a data message in evidence on the sole ground that it is a data message or, if it is the best evidence the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. (See meaning of data message ETA)

Originally, the best evidence rule insisted that only an original document could be admitted as evidence and copies were not allowed. However, this could cause significant hardship if the original had been lost or destroyed. The best evidence rule has all but disappeared but remnants of it still remain. The courts have recognised that a rigid adherence to the best evidence rule is inappropriate in the context of the accuracy with which copies of originals may now be made. Lord

Justice Lloyd said in **R v Governor of Pentonville Prison, ex parte Osman [1989] 3 All ER 701:** We accept that it [the best evidence rule] served an important purpose in the days of parchment and quill pens. But, since the invention of carbon paper and, still more, the photocopier and telefacsimile machine, that purpose has largely gone.

# AUTHENTICITY AND EVIDENCE IN UGANDA

**Sections 7 of the Act** provides for authenticity of electronic information or a data message which must ordinarily clothe it with evidential value. It provides that where a law requires information to be presented or retained in its original form, the requirement is fulfilled by a data message if:

(a) The integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) That information is capable of being displayed or produced to the person to whom it is to be presented.

Section 7(2) of the Act provides for the following criteria for assessing the authenticity of a data message:

(a) by considering whether the information has remained complete and unaltered, except for the addition of an endorsement and any change which arises in the normal course of communication, storage or display;

(b) In light of the purpose for which the information was generated; and

(c) Having regard to all other relevant circumstances.

**Section 63 of the Evidence Act, Cap. 6 of the Laws of Uganda requires proof of documents by primary evidence (Primary evidence** is defined **under s. 61 of the Act** as meaning the document itself produced for the inspection of the court) except in the cases where secondary evidence may be admissible (Secondary evidence **under s. 62 means** and includes: certified copies given

under the provisions hereafter contained; copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with those copies; copies made from or compared with the original; counterparts of documents as against the parties who did not execute them; oral accounts of the contents of a document given by some person who has himself or herself seen it).

In light of this existing strict rule of evidence, the Electronic Transactions Act, 2011 forestalls any possible hurdles by providing under section 8 that the rules of evidence shall not be applied in legal proceedings so as to deny the admissibility of a data message or an electronic record because:

(a) Merely on the ground that it is constituted by a data message or an electronic record;

(b) If it is the best evidence that the person adducing the evidence could reasonably be expected to obtain; or

(c) Merely on the ground that it is not in its original form.

Nonetheless, subsection (2) places on a person seeking to introduce a data message or an electronic record in legal proceeding the burden to prove its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

In **Kalungi Robert v. Uganda, High Court of Uganda (Anti-Corruption Division) Criminal Appeal No. 41 of 2015** the court confirmed the admission in evidence of a compact disc that had been submitted by the prosecution after it was satisfied that the disc's authenticity is all that the prosecution had to demonstrate upon presenting it as an electronic record. The court held as follows with regard to the rules of evidence and authentication.

Section 8 of the Electronic Transactions Act waives the application of rules of evidence to deny admissibility of data message or electronic record in legal proceedings. The section however requires the court to establish the integrity of the means with which that electronic record was generated, stored, and

communicated. The same provisions are found in section **29 of the Computer Misuse Act.**

The following rules are applied by a court in assessing the evidential weight of a data message or an electronic record:

(a) The reliability of the manner in which the data message was generated, stored or communicated;

(b) The reliability of the manner in which the authenticity of the data message was maintained;

(c) The manner in which the originator of the data message or electronic record was identified; and

(d) Any other relevant factor.

Thus, in **Dian Gf International Ltd v. Damco Logistics Uganda Limited, High Court (Commercial Division) Civil Suit No. 161 of 2010** the defendant submitted evidence of an email which he sought to rely on. This was objected to by the plaintiff on the ground of its authentication which, it was submitted, could not be verified when it was sent and whether it was received. In its response, the defendant submitted that the law relied on to attack the email it sought to rely upon was a statutory rule under American Federal law and would not apply unless there was as statute in pari materia in Uganda.

Upholding the objection to the email, the court cited the **Electronic Transactions Act, 2011** and held as follows: I do not agree that the case law is irrelevant because the **Electronic Transactions Act 2011, Act 8 of 2011** applies modern practices in this case at the point of admissibility of evidence as far as requirements for authentication is concerned. Secondly the principles upon which email evidence may be admissible are analogous to the traditional grounds under the **Evidence Act cap. 6 Laws of Uganda** for the admissibility of documentary evidence.

The Court of Appeal of Uganda also lent credence to the **Electronic Transactions Act, 2011 in Sematimba Peter Simon and National Council for Higher Education v. Sekigozi Stephen Court of Appeal Election Petition Appeal Nos 8 and 10 of 2016**where it upheld electronic information obtained from the internet, holding as follows:

"We have perused **Kabakubya Bashir's** Supplementary Affidavit in support of the Petition and noted that most of the annexures thereto were obtained from the internet and he acknowledges the source of the information. We agree with the trial Judge's reliance on the **Electronic Transactions Act, 2011** to admit the annexures on the affidavit. As rightly quoted by the trial Judge, **section 8(1)(a) and (b)** provide for the admissibility and the evidential weight of a data message or an electronic record … "

An aspect intrinsically related to the use of primary evidence is its storage in the original form. It is conceived that certain regulated sectors have a requirement for storage of information in its original form. For instance, **section 6(b) of the Press and Journalists Act** requires a proprietor and an editor of a mass media organisation to retain a copy of each newspaper published by the organisation and a copy of each supplement to it for not less than ten years.

Similarly, Financial Institutions are required under section **46 of the Financial Institutions Act, 2004 Act No. 2 of 2004** to keep financial ledgers and other financial records which show a complete, true and fair state of their affairs and which explain their transactions and financial position to enable the Central Bank to determine whether the institutions have complied and continue to comply with the Act.

The financial records envisaged include any book, computer record, report, statement or document relating to the business affairs, transactions, and property of a financial institution. (**Section 46(7)).**

The records must be kept for a period of not less than ten years.

In line with the above statutory requirements, **section 9 of the Electronic Transactions Act, 2011** provides that where a law requires that a document, record or information be retained, the requirement is fulfilled by retaining the document, record or information in electronic form if:

(a) The information contained in the electronic record remains accessible and can be used for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to accurately represent the information originally generated, sent or received;

(c) The information which is retained enables the identifification of the origin and destination of an electronic record and the date and time when it was sent or received; and

(d) The consent of the department or ministry of the government, or the statutory corporation, which has supervision over the requirement for retaining the record, has been obtained.

Protecting the Integrity of Electronic Transactions

Information technology is quite prone to manipulation and abuse by its users. Where there are electronic transactions which mostly involve money, the propensity of abuse naturally increases.

To nip the vice in the bud, one of the three earlier mentioned key cyber laws specifically provides mechanisms for this. The **Computer Misuse Act was enacted alongside the Electronic Transaction Act and the Electronic Signatures Act in 2011**.

Its long title carries its key purpose where it is provided that it is an Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of

electronic transactions in a trustworthy electronic environment and to provide for other related matters.

Key terms with specific definitions under **section 2 of the Act** include:

(a) A computer which means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices.

(b) Information system which means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system.

(c) Access which means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective.

(d) Damage which means any impairment to a computer or the integrity or availability of data, program, system or information that:

(i) Causes any loss;

(ii) Modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(iii) Causes or threatens physical injury or death to any person; or

(iv) Threatens public health or public safety;

The manner of regulation under the Act is the creation of offences for different kinds of infractions in respect to the use of computers. The starting point, however, is that every person may ordinarily have authorised access to a computer.

This is in two instances which are: where the person is entitled to control access to the program or data in question; or the person has consent to access that program or data from any person who is charged with giving that consent.

With access to a computer, a person's action is likely to result into modification of its contents. Content under **section 2 of the Act** includes components of computer hardware and software. Thus, modification of the contents of a computer is deemed to take place if, by the operation of any function of the computer concerned or any other computer connected to it result into:

(a) A program, data or data message held in the computer concerned being altered or erased; or

(b) A program, data or data message being added to its contents.

So far as directly relates to electronic transactions, the following infractions amount to offences:

(a) Intentional access or interception of any program or data without authority or permission.

(b) Interference with data in a manner that causes a program or data to be modified, damaged, destroyed or rendered ineffective.

(c) Unlawful production, selling, offering to sell, procuring for use, designing, adapting for use, distributing or possessing any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performing any of the foregoing acts with regard to a password, access code or any other similar kind of data.

(d) Utilizing any device or computer program in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data.

(e) Accessing any information system so as to constitute a denial including a partial denial of service to legitimate users.

(f) Causing an unauthorized modification of the contents of any computer.

(g) Securing access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service.

(h) Intercepting or causing to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device whether similar or not.

(i) Electronic fraud which is defined under **section 19 of the Act** to mean deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

Upon conviction, the penalties for the offences listed above include fines and custodial sentences or both. The custodial sentences are up to fififteen years imprisonment. Section 27 of the Act further provides that where a person is convicted under the Act, the court must in addition to the fifine or custodial sentence or both order the convict to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the

In **High Court (Anti-Corruption Division) Criminal Session Case No. 123 of 2012, Uganda v. Sentongo and 4 Others,** accused 1 was found guilty of committing Electronic Fraud contrary to s. 19 of the Computer Misuse Act, 2011 and was accordingly convicted. To reach the conviction, the court stated that to constitute electronic fraud, there must be proof of deception deliberately performed by the accused with the intention of securing an unfair or unlawful gain through a computer network. Accused 1 was found to have been very deceptive when he created electronic ghosts gave them pseudo names and obscene rights to do anything without authorization.

Although not directly relevant to electronic transactions, **Buganda Road Chief Magistrates Court Criminal Case No. 319 of 2017, Uganda v. Stella Nyanzi** in which the accused was tried and convicted of the offence of cyber harassment which is provided for under s. 24 of the Computer Misuse highlights the intent of the government of Uganda on implementing the provisions of Uganda's cyber laws.

The jurisdiction to try the above offences is vested in a court presided over by a Chief Magistrate or **Magistrate Grade I( s. 31 Computer Misuse Act).**

Furthermore, the reach and application of the Act is to any person whatever his or her nationality or citizenship and whether he or she is within or outside Uganda as long as he has committed an offence under the Act. (s.30)

Among the powers vested in the court under the Act is to issue and order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification; and a warrant of search and seizure authorizing a police officer to enter and search any premises, using reasonable force, where an offence under the Act is suspected to have been or is likely to be committed. **(s.28)**

CHAPTER 13

# LEGAL ASPECTS OF INFORMATION SECURITY

To say we are consciously or unconsciously sleep walking into surveillance society is a question of fact because frankly speaking individuals in the society go through some form of surveillance in one way or the other. This is because there is a sense of security that is attached to surveillance and as a result individuals embrace it sometimes with the knowledge that there could be risks that come with being watched meanwhile there are others who walk into a surveillance society without any knowledge of such dangers.

Judging from past and present events that were reported in several cases, journals and articles about the benefits and dangers that accompany a surveillance society, there is a need to analyze in detail the concept of a surveillance society in order to know if the concerns of the Information Commissioner are justified or not.

## SURVEILLANCE

Surveillance was described in a report ‘as having information about one's movement and activities recorded by technologies on behalf of the organisations and governments that structured our society. Surveillance was also defined as ‘a

purposeful routine, systematic and focused attention paid to personal details for the sake of control, entitlement, management, influence or protection'. In my opinion I would say surveillance is a total denial of one's right to freedom and control of life and this is so because to be under surveillance means that almost every aspect of an individual's life is been watched, monitored and controlled by others who consider themselves superior and thereby deny people of their right to privacy and control of different aspects of their lives.

Professor Ian J.Lloyd in his book 'Information Technology law' said that as individuals in a society we go through different types of surveillance and made reference to Alan Westin who in his seminar work 'Information Technology in a Democracy' identified three types of surveillance as follows;

1. physical surveillance
2. psychological surveillance and
3. data surveillance

Physical surveillance is a form of surveillance that involves the watching and monitoring the acts of individuals in a society and can be carried out with or without the use of surveillance technologies for example the use of spies and spooks whereby a person is being followed and watched by a private investigator or security agencies and has been said that such surveillance can only be used applied to a minimum amount of individuals.

Psychological surveillance on the other hand involves the use of surveillance technologies to monitor the activities of individuals in a society by the use of interrogations i.e. asking questions in order to extort information either with the use of torture, personality tests e.t.c and this form of surveillance often violates the rights and privacy of individuals in a society.

Data surveillance which is the third form of surveillance involves the use of one's personal information to monitor their activities because also everything we do as individuals gives out some form of information about us and if not used

properly by the data controllers and for the right purpose could end up posing great risks and dangers to lives of individuals in a surveillance society and I am of the view that ‘data veillance' is the most prominent form of surveillance that is being used in our present day societies due to the fact the almost all countries are technology compliant and as such the movement of personal data can be carried out with ease with the use of devices such as the computers, telecommunications and so on.

Having looked at the various forms of surveillance that are present and being used in our society today, I will then go further to explain the how we as individuals live and co-exist in a surveillance society looking at the different types of surveillance technologies and how they are used to control the activities of individuals in a surveillance society.

## *Living In a Surveillance Society*

The idea of a surveillance society arouse from the fears of the government and people as regards the reoccurring danger and threats to lives of individuals coming from past events like terrorism, high crime rates in the society such as fraud, armed robbery, shop lifting e.t.c. In other to have a degree of safety and find solutions to these problems, and as such certain measures and forms of surveillance were introduced in other to provide security, but we forget to ask whether these solutions are even appropriate and there might be more less invasive answers and as a result, individual's right to privacy and anonymity are infringed on but we don't see that because of our fears with risks and dangers, rather than with more positive social goals and has closed our eyes to the dangers and consequences of living a life under surveillance.

The United Kingdom (UK)is an example of a country that is fully compliant with the idea of a surveillance society because almost every aspect of their lives starting from taking a walk on the streets, driving their cars, taking kids to school, going shopping in the supermarkets, going to the hospital and even in their work place they are under surveillance and this is so because the UK is a highly technological developed country and as such has access to a lot of

surveillance technologies that can be used to monitor and control the activities that take place in the life of their citizens and has also been described as the most surveilled country with more CCTV cameras but the irony of this is that it still has loose laws on privacy and data protection.

In Britain there are about 4.2 million CCTV cameras, one for every fourteen people that means that an individual's activities can be captured by over three hundred cameras a day, it was also accessed by reporters to have the biggest DNA data base with over a million innocent peoples data or information on it some of which they are aware of and some of which they are not and with the advent of new and improved modern surveillance technologies being introduced individuals will be subjected to even more surveillance than they are going through today.

A surveillance society is not a total bad concept in the sense that it has its advantages and its disadvantages but the important thing is to weigh which one carries more weight after which we can decide the way forward. Some of its pros are that it provides security and prevents the people from computer hackers, terrorists, threats to public security e.t.c. Another one is that it helps in improving services like healthcare and it makes our daily lives more convenient such as paying bills because of the different forms of technology that are being used.

Having said a little about to pros of a surveillance society let us also look at some cons with the mindset that I intend to delve into it in a more detailed manner later in this work. The first one which I consider the greatest negative effect of a surveillance society is that it is a threat to the privacy ofindividuals in a society even though we seem to be more concerned with our fears and in the process over look the possibility that being fully dependent on surveillance technologies for safety could end up being of more harm to us than good. Another one is that surveillance yields lack of trust and raises suspicion between citizens, and citizens and the state in the sense that if we both have nothing to hide or if we are not looking for something to use as weapon against ourselves, why do we as individuals in a society always feel that there is a need for us to

control and monitor our activities. This few positive and negative effects that I mentioned above is just a brief insight into the effects of a surveillance society in our lives but for now let's take a look at a some surveillance technologies and how they are being used to control our lives in the society today.

## *Surveillance Technologies*

There are different kinds of surveillance technologies that are used in our society today which can also be summarized under the different forms of surveillance as I have spoken about earlier and the reason for this is that it makes it easier for both we the individuals also known as ‘ data subjects' in relation to ‘dataveillance' and the state who are said to be the ‘data controllers and processors' to be able to monitor and control our activities in an easy and efficient manner in the sense that such technologies can performs different activities in accordance with the particular purpose for which they were made. Some examples of surveillance technologies includes as follows;

Video surveillance i.e. the use of Closed-circuit Televisions (CCTV)

(a) Telecommunications surveillance

(b) Biometrics

(c) Shop Radio Frequency Identification (RFID) tags

(d) Loyalty cards

(e) Internet cookies

(f) Data flows

(g) Locating, Tracking Tagging technologies

(I) London Oyster cards e.t.c

**Video Surveillance**

This form of surveillance is considered the most popular kind of surveillance technology that is used in a surveillance society because it in the use of CCTV camera and its function is to be able to capture the image of individuals in a society while going about with their activities with the aim of preventing crime. CCTV cameras are devices that are actively been used in Britain today in the sense that almost everywhere you go, there are cameras watching you and as such uses a lot of money on the production of these cameras and it has been predicted by experts that by the year 2009, theywould will spend up to 642 million on video surveillance software which in the year 2004 cost them 147million and has not helped in solving their crime rate.

**Telecommunications Surveillance**

This involves the use of technical equipment such as Global Positioning System (GPS), tapping of phones by the police or security services and it involves communication and the exchange of data and information which is enabled by large scale digital and computing systems such as the internet.

**Biometrics Surveillance**

Biometrics is another very common surveillance technology that is really being used in our society today because in most big organizations, embassy, airports e.t.c and it is a form of identification that includes body trace e.g. fingerprints, iris scans, facial topography and hand scans which are all used on different passports and I.D card systems. Biometrics has also been predicted to cause UK a healthy sum of 4.7 billion industry in 2009 which initially in the year 2003 cost 675 million and this is so because of the creation of more sophisticated surveillance technologies like smart cameras to iris identification all with the belief that there will be accuracy in identification and crime will be reduced.

**Radio Frequency Identification Technologies (RFID)**

It involves the use of radio frequency communications as a way to track goods as they move through the supply chain. RFID are embedded into products, pallets and cases thereby enabling the RFID readers read information from those tags.

**Data Flows Surveillance**

This is a very sensitive form of surveillance in the sense that it involves data that is gathered by surveillance technologies and it flows around computer networks and has been described by ‘Clarke R 'as ‘dataveillance' which is ‘the systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons'. In most circumstances of data subjects consents to giving their data, but what now happens in a situation whereby the data is transferred elsewhere and there is no idea as to where the data goes by either the public or data sharing agencies. In such a case one tends to wonder if we can say we have confidence in the state as regards the safety of our data.

With the use of these technologies you can see that in a surveillance society ones live can be monitored in its entirety in the sense that everything you do has one form of surveillance technology which can be used to track you some of this other technologies include Global Positioning System(GPS) which can be use in tracking your precise location, loyalty cards which can be use to determine your capacity in shopping and as such marketers know how to target a customer based on his or her spending habits and even the internet can be monitored because every individual leaves trails when browsing the internet and this trails are called ‘cookies' which are left on a user's machine which recognise the machine when it next visits that site thereby making the activities of user traceable.

There are also non-technological means of surveillance of surveillance which we practice as individuals in the society such as eavesdropping, watching, use of human spies and many others but these methods due to the advent of technology and modernity are gradually fading away because they are looked upon as effective as the technological means do. This is as a result of a belief that surveillance technologies will provide faster means of security ,safety and

certainty and instead of individuals to also have in mind the dangers and consequences that this surveillance technologies could have on their lives because all this forms of technologies involve the transfer of personal data from one data base to another which could also move from country to country and could eventually fall into the wrong hands thereby defeating the whole reason for their use in the first place.

That leaves us with the question of how effective are these surveillance technologies to our lives and to what extent can we say that they have made more of a positive impact on our lives than the negative ones.

## *Negative and Positive Impact Of Surveillance On Our Society.*

A surveillance society has its negative and positive impacts on our lives as individuals in the society but the negatives impacts are greater than the positive ones and this is so because surveillance in the information commissioners report it was brought to my knowledge that the surveillance society has a way of setting traps for individuals in a society and this traps includes;

- Thinking that surveillance is a product of new technologies and
- Thinking of surveillance as a malign plot hatched by evil powers.

Ones an individual's looks at the concept of a surveillance society in this light then it is easy for one to fall into the trap of a surveillance society and the dangers that it poses to how lives.

Apart from a sense of security, safety, minimum amount of risks ,swift flow of goods, people and information which we as individuals believe are the positive effects of surveillance on our lives, what other way can we really say that a surveillance society has improved our lives or limited the risks and dangers we go through every day because irrespective of all the different forms of surveillance both technological and non-technological means, it still in my opinion has not kept us out of harm's way and has been described in many reports, articles, journals and so on as been a failure and is in fact the source of most of our problems instead of a solution because today in the UK for example

with all the millions of CCTV cameras everywhere, the level of crime on the streets are still high, terrorists are still attacking innocent people, individuals personal data are still being used against them and so on and this is all thanks to surveillance.

Surveillance creates room for suspicion and lack of trust in the society because why should employers feel there is a need to monitor the affairs of their employees at all times by monitoring their actions at all times, bugging their cell phones, putting tracking devices in their cars company vehicles, storage of employees personal data, making them under certain medical tests and answering personal questions about their lives which could be used against them in the future for instance if an employer was to find out that an employee is suffering from a medical disease, it cost that individual his or her job and may even affect them elsewhere if such personal information was to leak.

Surveillance exposes individuals in a society to harm in the sense that we as individuals don't know sometimes who is watching us and what purpose our data is being used for because in the UK and the world at large, we still do not have competent and secure data protection laws that would secure our database from unauthorized access or leakage and therefore leaving us in harm's way if our personal data was to fall into the hands of the wrong person in the sense that even those people watching us could be a threat to us instead of providing us with security.

Surveillance encourages social discrimination as to race, ethics and class in the sense that sometimes our personal that is being used to determine the level of surveillance we get in the society for example the minorities in a society when it comes to movement from one country to another tend to be scrutinized more than the elites and this could result in their being denied visas to move around the world and another example of this is in a movie titled' 2012' which was a movie about the world coming to an end as a result of a ‘natural disaster' and the state who are suppose to be the guardians of the public and provide them with security and information being that they have their personal data, informed the elites of the society of this terror in time and offered them protection of their

lives for a certain amount which they could pay and where ready to leave the minority or lower class to die just because they don't have such resources. This is a high level of social discrimination because how can our so called data protectors claim to have all the surveillance different surveillance technologies at their disposal and still not be able to provide people in a society with a minimum amount of security.

Surveillance encourages deceit and dishonesty and function creep in the sense that the data controllers tell the people that they need their data for a particular purpose and end up using such data for another purpose. Also surveillance technologies help to marketers to manipulate customers data in the sense that the use of ‘Loyalty Cards' which is common in the UK helps producers and marketers to be able to monitor the resources of a customer by their shopping habits and as such they come up ways to direct marketing to that customer in order to make profits and this is wrong.

Another negative effect of a surveillance society which I consider to be the most crucial is the infringement of one's right to privacy and the total loss of an individual's anonymity in the society. Privacy is a fundamental right of every individual in a society but you find out that in a surveillance society, it is not possible for one to exercise that right because everywhere you go, you can't be anonymous because there are either cameras watching in on the streets, offices, shops even in your car you are being watch and as such the whole idea of privacy and anonymity has been defeated.

This and many others are the effects of surveillance on our society today most of which are negative than positive and I must said that our regulatory bodies with regards to surveillance still have a lots of work to do with regards to the surveillance society try to come up with more effective ways in which they can grant us more confidence that our society is safe as a result of being under surveillance.

The Right To Privacy In Relation To A Surveillance Society.

The issue of the concept of Privacy in relation to the context of a surveillance society has been one of

great contention in my mind because I am of the view that an individual's privacy in a society is aconstitutional right which should not be infringed on but it seems like there is no way that individuals in a society can be under surveillance and exercise that right over their lives.

There is also no way that one can talk about the surveillance society without the issue of privacy. Privacy and surveillance cannot co-exist together without one being a hindrance to the other because a surveillance society cannot function properly without crossing the path of privacy and the concept of privacy cannot be practiced within a surveillance society and this poses as a dilemma to us as individuals in the society because we are now left with two option which are as follow;

- Choose Surveillance and forego your privacy and
- Choose your Privacy and live with the possibility of being exposed to danger and risks at any time

Having been giving this options what choice can we make from the two because either way it seems like you will be losing something important. In light of the above will then go further to analyze the different definitions of privacy and relate it to the present day surveillance society and see how far we have gone.

# DEFINITIONS OF PRIVACY

Privacy was defined by Judge Cooley in the year 1888 as ‘The right to be left alone ‘another definition of privacy by some writers in the report defined privacy as a matter as;

‘The right of the individual to be protected against intrusion into his personal life or affairs or those of his family, by direct physical means or by publication of information'

Privacy which is very important in a individuals life in the sense that it is the only form of dignity and pride that any individual has and if no laws made to protect this right people in a surveillance so will seen just become like ‘puppets' in the society whom have no form of control what so ever as to how their personal data and information are being used and manipulated by the ‘Puppet masters' also known as the ‘Data controllers' as they please which could be dangerous to individuals in the society.

**Article 8 of the Fundamental Human Rights and Freedoms (Convention), 1985** provides which was ratified by the Council of Europe provides that;

1) ‘‘Everyone has the right to respect for his private and family life, his home and his correspondence.
2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety of economic well-being of the country, for the prevention of disorder or crime, for the protection of health morals or for the protection of the rights of freedoms of others."

This convention as of that year was not a confirmed law and as such so its provisions could only be confirmed in European Courts and because UK was a signatory for the Council of Europe, the Convention applied to the UK but in 1998 the Human Rights Acts (HRA) was enacted in the UK and were incorporated into the UK law and a more recent Law was enacted in 2000 in charter 7 of the Fundamental rights of the European Union which provided for right to privacy in respect to modern day communication."

Despite all these laws in relation to privacy there are still many issues in relation to surveillance and privacy as will be discussed below.

# ISSUES OF PRIVACY IN RELATION TO A SURVEILLANCE SOCIETY

A surveillance society is a huge area of contention in relation to privacy in the sense that it affects an individual's privacy in every aspect of their lives e.g. privacy in relation to health, employment, press, race, ethics, finance, reputation e.t.c.

Eric Barendt in his book **Privacy and the Press described** the fight between surveillance and privacy as (‘Political') in the sense that the ‘prominent figures mostly politicians, celebrities, members of the royal family are trying to protect their lives from media scrutiny meanwhile on the other hand the press which is surveillance in this case is fighting to retain their liberty of publication'

He was also of the view that ‘privacy is a fundamental human right that should not be Infringed on either by the government, business, individual or the media"

As individuals in a surveillance society we need to have the right to preserve our privacy but if our actions keep on being monitored all the time either by technological or non-technological means of surveillance this aim cannot be achieved because everything we do in a surveillance society leaves a trail behind that can be traced back to us and also joint with the fact that our personal data is constantly being transferred from one data base to another and processed by different processors makes access to our personal information easy for people.

In the case of **R v Brown,** Lord Hoffman passed his judgement stated that, ‘Privacy which is the right to keep oneself to ourself,to tell other people that certain things are none of their business is under technological threat due to the different and various types of surveillance e.g. surveillance cameras, telephone bugs e.t.c that are used by individuals in the society today.

Also in the case of **Leander v Sweden**, Mr Torsten Leander was denied employment as result of his personal information which was held in a register and was revealed to his employer without the knowledge of the kind of information that was kept about him and for what purpose it will be used for and

this constitutes a breach of his right to privacy provided for in Article 8 (1) Fundamental Human Rights and Freedoms (Convention).

In the case of **Campbell v Mirror Group Newspapers** which relates to privacy and the press in the sense that taking pictures of Miss Campbell right to privacy was breached when the this media house published photos of her leaving Nacortics Anonymous which was a facility where she used to attend therapy as a result of her drug addiction. She appealed on the grounds of breach of confidence by the media and which is one of her fundamental human right and against the provisions of the Data protection Act (1998). The court of appealed was against the verdict of the case but on appeal the House of Lords passed judgement in her favour which also gave rise to other opinions concerning the extent to which ones privacy can be said to have been breached and this is as a result of the fact that there are no unified laws that protect individuals privacy in the society because what might constitute privacy in one country may not be viewed the same way in another country.

In a more recent case of Craxi v Italy judgment was passed and it was established that there was indeed an infringement of **Article 8 of the European convention on human rights** in the sense that even though Mr. Craxi was guilty of committing certain offences, it was held that:

'the state failed to provide safe custody of the transcripts of telephone conversation which Were presented as evidence before the court and to subsequently carry out an effective Investigation as to how those private communications were released into public domain"

This and many other issues reflect the gradual and total loss of our right to privacy and anonymity in a society because irrespective of the different Laws that have been established in our society today can we honestly say that they are protected our personal information from the dangers of a surveillance society such as globalization, the internet and the continuous invention of new technologies by virtue of new modern discoveries.

## *Regulations.*

It is a known fact that a society cannot exist without laws and supervisory authorities or bodies that would regulate the actions and behaviours of individuals in a society. In a surveillance society most especially there is a great need for laws and bodies to be established in other to oversee and supervise the way our personal data is being used and transferred from one place to another because without people watching those who process our data, there is a risk of danger to us as individuals in the sense that our information could be manipulated and used against us if it were to fall into the hands of the wrong person, we could be subject to blackmail by criminals, discrimination to our person for example if medical data about an individual who has a disease such as "HIV" or other deadly diseases was to leak, such a person could be subject to social discrimination and stigmatisation to his person, reputation and so on.

As a result of this, different countries have different supervisory authorities who possess some powers to ensure that our privacy and lives are protected in a surveillance society. Article 28 sub sections (1) and (2) of the data protection Directive provides for the establishment of these supervisory authorities and their powers. In the UK we have the information commissioner meanwhile other member countries except Germany have a single supervisory authority who supervise the affairs of their personal data.

Different Laws have been enacted and put in place in our society today so as to make sure that our personal information is protected but these laws have their strengths and weaknesses and cannot be relied on completely by in individuals in a surveillance society. Most of this law are guided by some basic principles such as;

(a) Personal data must be processed fairly and lawfully.

(b) Personal data should not be use for any purpose other than the purpose it was obtained for.

(c) Personal data must be accurate and kept up to date.

(d) An individual must be informed of when personal data about them is collected.

(e) The purpose for which personal data was obtained should be stated.

(f) The consent of the individual must be obtained before obtaining their personal Information

(g) Individuals must be told how their data will be protected from misuse.

(h) Individuals should be told how they can access their data and should be able to verify Its accuracy and request changes where necessary and so on.

These and many other are the basic fair information principles(FIP) the regulate the control of our personal data in a surveillance society these principles exist side by side with some other laws in controlling the use of our data some of these laws include those discussed under the section on the right to privacy and data protection.

## *Recommendations*

Judging from the analyses of the concept of a surveillance society it is true to say that there is still a lot of work that needs to be done in other for individuals to have full confidence in the state and surveillance technologies this is because many of these surveillance technologies and tools have turned out to be failures in one way or the other such a CCTV cameras displaying wrong images of people thereby causing harm to innocent citizens, loss of individuals personal data as a result of improper storage in data bases, personal blackmail to an individual life due to poor data protection facilities which eventually causes more harm than good to the individuals in the society.

The following are a few suggestions that may aid in helping to solve or at least reduce the threats and dangers that a surveillance society poses to an individual which are as follows;

The use of cameras should be regulated on a statutory basis in the UK with a legally binding code of practice governing their use.

More powers should be given to the information commissioner.

There should be better regulation of the DNA data base and reassessment of time samples are held.

Introduce privacy impact assessment for new data collection schemes

There should be a judicial oversight of surveillance.

There should be more transparency as to how data of individuals which were collected are being used and they should be told who is watching them, why and what information is being captured.

More powers should be given to the information commissioner to carry out inspections on private companies.

There should be proper implementation of laws and the guarding of people's rights as human beings

Provide law enforcement agencies with tools to protect the public while ensuring there are effective safeguards and a solid legal frame work to protect civil liberties.

CHAPTER 14

# CLOUD COMPUTING

## INTRODUCTION

The legal and regulatory landscape around cloud computing is by no means static. Cloud computing that employs a hybrid, community or public cloud model "creates new dynamics in the relationship between an organization and its information, involving the presence of a third party: the cloud provider. This leads to new challenges in understanding how laws apply to a wide variety of information management scenarios and to the different parties under these various scenarios.[231]

Currently it is very difficult for organizations to survive without the support of information technology, which enables a great improvement of business competitiveness.

With the growth of internet speed, business learned the need for a more quick and efficient interaction with clients. So, companies started to focus on their core business, leaving other activities to third parties. Cloud computing is a good tool for companies to accomplish such a goal.

At this point in time, cloud computing is widely used by big companies. It offers more advantages than disadvantages to companies, allowing them greater productivity, great data processing power and cuts desk costs.

In addition, cloud computing also allows IT companies to store and process their data remotely. Data can be retrieved anytime and anywhere through simple devices such as smart phones.

There are several services offered by the cloud providers, such as the storage of files, backups, provision and management, and software updating and service support.

However, in order to assure the security of the information, it is important that data is not accessed by third parties, including competitors, government and non-allowed users. Thus, regarding the security of information, it is important that the service provider pays strict attention to client identification, to the use of encryption and the security of the whole infrastructure.

In order to maintain the legal certainty of the stored content it is essential to have a comprehensive business contract between the provider that offers the service of cloud computing and the client who uses the service.

The areas that require attention in this area include:

1. ICT contracts, and more specifically for Software as a Service
2. Protection of data and privacy
3. Regulatory frameworks
4. Responsibilities of the different parties
5. Data security

# CLOUD COMPUTING AND THE INFORMATION SECURITY CONCEPT

Cloud computing and its concept have evolved significantly in recent years.

Initially, data was stored inside the company's own computer systems, with no possibility of external storage neither remote access.

Subsequently, data began to be stored on a computer of external company, outside the corporate environment, the so-called data centers - often outsourced services.

They had several servers, which enabled the storage of large volumes of data, including the data of more than one company.

Nowadays, the storage service has evolved considerably, allowing us to store important corporate data in the clouds. Thus, authorized corporate users access information easily from any location, at any time, via mobile devices.

Large organizations or large regional providers, such as Google, Amazon, Microsoft and HP, offer those services. However, the growing fear for leakage and unauthorized data access is noticeable.

Many theorists claim as the most relevant definition of cloud computing the one issued by the National Institute of Standards and Technology-NIST:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Mell & Grance, 2011, p. 2)

Finally, cloud computing is a service offered by a company to natural persons or client companies upon an atypical contract, which has as its object, services such as storage, processing and backup content, providing customized applications and others on the server contractor, allowing the client or other authorized

person to have secure access from anywhere, anytime, through any mobile device.

## *Some advantages and risks of cloud computing*

There are many advantages of cloud computing, but biggest advantage is the fact that there is no need to worry about complex tasks of indexing data, and thus the client company can focus on its core business and consequently be more competitive, efficient and profitable.

The benefits from the enormous processing power that it is offered by the provider of cloud computing services are growing. The client company does not have to invest a large amount of capital in hardware and software, maintenance and upgrade, neither in the management of information technology.

Consequently, another important point is cost reduction, which allows the allocation of capital in the core business.

Cloud computing relies mostly on the internet, which is already available to most large companies.

It is also important to mention the ability to optimize data processing. In most cases large companies fail to utilize much of their IT during off-peak times.

In this way, the underutilized resources are offered to another organization that is demanding on that moment, without delays to other companies. Thus, the service provider can optimize the resources available from one company to another, depending on the demand that occurs at that moment.

Cloud computing also enables the employees of the client company to use the information and data anywhere in the world, at any time and on any platform (mobile or not). In the past it was common to find enterprise environments with their own providers. By accessing cloud computing, the collaborative work is strengthened, and it allows the employees of various areas of the organization to access and modify documents 24 hours a day, 7 days a week, regardless of where they are.

Seasonal or cyclical businesses that do not constantly need large processing capacity can hire the services of cloud computing for a specific period. According to their needs it can be done without major investments in personal computing, and without hiring an overestimated computer service.

Regarding data safety, the risk of data loss is reduced with cloud computing service, since there are many processors at work and there is a specific structure of hardware to perform periodic backups. The service provider can also be held responsible for the loss of data. However, this issue must be properly addressed in the agreement. In addition, the traffic of peripheral equipment with business information (e.g. thumb drives), some of them with possible highly confidential content. This could jeopardize the whole business strategies, but such a risk is reduced with the implementation of cloud computing.

Another advantage of cloud computing is the energy efficiency related to the companies that adopt this system. The amount of energy expended by a cloud computing service (which is a large center of storage and data processing) is lower than the amount expended by several centers of traditional data processing. The cloud computing servers have energy efficiency programs and seek to consume clean energy or are installed in locations where the temperature is low, to reduce the use of chiller machines.

Last but not least, the availability must be addressed. As to the cloud computing hardware, if a failure occurs, the machine is automatically relocated in a matter of seconds, which makes the impact (downtime) imperceptible - there is no harm to the company core activities.

**Risks.**

There are some disadvantages in the use of cloud computing, such as the possibility of information leakage. Therefore, it is essential that the staff responsible for contracting the cloud computing service performs detailed analysis, seeking to maximize the guarantees offered by the service provider.

Companies interested in cloud computing services should keep in mind that they might not have exclusive control over the data stored in the cloud.

There is also the risk of loss of data and sensitive information by the contracting company, which can have directly impact on the company results. Therefore, it is important to know the backup plan available by the service provider, but many providers refuse to inform it, stating that it is confidential information.

Another critical point of any service cloud computing is data security (including privacy), especially in these days with so many issues relating to leakage and theft of contents being addressed.

In terms of information security, many topics can be addressed, among which, the integrity and updating of systems, protection of stored information and information in transit, besides data recovery procedures against disasters.

These issues can be addressed in the cloud computing contract as well as in the Service Level Agreement (SLA), which should appear as an attachment of the contract.

Regarding the reliability of the stored content it is important to emphasize that the provider may be required, by court order, to make such content available or to disclose it even if the contract has a specific clause of reliability. Thus, it is important to make the client company aware of the data protection legislation of the countries where the content is processed and stored.

The location of the servers that store and process the contents of the client company shall also be verified, because such data may be stored or processed in one or more locations, which can later cause problems for the client company.

The actual availability of the internet is also important. Due to the growth of internet usage and the migration of many computing resources to the cloud, flaws that preclude access to part or all of the content stored in the cloud may occur. Unfortunately interruptions have been more than desired. It generates damages to the client company, which has a direct impact on its revenues.

Finally, cloud computing has evolved considerably, including bringing new services to client companies and natural persons. Along with this evolution many strengths and opportunities for improvement have emerged, which should be carefully evaluated by potential client companies which want to use cloud computing service.

## *Deployment Models*

The basic deployment models are: private cloud, public cloud, hybrid cloud and community cloud.

Private cloud (or internal cloud), is typically the first step of a large company. It is one whose infrastructure is acquired and managed by the client company itself or by a third party, but operated exclusively for the benefit of that client company (exclusive use of the company and authorized users).This type of cloud is costly for developing, deploying and for maintenance. This cloud can be hosted by the company itself or by a service provider.

Despite the minimal dependence of the company that uses this model with respect to other companies, the service will be subjected to the public internet service, since the internet is necessary for accessing the cloud. Private cloud presents a main advantage in higher security control.

A community cloud, usually the first step undertaken by small and medium businesses, is shared by several companies with common principles and interests, as, for example, security requirements and policy. Such a service may be administered by any organization that is a part of a consortium.

The hybrid cloud has its structure composed of more than one type of cloud. The private cloud, for example, may have its resources increased from the resources available in the public cloud. In this case the desired level of service can be maintained even if there are rapid changes in the resource needs of the client.

## *Models of Service*

As for service models (or business), researchers emphasize three main models of cloud computing service: Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). (Valenzuela&Montoya, 2012, p. 31-32)

It is noticeable that each service model entails different legal responsibilities by the service provider and regarding the client.

Thus, it is important that those provisions must be included in a computing service contract, and all information related to the ability of the service should also be included in this document.

It is also noticeable that there is a trend to create new models in the future, according to the growth of the services offered by cloud providers.

## *The Services Provided By Cloud Computing Companies.*

The main services offered by cloud computing companies are the storage and processing of files, backups and the availability of software.

As to data storage cloud service providers ensure that one can store any type of files such as text, spreadsheets, music files, photos, and presentations, among others, assuring reliably, full availability and low cost.

Besides the storage, management and the updating of applications are also some services offered by cloud computing providers. They also allow the employees of the contracting company to access software and information they need. This avoids unnecessary expenditures on the acquisition and continuous updating of applications used by company employees.

There are also cloud computing providers who are willing to develop applications accordingly to the needs of the contracted third parties. This service is tied to the upgrade, maintenance and management of the customized application which will be available in the cloud.

Another service offered is the reliability of the data and information available in the cloud. Undoubtedly, no cloud computing provider can guarantee 100% reliability, but can reduce the instability of the information system. Goals of service stability and sanctions, in case the indicator will not be achieved, should be addressed in the terms of the service agreement.

Moreover, cloud computing providers usually offer support by their own technical staff. With cloud computing, technology employees of the client company tend to be reduced. It is important that the service provider offers available support, over telephone or physically, aiming to remedy any operational problems or questions, especially those that cannot be solved by the internal IT staff of the client company.

Thus, it is noticeable that there are many possibilities of combination of services to be contracted, and, of course, other customized services may also be developed. The optimal configuration of services varies from organization to organization and must be analyzed in detail.

The market for cloud computing is expanding rapidly and offers great business opportunities. Accordingly, companies wishing to make use of this technology should consider what services they really need. In the manner indicated, they will enjoy those that offer more advantages to the various types of business enterprises.

## *The Contract of Cloud Computing.*

The relationship between cloud providers and their customers generate wealth for society, but can also generate conflicts, mainly because it involves a service of technology and information security. Regarding large enterprises, focus of this study, a clear and well-written contract is more important due to the great amount of data and sensitive information to be managed. Such data is related to customers and employees information. Generally, when the customer is a large organization, the service contract can be customized, aiming to supply its specific goals and objectives, which does not occur when the customer is a

natural person or a small business. Such clients are subject only to the provision of a standard service, without any of the adaptations, which will be detailed later.

Moreover, the contracts signed by large corporations, as all types of contracts, requires the presence of basic details, as the names of contracting parties and the object of the service to be contracted. However, a previous detailed analysis of the important requirements for both contracting parties must be done. For example, some items are to be discussed previously: the privacy of information, interruption in service provision and data security.

Generally, bigger users, particularly from regulated industries, try to negotiate more. Some even require contracts to be on their standard IT services or outsourcing terms, on a 'take it or leave it' basis.

As to the will externalized in a contract by the customer:

Quanto maior o afluxo constante de novas e mais sofisticadas tecnologias, tanto menor sera o poder de reflexao e a possibilidade de se externar uma vontade racional, pois esta sera apenas uma vontade distorcida pela pressao psicologica, expressando, por consequencia, muito menor do que deveria ser, pois incapaz de externizar a verdadeira liberdade contratual. (Rohrmann & Machado e Campos, 2009, p. 70).

This is easily seen in consumer contracting, where in most cases, consumers sign contracts online without analyzing them in detail or even without reading them. They do so because of the need to access, for example, a particular content or application. Some of them explain that they do not understand contracts in general, even a contract involving technical terms related to technology. Consumers mostly sign electronic service contracts without reading the terms.

## *Contractual Parties*

With regard to the parties that constitute the contract of cloud computing, they are identified as the supplier of the service or Cloud Services Provider (CSP) and the client company (or a natural person) that will use the cloud storage.

The client is interested in the services offered by the service provider and is willing to sign the contract for cloud computing, aiming to benefit from the service upon payment (free service can also be provided).

The client may be a natural person or a legal entity, which directly influences the possibility of discussion and negotiation of the contractual clauses which are being studied at this point in the process.

Large companies, including banks and public corporations have more power to discuss such clauses. This way, they are able to customize, at least in part, the contract of cloud computing.

However, contract customization is difficult when it refers to a natural person or small and medium- sized companies. They generally enter into contract without modification, i.e. an adhesion contract.

It is noteworthy that this type of agreement can be celebrated online. It will probably be difficult to find few suppliers willing to negotiate the terms, even if the other party is a great company.

Usually a cloud service provider is a legal entity. However, a natural individual can also perform the task of a cloud provider, since they have the infrastructure and other necessary resources. Nevertheless, in the survey conducted for the preparation of this study, individual cloud providers were not found worldwide. Generally cloud computing providers are large multinational companies.

## *Object of the Contract*

In cloud computing contracts the detailing of the object must be written accordingly to the service model to be adopted. For example, the object of the provision of application (SaaS) is different from that one detailing only the provision of the infrastructure (IaaS).

Anyway, it is very important to emphasize the significance of the description of the object of the contract.

The description and the scope of the object of the contract are, in practical terms, determinants on the technical scope of the service to be provided and the content of the obligations of the parties.

Therefore, clients that will use the service should pay attention not only to their needs, but also to the terms of the service contract. Such a document regulates the relationship between the parties and will clarify the scope of the contracted service in the case of future litigation.

To use a program or an online service in the online world, the agreement terms of the supplier must be accepted. This also occurs with cloud computing, in which the client must agree to the terms of the service agreement submitted by the supplier.

Usually when clients of cloud computing services are large companies, some terms are widely discussed and negotiated. However, for small and medium sized businesses and consumers, service providers offer their service as packages and standard contracts. For example, when a consumer registers in an information store service in the cloud, such as Mega, she clicks accepting the terms of service and there is no room for changing any of the contract clauses.

Whatever the type of contract of cloud computing, such contract should always be as clear as possible. It should also be interpreted in accordance with the intention of both parties, with preference to consumer protecting policies.

In addition to the various clauses that can be part of the cloud computing contract, such contract should also be drafted considering the client's business, the type of customer (industry or government, individuals or companies; small, medium or large corporations, for example). The contract also should be suited to different models (public cloud, private, hybrid or community) and service (IaaS, PaaS and SaaS).

The European Network and Information Security Agency ENISA (2009), a center of excellence in network security and EU information, identified some issues that must be addressed in terms of cloud computing contracts: data

protection, availability and completeness, minimum standards of security, confidentiality, intellectual property, professional negligence and subcontracting and exchange control services.

Therefore, there are many contract terms, and some are more relevant in certain models of service and business than in others. This text addresses some clauses considered most relevant in the cloud computing contracting.

Some contracts are not denominated Cloud Computing Contracts, but Terms of Use (usually between natural persons or small businesses), Terms and Conditions, or even are part of the SLA.

There is no doubt that the typical contract clauses must be included in any contract under study, as the complete qualification of the parties and their legal representatives, place of celebration, duration and renewal. Other important clauses are price and terms of payment (date, form of payment, bank transfer, implications of non-payment of monthly fees, late payment fees, suspension and cancellation of services).

However, some of the agreements refer to the Privacy Policy, the SLA or the Policy for Use of cloud provider, which form a part of the contract. Some contracts have focused on consumers and small- medium enterprises, and refer to the Terms of Use, the SLA, the Privacy Policy and the Acceptable Use Policy.

As for software, the contract must regulate its support, maintenance and updating, in addition to the responsibilities of the parties. In contracts involving large corporations, usually software may be developed as a customized computer program.

The provision of service availability is especially important for the enterprise customer. Usually performance indices according to the efficiency of the provider are established around 97% or 99%. Furthermore, some providers contractually describe exceptional situations which might not provide the service, such as power outages, fortuitous events or public internet service interruption.

Schedules for performing maintenance can be provided in a clause of availability, as well as improvement and updates by the cloud computing provider, thereby generating the least possible impact on the client company activities.

The integrity of the content regarding storage and preservation is linked to the liability of the cloud service provider.

Many service providers do not allow the inclusion of a contractual provision regarding security against loss of data, especially those who provide free cloud services. In this case, at most they are committed to make the "best effort" to maintain the integrity of information in the cloud, which means that if any loss occurs they are not held accountable.

Eventually server failures take place in the cloud, even though the service providers might not confirm such events. One way to minimize the impact of failures is to guarantee contractually that the content of the cloud will be stored in different virtual machines, thus reducing the risk of loss of data.

The protection and privacy of content stored in the cloud should be mandatory in all contracts for cloud computing, because if there is no contractual provision in this regard, theoretically the supplier could even sell third parties data (of course depending on the legal regulation of the jurisdiction regarding personal data).

In some cases, data protection is subject to specific and detailed document that is part of the cloud computing contract, which reinforces its relevance.

To reinforce the privacy of the data stored and processed in the cloud, the client company can contractually require the service provider to record the activities (logs made with date and time) during a specified period. This policy will enable a rapid and accurate response in case of an incident, because the logs can be available easily. However, those logs should never be changed by any party. It can also be agreed that the service provider will conduct random testing on the availability of logs and send the result to the other party.

It can also be discussed between the parties to provide a clause stating that the client company will be notified of legal and administrative requirements for content delivery; in this clause it would be stated what was available, when and to what legal authority. Exception should be made in cases where the legal authority prohibits such communication is performed, for example, when it is necessary to maintain the confidentiality of a criminal investigation.

Another important clause is the confidentiality, whereas employees and subcontractors of the cloud provider may have access to sensitive client company information, due to the performance of their function (maintenance, administrative, technical and other). Generally providers seek to make the other party aware of this issue. Some providers demand that contracted staff and outsourced service personnel sign an agreement regarding this.

It is important to make it clear that the reliability of a cloud computing contract is not restricted only to the data and information stored in the cloud. For example, it should cover documents exchanged between the provider and the client company, conversations and understandings as well as the business model adopted.

Furthermore, the contracting parties should discuss the liability of the service provider for any willful or negligent action that should be undertaken by its employees or subcontractors, which could be contrary to the contractual confidentiality clause.

It is important to negotiate the possibility of the cloud computing provider to contract (or not) subcontractors, what should be foreseen in the service contract, and to what terms third parties would be bound by the original agreement.

It may be agreed, for example, that service providers will only be allowed to contract subcontractors eventually and under express approval of the other party. In this case, safety conditions must also be applicable to subcontractors. Some companies require that they must be informed about the identity of the subcontractors' employees and the changes in the staff; this should be a provision of the service contract.

Another important issue to be handled by the contracting parties is the law applicable to the contract, since the data can be stored in other countries.

The law applicable to this type of contract in most cases is related to a jurisdiction which may be the jurisdiction in which the provider has its principal place of business.

However, the acceptance of a clause with such applicable legislation by the cloud provider is difficult, since the vast majority of providers have infrastructure in several countries, according to the low cost of maintenance, cost and availability of energy and technological resources, which make it difficult to customize the service.

The contractors must also choose a territorial jurisdiction that will be responsible for applying the law elected by the parties. In Brazil, when choosing the national law, the parties also elect the Brazilian jurisdiction to deal with conflicts. In this case what can be changed is the court, and, generally cloud providers elect Sao Paulo.

Being elected arbitration for dispute resolution, the parties should choose the regulation and the jurisdiction that will be applied.

In some countries there is no specific legislation related to cloud computing. Other jurisdictions such as the European Union have enacted legislation regarding the issue. In the United States, for example, there is a legislation that permits the government to have access to any information stored and processed in the country, for reasons of national security.

So, it is prudent to discuss widely the question of legislation on cloud computing. This may occur through international bodies, since it has an impact all countries and the international law.

Protecting copyright, trademarks and trade secrets stored in the cloud is also a huge issue that is beyond the scope of this article.

As for the software developed and marketed by third parties used in the cloud, it is important that the contract for cloud computing specifies which contractor will be responsible for licensing, as well as for its update.

Normally the contracting companies share the cloud environment with other client companies of the provider. In these cases it is important to use and contract the encryption of data as well as the encryption program to be used (preferably with international certification). Another issue to be discussed is the separation of data, since some IT experts say that if such activity is not performed eventually there may be impact on access and recovery of encrypted data.

As for the providers monitoring of the cloud, many clients fear that by accomplishing it the provider may access restricted content and disclose both the content stored in the cloud and the result of monitoring. In contrast, providers ensure that monitoring occurs only in order to arrange the cloud properly to the client company needs; in other words: auditing storage space and processing regarding the size, the verification of time response and the suitability of bandwidth, among other details should be required. Therefore, the contracting parties should establish whether the monitoring will be admitted in the contract, and if so, what type of monitoring will be authorized.

Another issue that should be discussed by the contracting parties is the retrieval of content in the event of tampering or deletion. Will the provider of cloud computing backup data stored at what rate?

Another important issue that must be addressed in the contract under analysis is the security of information to be transferred, i.e. the security of the content that will be transferred between the parties over the internet. This concern is due to the fact that large providers of cloud computing services have multiple data centers and develop their own safety nets.

There may contractually be set an audit, for example, with respect to the integrity of the stored content, to the security of the contents to be transferred, to the performance of the service and to the safety of the cloud provider's

infrastructure. This audit should be performed at the direct service provider and at the subcontractors. However, if there is no contractual provision to allow it, the service provider is not obliged to consent to it. It is noteworthy that the audits are difficult to carry out, given the large number of servers, the various locations where they meet, besides the high cost involved in such activity, which, however, does not diminish the importance of the audits.

The auditing companies may be stipulated in the contract of cloud computing, as well as the frequency of the audits. Ideally, the audit firm should be an independent one, and if the data is to be stored in different countries, the best firm to conduct the audit would be an international service company. This company should be specialized in information security audit, data processing and cloud computing. Regarding the audit report it can be stipulated that it may be sent to one or both contracting parties.

It can be predicted that the provider will have a deadline to act on correcting problems found by the audit.

It can be reason for the termination of the contract, as well as penalties against the provider, if the vulnerability or flaw is not corrected in a timely manner.

And as to whether the supplier ceases to exist or undergo a merger or acquisition?

When it comes to merger or acquisition, often the new company has no interest in keeping some of the customers or the strategies previously established. Any of these situations may lead to improper disposal of customer content or even service interruption. Therefore, it should be stipulated contractually that the new provider will comply with the contractual terms agreed during the contract negotiation. It can also be agreed that the provider will notify the client company on the operation performed (e.g. merger and bankruptcy, among others), and may terminate the contract.

Another issue that must be included in the cloud computing service contract is related to the preservation of the content at the end of the validity period of the

contract. Will the provider hold the content or must it be returned to the customer? Will it be sent or made available to another provider indicated by the provider or by the customer? In what format should it be done? Will the provider delete the content safely (including backup)?

When it refers to a company that deals with ultra-sensitive data, such as financial and medical institutions, it can be defined that the client company (or a third party indicated by it) will audit the provider when the contract expires, in order to verify if all company data were actually deleted.

The time of preservation of the content by the provider can be radically reduced if there occurs breach of the contract or breach of any document that is part of it, as the Usage Policy. With respect to non-payment of the contracted service for a certain period, it is common the provider does not accept the task of keeping the agreement, as well as the storage of the content in the cloud.

What about a content infringement, invasion or attempt of invasion? It is important to discuss a clause that foresees that the supplier shall communicate the fact to the client company, as well as the measures taken and what content was accessed.

It is also important to foresee penalties for breach of contract, such as providing information to unauthorized persons, not providing the contracted service capacity, as well as a contingency plan to be adopted by the service provider. Example of penalty is a financial compensation for the damage caused. Regarding secrets, for example, attention should be paid to the importance of its protection, even when it is available in the cloud.

With respect to changes made to contracts, it was found that in a contract where the client party is a small-medium sized company or a natural person, usually unilateral changes are conceded as valid by the provider, which the client undertakes automatically.

With reference to large companies, as they have greater bargaining power, it may be agreed that any contractual changes must have the prior written consent of both parties.

Contracts generally exempt providers of cloud computing of any kind of accountability, which can be negotiated mainly by large clients, such as financial institutions and government.

Cloud computing contracts stipulate the basic features of the service that will be available, as the size of memory for storage. Generally the monitoring of services is performed by cloud provider and such monitoring is made available to the customer.

As to changes in the service offered to a natural person or a small business, such changes happen without the full knowledge of such natural person or small business. In these cases, as a rule, the client is aware of the change if the new term of service is available in the provider web page or if there is a notification by email or other means by the service provider, which rarely happens.

However, as to big client companies, this issue is largely negotiated between the parties and is subject of a contractual provision. In some contracts changes with specific deadlines for advanced notification by the provider are established. There are also contracts that admit their termination if the change made by the cloud computing provider impacts substantially on the service offered. In such cases, the parties must agree on a time that allows the client to migrate to another place

A great part of the cloud computing contracts deals with the possibility of suspension, resolution, and termination. But any contractual termination of the cloud computing service, especially the case of a big client company, must be well planned. When the client company takes the initiative of ending the contract service, it must first hire another service provider or have hardware and software to absorb the service that was previously provided by the third party.

Finally, in certain contracts for cloud computing service there is an item relating to definitions. This item clarifies the concepts of specific words that have been used throughout the document, which helps its interpretation by contracting parties, judges and arbitrators.

Thus, there are various issues to be negotiated between the parties, but the interpretation of contractual clauses should be carried out in accordance with good faith and the intention of the parties involved.

## *Conclusions*

The digital world is a reality that affects the society as a whole, individuals or legal entities. Initially cloud computing may have been more widespread among individuals, however, now its diffusion into business is greatly increasing.

Therefore, it is essential that professionals in information technology and the legal department of large companies are technically prepared to negotiate and enter into comprehensive contracts providing cloud computing.

In such context it is necessary to properly understand the services and deployment models available in the market, as well as the various solutions offered by companies providing this cloud computing services, which usually have a global scope.

Thus, contracts for the supply of the cloud computing services shall stipulate clauses that meet the interests of both parties. For example, not only security, integrity and reliability of the information stored and processed in the cloud, but also issues regarding intellectual property and data encryption.

As addressed in this brief study, there are many legal issues to be discussed by the parties in this new environment such as the right to remove personal data stored in the clouds, accordingly to the right to be forgotten.

Finally, cloud computing is an increasing IT model with new advantages for companies that hire that service. These advantages are the ability to focus

resources and energy on their core business, cost savings, high availability of data storage and increased productivity and profitability. But it is important to address the potential new legal impacts of cloud computing. It is also important to write contracts of service where duties and obligations of each party are clearly understood, thus avoiding subsequent drawbacks, such as loss of strategic and sensitive information to competitors.

CHAPTER 15

# ELECTRONIC GOVERNMENT SYSTEM

## INTRODUCTION

### *Definition of E- Government.*

As it is with any phrase, "e-government" can be amenable to different definitions, depending primarily on one's perspective or viewpoint. In general however, is a process of public administration and the provision of government services through the use of information and communication technology. This definition is wide enough to cover the use of facilities provided by the Internet, intranet and extranet communication systems

The general idea behind such a wide definition is to ensure that the resultant e-government structures are in a position to facilitate effective public administration within national or local government sectors.

The democracy that is the "mainstreaming of diversity, communication and cooperation approach," that is, the idea of rights, freedom and collective intelligence in open and/or virtual spaces.

Cyber democracy is a study of the potential for "electronic democracy" through the examination of case studies in US and European cities and civic projects. It aims to strike a balance between enthusiastic and dismissive approaches to "electronic democracy." The authors consider the impact of new technology with regard to the history of broadcasting and communications technology--in particular, the ways in which the principles and requirements of public service and universal access will, or will not be maintained.

This is a vigorous contribution to a vital debate about the state of democracy and the impact of communications technology. It will be essential reading for both students and policy makers.

The Internet's potential for interactivity permits it, like no other medium before it, to radically change the interactions between citizens and their governments, opening up greater transparency and participation. They also open the path to the renewal of democracy.

Cyber-democracy should be understood in its broad meaning as the practice of democracy via active participation in dialogue and in decision-making in the myriad public areas of civil society and provincial, regional and national political action. Governments and communities have the duty and responsibility to create the conditions for participation in democratic life in organisations, and publics spaces and arenas.

Cyber-government should not be limited to merely onlining administrative and governmental information or participation in online elections. As for community participation, it should not be limited to simple access to information, administrative transactions and online voting.

Mancini also highlights the difficulty of imposing a cyber democracy into a system which hasn't evolved much over the past hundred years. The Internet is an indispensable communication tool which has transformed the way much of society goes about accessing their information. A cyber democracy might not totally radicalize the way political decisions are made but it will provide greater access to a very inaccessible platform for the public

## *E-Participation.*

The basis of which cyber democracy would be built on is called e-participation. E-participation is the participation of citizens online, though ICT **(Jafarkarimi, Sim, Saadatdoost & Mei Hee, 2014).** ICT is a synonym for information and communication technology.[46] Examples of ICT would be Twitter, Facebook, or any platform which allows users to interact with one another and exchange ideas. E-participation is already in place in our society, "sending e-postcards or political jokes, downloading campaign software, forwarding an online, petition or signing up for an e-news bulletin, etc. Jafarkarimi, Sim, Saadatdoost & Mei Hee, p.643 2014) are examples of e-participation. Even in countries where government media is heavily censored, ICT platforms are able to go above the governments rule and broadcast events and ideas.

To implement a cyber democracy steps need to be taken to ensure that all users have access to a voting platform. The younger generation is more inclined to use newer technologies, while the older generation is more inclined to use traditional methods. Traditional methods would be treated as 'offline' modes of participation. Also the educated and the wealthy would also increase e-participation. Educated individuals increase democratic participation regardless if it's through online, e-participation, or offline participation.

A major critique of a cyber democracy is the issue of voter fraud. This is not true. John Wasik of Forbes suggests that if trillions of dollars can be sent via the Internet around the world everyday then there must be adequate security measures already in place (Wasik, 2012). Wasik also provides some suggestions which would increase voter participation:

1. Make voter registration seamless by having it tied to your social security number

2. Have more than one election day

3. Tie in voter identification to any number of biometrics such as fingerprints or retinal scans

4. Make voting mandatory

5. Don't link voting to polling places, allowing voting to be accessed anywhere

## *Benefits of a Cyber democracy*

A cyber democracy would affect many democratic governments, With less focus on individual parliamentary figure and a greater focus on political decisions governments would be more progressive and would theoretically eliminate individual error and political scandals. Through e- participation individuals would be allowed to vote in a bipartisan manner rather than having one individual make a discoing on behalf on a constituency, which could have a varied opinion on certain subjects. An example of this would be the Diane Finley public works funding scandal in which she granted over a million dollars for a project of, allegedly, personal interest and bias (Cbc.ca, 2015). If this issue of rewarding grants for public projects was allowed to be handle by the public then issue of bias would be eliminated. In turn a cyber democracy would lead to better government decisions, increased citizen trust in the government, and increased government accountability and transparency.

Cyber democracy would pave the way for a new public forum, which is "at the heart of any reconceptualization of democracy" (Poster, 1995). Poster also suggests that the age of face-to-face conversations in a public sphere is over and has been taken over by email, video conferencing, and other Internet based forms of communications.

The current issue with modern democracy are that it does not represent how citizens communicate. In Pia Mancini TED talk, How to upgrade democracy for the Internet era, she examples how political conversations are nearly impossible for the average voter to understand The political dialogue used is, "incredibly cryptic. It's done for lawyers, by lawyers" (Mancini, 2014). The internet is a tool which allows citizens to gain access to such a vast amount of information normally in common language. By allowing more accessible information it

provides a gateway to more discussion, the "…barriers of information are completely lowered and [citizens] can express [their] desires and [their] concerns" (Mancini, 2014).

**Examples of Cyber democracy.**

In Barack Obama's 2008 presidential campaign he introduced an online presence which had never been seen before. Although Obama being elected cannot be totally due to his campaign initiatives on the Internet, it was large enough to grant him 600 million dollars in web contributions and 1.5 million accounts on his campaign website, myBarackObama.com (Stirland, 2008). Obama's successful campaign attests to the power of ICT and examples how the Internet can gather an audience better than traditional methods. President Ronald Regan also used new technologies to his advantage. During his time in office the television was used to speak to the American public. Postman suggests in his book, Building a bridge to the 18th century: How the past can improve our future, that because Regan was on the 'magic of television' that his image "… projected a sense of authenticity, intimacy, and caring." (Postman, p. 5, 1999)

A more modern example of using the Internet as a democratic tool is the smartphone application, DemocracyOS. DemocracyOS is a platform for political discussion and allows voting on political issues all while encourages transparency between politicians and citizens. Lawyers, politician, and even whole governing bodies have started to adopt this open-source tool, including the Government of Mexico *(Finley, 2014).*

Although it is highly improbable that we will ever see a cyber democratic utopia where every parliamentary decision is made entirely by citizens via the internet, but, as Pia Mancini suggests; there is hope for better government transparency and a chance for citizens to become more involved in decision making through Internet-based programs. Websites like myBarackObama.com and software programs like Democracy OS example that citizens now have more decision making power when it comes to government issues, whether it is federal

elections or learning and voting on proposed bills Barack Obama and Roland Regan used the newest technologies of their time to work to their advantage and the way our society is becoming more Internet based is it inevitable that we will see the Internet being used as a political tool more often.

Facebook, Twitter, and other social medias have taken the place of traditional public forums granting access to millions of people worldwide to educate themselves on political issues and encouraging them to make an informed decision on what they are voting on and allowing more interaction with elected officials (Mancini, 2014).

A cyber democracy would reveal inner workings of the political process and allows citizens to weigh in and discuss their opinions, as Marcini says "…democracy is not just a matter of stacking up preferences, one on top of each other, but that our healthy and robust public debate should be, once again, one of its fundamental values". A successful cyber democracy would not try to reinvent the wheel but rather replace the spokes with broadband cables.

In the alternative; E-governance is the application of information & communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational & transactional exchanges with in government, between govt. & govt. agencies of National, State, Municipal & Local levels, citizen & businesses, and to empower citizens through access & use of Information.

## *Overview of E-Government*

In discussing the legal aspects of the structures supporting e-government, a number of theoretical underpinnings become immediately apparent: firstly, because of the nature of digital technology as a facilitative medium; and secondly, because of the legal effects of the decisions reached in relation to the nature of the supporting electronic structures.

Without electronic systems, processes and decisions of governments are usually effected manually. However, the introduction of e-government will equally bring

with it the need for decisions to be automated. Thus, the extent to which a merger of conventional and automated decision-making processes is to be established and in what specific areas of public administration are crucial to unanding the legal effects of e-government processes This also raises another issue- the legal effect of the interface between manual and automated decisions.

The introduction of e-government will also significantly impact on the normal working environment. The conventional working environment (which usually is defined by physical space and interactions) will now be replaced by either a virtual working environment or a combination of the two. The extent to which public sector employees are or can adequately be prepared for this transition also needs to be carefully examined.

It is also obvious that because departments of governments are structurally different and perform different functions, the level of e-readiness might not be uniform across the various levels of staff and between departments. To that extent, interoperability or the interface of the different e- government systems within and outside the public sector creates additional legal and security dilemmas.[236]

The establishment of e-government needs to also focus on the difficulty of clearly delineating the boundaries between the legal effects of automated as against those of the conventional executive and judicial decisions. A crucial question to ask is - where should the responsibility for such decisions lie. On machine or human or on both?

E-government structures help to facilitate meaningful civic dialogue and engagement between the public and government officials. This is healthy for effective governance and transparent administration. The need for this sort of engagement is no better needed than in island democracies with multiparty politics.[237]

## *Types of E-Government Structures.*

Here, are four basic structures which e-government in the Pacific could take. These are: Information Portals; Legal Services Portal; Judicial Services Portal; and e-Voting Portal. Of course, the circumstances in individual countries might dictate what is or can be added to these initial e- structures.

**Information Portal.**

This is by far the commonest e-government structure available. The rapid development of information and communications technology has brought with it the need for faster and easily accessible information on government functions and institutions in primarily two areas:

(a) Ministries, departments and statutory boards are generally expected to provide their email addresses and to also host websites detailing their functions and responsibilities. These sitescould also act as information hubs on a wide variety of government services by providing information on investment opportunities, tourism potentials, health, and environment, to mention a few.[238]

(b) Electronic filing of government documents, processing of on online permits, electronic tax payments and the submission of online public employment applications, to mention a few, will minimise wasting time on long queues and in getting mired in bureaucratic red- tape.[239]

**Legal Services Portal**

The provision of legal services to citizens should be distinguished from judicial functions performed by the courts. The emphasis here is on information, advice or materials that will improve access to justice. The recipient of such information, advice or materials will then be in a more informed position to process their rights. Three areas outline these e-government structures:

(a)Free-access online laws and regulations to help litigants who represent themselves in court or who may want to acquire a basic and

rudimentary understanding of legal processes. This includes the provision of wider public access to legal materials and advice in form of online legal aid and assistance.

(b) Electronic law reporting which covers statutes and judicial decisions made freely available to the general public.

(c) Online legal opinions to support the provision of legal aid and community legal service which may be automated, interactive or manually operated but processed online.[242]

While the first portal is merely informational, the second is both informational and interactive allowing for valuable processes to be completed online, thus saving a lot of precious time. In general, portals cover the activities of the three arms of government, namely the executive, legislature and the judiciary.

**Judicial Services Portal.**

The role of the judiciary as a constitutional arm of the government and an independent and impartial arbiter of disputes forms the third organ of e-government. The role of the judiciary in upholding the rule of law, good governance and democracy cannot be over-emphasised be it in developed or developing countries. The importance of the role is more pronounced in island countries, which in addition to the demands of modernity are at the same time also expected to integrate and balance customary practices in their ways of life or even in some cases in the governance of their communities. For this reason, the role of e-government in relation to the judiciary is manifested in three main areas:

(a) Information and communication technology supporting systems for the recording of customary or formal court proceedings and filing of non-contentious court documents.[243]

(b) The development and use of laws of procedure which support the admission of electronic evidence in civil and customary law claims and as a basis for settling such disputes.

(c) The use of automated electronic judicial decisions without human interface- a future possibility?

**E-Voting Portal**

Another important aspect of e-government is an e-voting system. The conventional and manual voting system has it strengths and will for some time to come continue to hold sway. However, attendant problems associated with vote rigging, falsification of election results and general apathy towards the conventional voting system may in the long run help popularise the electronic alternative. An e-voting system is also not without its problems, particularly when viewed in the context of some countries in the region. However, it is worth mentioning that these problems are by no means only confined to either the South Pacific or to developing countries.

In the context of Pacific island countries, issues relating to digital access and digital divide between urban and rural settlements, problems of security of electronic votes and counting procedures and the security of e-voting systems in terms of authenticating signature and identity need to be addressed first. To establish the integrity of an e-voting system as an integral part of any e-government structure, it has been argued that it must in addition to all other safeguard and security measures also leave a paper trail. The cost and operational implications of this requirement will be enormous for countries with limited national budgets.

## *Cost and Benefit of E-Government.*

An understanding of what is to done to ensure that e-government is effective and meaningful to the lives of people also requires an analysis of the problems and prospects of the system. It is against this background that the following points are discussed.

**Cost of Software and Equipment.**

The cost of software and equipment is fundamental and is one that will severely impact on the progressive development of e-government in the region. At the moment except for a few countries, the vast majority have no specific national ICT policies in place. To that extent, the creation of a knowledge-based and computer literate society does not represent an immediate priority for such governments. This trend needs to be reversed: by prioritising information and communication. technology; the development of supportive legal framework; and the granting of appropriate incentives to the private sector to support electronic transactions both at the public and private sector levels.

**Limited Bandwidth and Speed.**

While this is a problem, it is by no means confined only to Pacific island countries. Across the world, citizens generally suffer from this constraint which impedes the rapid download of data, voice or video transmissions. This also clogs the Internet highways and prolongs the time spent on accessing information on the Internet, thus negatively impacting on the availability of e-government services and products.

**Access to Government Services.**

The establishment of appropriate e-government structures in the form of portals for online legal, judicial, corporate and voting services will go a long way in improving the scope of access to government services. It will also speed up the utilisation of these services by the general public in view of the relative speed with which these can be processed. This is good not only for the economy but also helps in improving the quality of government services.

E-government structures have the capacity to improve the provision and delivery of government services. This will be a plus for democracy in that it can also promote good governance and transparency by linking public and private sectors online. The opportunities offered by the Internet need to therefore be fully tapped by the public sector in the region. According to Toland and Purcell:

South Pacific governments can use the Internet to assist with public sector operations. For example, ICT can provide governments with an increased capacity to collect revenue from fishing, agriculture and tourism. An intranet can allow different government departments to share information without having to make it available to the general public.

**Opening up Rural Communities.**

The establishment of e-government will foster development opportunities in rural communities. It has been asserted that this will also promote civic engagement between public government officials.[250] This is especially necessary in remote and rural communities which are far-removed from the main municipal and administrative centres of national governments. E-government structures will assist in bringing government services closer to the people thereby leading to effective24/ 7 Cf with the case of Malaysia where the National Information Technology Agenda of 1996 set the momentum for e-commerce, the development of appropriate hardware and software technologies and the institution of a legal framework to accommodate any accompanying changes. A significant aspect of this policy was the creation of the Multimedia Super Corridor aimed at fostering the development of e-commerce. Similar measures were taken by Singapore. This started in 1996 with the Electronic Commerce Hotbed Programme- a national policy initiative aimed at facilitating e-commerce in the country. In 1998, the country moved another step forward by inaugurating the Electronic Commerce Master Plan. See generally, P. S. Sangal, 'Malaysia Creates Legal Infrastructure for its Multimedia Super Corridor' (1997)12 *International Company and Comparative Law Review 428-430*.

Electronic governance because of transparency, greater and freer flow of public information. According to Chowdary, 'information and knowledge are what enable individuals to develop intellectually and economically. The dispersed nature of island communities makes them ideal candidates to greatly benefit from the potentials of information and communication technology.

**Attendant Risks.**

Continuous dependence on computers and related equipment and software may lead to associated physical and health risks. Although there is at present no evidence of this epistemological trend in any island country, it is time to begin considering appropriate policies and laws that will guard against that. The extent to which this may present significant occupational health problems in the region, only time will tell. However, it is still doubtful whether existing health, safety and occupational laws in the region can effectively deal with this new threat.

**Technical Issues.**

These generally relate to security, data integrity and privacy. These issues are very crucial not only to the development, but also to the operations of e-government structures in the region. Because decisions governing various aspects of peoples lives are automated, the source and authority of decisions made online must be easily identifiable. This will be addressed in four ways:

**Security.**

The use of technology to transact online has brought with it the problem of user-identification.[255] This is particularly so because of the remote nature of the transaction, the physical distance separating the parties and the ability to make instantaneous changes to electronic documents with little or no trace of detection. The cost-factor associated with putting in a place a reliable e-identification system will for some time to come make the technology suspect, at least from a legal point of view and particularly in the context of countries in the region. Perhaps a way forward for countries in the region is to set up a regional authentication agency which will integrate, optimise resources and save costs.

**Signature Authentication.**

Flowing from the foregoing is also the problem of writing and authenticating digital signatures, which is equally very crucial to e-government operations. The use of private and public keysencoded in electronic documents to authenticate or validate electronic transactions is widely regarded as a means of safeguarding the integrity of online transactions and business deals. While encryption

technology is also aiding the process of authenticating digital signatures, appropriate laws will however be needed to support the transition from conventional to electronic signature systems. At. present, almost all countries in the region are behind and need to catch-up by promulgating suitable laws to deal with issues pertaining to digital signatures; privacy of online public records and computer crimes, to mention a few.

**Data Integrity**

There are other problems associated with creating and managing 'round the clock' electronic databases, whether for public or private sector use.A fundamental issue here relates to data integrity. It is of utmost importance for the database to be accurate and up-to-date because it helps to prevent fraud and unauthorised access or misuse.

Because e-government structures aggregate and process enormous amount of data and do so from different sources, the integrity of electronic records must therefore be of utmost consideration in the establishment and management of reliable online government systems and services.

**Certification Authority.**

It is difficult for a single country to establish and manage a national certification authority[262] to process digital signatures as a means of validating automated public decisions. There are financial and technical issues associated with the storage of digital signatures and the protection of such databases from viral and other attacks. For a certification authority to be a reliable manager of digital signatures, it must eliminate the major risks for using these signatures between the sender and recipient.[263] Countries in the region need to put in place coherent national policies and legal frameworks to address the establishment and management of national digital certification agencies. In the alternative, stakeholders may consider establishing a regional certification facility to serve this need

# ELECTRONIC GOVERNMENT (E-GOVERNMENT) IN UGANDA

The way of carrying out business in the world today is changing at a very high speed with new technologies taking a center stage. Both government and the private sector have no alternative other than to move in that direction and adopt the emerging new technologies to modernize their service delivery. One of the major problems of developing countries today is the adaptation and adoption of these new technologies that will enable them utilize their information resources efficiently and effectively to propel them towards economic growth and development. Governments must position themselves to ensure investment in and application of new technologies to harness the benefits of these technologies.

## *National E-Government Policy regulations.*

The Government of Uganda (GOU) recognizes the role of Information and Communications Technology (ICT) in fostering economic development and is taking steps to adopt the emerging new technologies in order to modernize service delivery. It is also the belief of the GOU that ICT should be utilized to move into the era of electronic Government (e-Government) that is aimed at demystifying the role of Government, simplifying procedures, bringing transparency, accountability, and making credible timely information available to all citizens and at the same time providing all services in an efficient and cost-effective manner.

The Government of Uganda has a strong belief that ICT has the potential not only to revolutionize the way Government operates, but also to enhance the relationship between Government and Citizens (G2C), Government and Business community (G2B) and within Government to Government departments (G2G).

With this in mind, the GOU has developed the eGovernment Policy Framework which clearly identifies the goal of e-Government and spells out its core pillars,

critical success factors and a roadmap which will be adopted to achieve it. To operationalize the Policy Framework, Government has developed an eGovernment Masterplan to guide implementation over an initial period of five years.

**Purpose of the National e-Government Framework for Uganda**

The GOU recognizes the need for developing and implementing a national e-Government programme aimed at the efficient use of ICT in public administration in order to improve public service delivery and democratic processes and also to enhance the attainment of the then Millennium Development Goals (then MDGs). Now transformed into the Sustainable Development Goals (SDGs)

Ensure online accessibility of all government services and opportunities for community participation in a friendly, transparent and efficient manner for all sections of the society.

**Mission.**

Enhance and promote the efficiency and transparency in the functioning of government through the increased use of ICT for online service delivery to citizens and business

**Electronic Government Objectives.**

The following objectives represent broad statements of the e-Government Framework:-Objective

1. To continuously improve the efficiency of, and access to government information and services to meet citizen's expectations

2. To use the successful development of the e-Government initiative to promote Uganda, as an Information Technology centre for excellence in Africa.

3. To establish leadership and partnerships that advance e-Government services.

4. To develop and maintain a secure seamless and comprehensive e-Government interface (one- stop centre integrated service delivery mechanisms).

5. To manage the cost of e-Government implementation through effective use of technology.

6. To institutionalize the use of e-Government information and services through the adoption of appropriate organizational models.

## TRANSFORMATION OF THE UGANDAN SOCIETY.

As part of the national efforts to transform society and the economy through harnessing of ICT, the government of Uganda is pursuing an e-Government programme to be able to:

Improve services and convenience to citizens;

1. Improve the productivity (and efficiency) of government agencies;

2. Create a more accountable government;

3. Increase transparency and fight corruption;

4. Empower public access to information/records in possession of the state or public body, so as to effectively scrutinize and participate in government decisions that affect them;

5. Improve the quality of life for disadvantaged communities, promote gender equality and minimize the national digital divide;

6. Strengthen good governance;

7. Broaden public participation and promote democracy;
8. Strengthen the legal system and law enforcement;
9. Facilitate commerce and services for businesses online; and
10. Make private sector more competitive by reducing the cost of transacting with the Government e.g. in tax collection and e-procurement.

## *Expected Outcomes from e-Government Implementation.*

1. enhancement of the capacity of Government to deliver services
2. reduction in the costs of service delivery
3. improvement in the quality and speed of decision making processes
4. increased transparency of Government processes
5. Delivery of key enablers to societal evolution and reforms, through the provision of better and more timely citizen/government interaction.

## *Key initiatives for the adoption of e-Government in Uganda (enabling environment)*

1. establishment of a Ministry of ICT,
2. ongoing deployment of a fibre optic backbone and e-government infrastructure across the country,
3. enactment of the NITA-U Act 2009 to champion the implementation of e- Government in the country and
4. development of a National e-Government Framework for Uganda
5. formulation of National Cyber Laws including e-Signature, e-Transaction, Computer misuse acts of 2010

## *Ongoing /Planned e-Government initiatives in Uganda.*

1. Inter and Intra Governmental communication - internal and external email, with secure mail subsets (Intranet and extranet)
2. Document management
3. National Backbone Infrastructure Project (NBI/EGI)
4. Management of a wide range of applications for public services
5. Management of parliamentary queries and responses (e-Parliament)
6. Management of judiciary queries and responses (e-Justice)
7. Inter and Intra Governmental performance management (PMS)
8. Integrated Financial management Systems (IFMS)
9. Personnel and Payroll management (IPPS)
10. Public Procurement (e-Procurement)
11. e-Banking and e-Commerce
12. Project management and tracking
13. Immigration services (e-Visa, e-Passport, e-Border)
14. National Identification System
15. One Stop Centre (OSC) Web Portal eBiz (www.eBiz.go.ug)
16. eCitizen Portal
17. Monitoring and Evaluation

## *Highlights of Achievements of E-Government*

**In the FY2014/15, the sector achieved the following**:

1. NITA-U is undertaking consolidation of hardware and software licenses of government with the objective of accelerating delivery of e-government services through reduced costs of licenses. Master Business Services Agreement was signed with Microsoft that will enable consolidation of all Microsoft agreements. While negotiations with Oracles are also in advanced stages;

2. An Information Access Centre (IAC) has been set up in conjunction with the Government of Korea. The centre will enhance citizen participation and engagement in public policy and governance;

3. Technical support has been provided towards the establishment of a Government Citizen Interaction Centre (GCIC) championed by Office of the President;

4. Technical support offered to Uganda Investment Authority in the establishment of a One Stop Centre (OSC). The OSC will promote investment by providing easy access to the investment information while reducing the cost of doing business;

5. Technical support has also been provided towards the establishment of over 20 eGovernment systems including the integration of national systems and databases,

Electronic Single Window, eProcurement, eVisa, standardisation of Government websites, etc.

## *Legal aspects of Electronic Government in Uganda.*

Laws and Regulations that provide a conducive environment for the use of e-Government services Laws and regulations (legislations) may be in the areas of

Telecommunications, Protection of rights of ownership, Broadcasting Services, Internet Services,Information Technology/Computing, Music and Film Industry, Information/Data Access, Network security,Privacy and Data Protection,Information systems, e-Commerce (e-Transactions, e-Signature, Computer Misuse), Postal Services and Cyber Crime.

In **Ezeemoney Uganda Limited V MTN (U) limited**, the plainitiff successfully sued MTN for causing loss by unlawful means and inducing a breach of contract

In **Al Hajji Nasser Ntege Sebagala V MTN**[149], the plaintiff sued mtn for using his voice recording as a caller tune . However he was not successful because he had not copy righted the recording.

In **Byte Legion Technologies V MTN Uganda Limited**, [150]the plaintiff developed a soft ware programme and shared it with MTN company in making proposals for the two to work together. However to the shock of the plaintiff the company launched another similar product called GOOGLE SMS TRADER that was similar to that of the plaintiff.

The court dismissed the suit and held that the defendant was not obliged to inform the plaintiff about its simultaneous negotiations with Google. Court further held that the plaintiff was unable to prove copyright for his product.

In **Bassajjabaka Yakub V MTN**[151] , the plaintiff successfully sued the defendant for violation of his right to privacy when the company used his photo on abillboard without his permission.

[149]Al Hajji Nasser Ntege Sebagala V MTN Highcourt Commercial division Civil suit 283 of 2012

[150]Byte Legion Technologies V MTN Uganda Limited, High court commercial division 395 of 2009 .

[151] Bassajjabaka Yakub V MTN, high court Civil Division 100 of 2012.

## *Challenges.*

1. **Cyber or Computer Crime and System jurisdiction.** Most laws do not provide for cyber crimes and issues arise as to which legal system may apply as well what type of court that has jurisdiction

2. **Digital/ electronic Signatures.**Current laws recognize e-signatures but human acceptance a problem (resistance to change).

Most business Laws-contracts to day still requires evidence with original documents, including witnesses

3. **E- Payment/ e- banking.** Most Banks and other financial institutions have introduced ATMs Cards and other related Cards but some laws are not harmonized with e-banking transactions

4. **Taxation System**. Tax principles of source, residence and jurisdiction are affected by e-commerce, as goods delivered electronically pose a challenge on taxation system - URA is however demystifying this aspect through the e-Tax portal

5. **Data Protection and Privacy**. There is need to balance between the right to privacy and public interest

6. Intellectual Property Rights and Digital Technology infringement of IP rights under electronic publishing such as Copyright and software, web piracy

7. Reliability and admissibility of Computer Evidence

8. Lack of IT Literacy and awareness regarding benefits of e-governance **There is general lack of awareness regarding benefits of e-governance** as well as the process involved in implementing successful G-C, G-G and G-B projects. The administrative structure is not geared for maintaining, storing and retrieving the governance information electronically. The general tendency is to obtain the data from the files

(print) as and when required rather than using Document Management and workflow technologies. Lately the use of DMS and workflow technologies hasbeen able to find its use only in those departments where there is perceptible lightening of workload of the subordinate staff.

9. **Underutilization of existing ICT infrastructure**.To a larger extent, the computers in the department are used for the purpose of word processing only, resulting in the underutilization of the computers in terms of their use in data mining for supporting management decisions. The time gap between the procurement of the hardware and development of the custom applications is so large that by the time application is ready for use, the hardware becomes obsolete.

10. **Attitude of Government Departments** The psychology of government servants is quite different from that of private sectors. Traditionally the government servants have derived their sustenance from the fact that they are important repositories of government data. Thus any effort to implement DMS and workflow technologies or bringing out the change in the system is met with resistance from the government servants.

11. Lack of coordination between Government Department and Solution developers. Designing of any application requires a very close interaction between the government department and the agency developing the solutions. At present the users in government departments do not contribute enough to design the solution architecture. Consequently the solution developed and implemented does not address the requirements of an e- governance project and hence does not get implemented.

12. **Resistance to re-engineering of departmental processes.** Successful implementation of e-governance projects requires lots of restructuring in administrative processes, redefining of administrative procedures

and formats which finds the resistance in almost all the departments at all the levels. Additionally there is lack of expertise of departmental MIS executives in exploiting data mining techniques, updating and collection of real time content onto website etc. Therefore the content as is collected or maintained by various e-governance portals is unreliable or full of gaps. In such a scenario, it's difficult for any e-governance solution to achieve its intended results.

13. **Lack of Infrastructure for sustaining e-governance projects on national level.** Infrastructure to support e-governance initiatives does not exist within government departments. The agony is that the government departments are not equipped to be in a position to project the clear requirements nor are there any guidelines for involving private sector. Whatever efforts have been made by various government organizations may be defined as islands of computerization. The infrastructure creation is not guided by a uniform national policy, but is dependent on the needs of individual officers championing a few projects. Therefore, the required networking and communication equipment is either non-existent in government departments, or if it exists at all, it does not serve any tangible purpose as far as the requirement of e-governance project is concerned.

## *Solutions to the problems.*

There is need for both high level political and technical support and leadership is a prerequisite, Collaborative Relationships. Synergies must be shared to share resources and optimize the economies of scale, Proper Planning, Budgeting, Monitoring and Evaluation, Lobbying and Advocacy program is necessary, Mainstreaming of gender aspects and disadvantaged groups in all projects And Creating Literacy and commitment to e-governance at high level

The most important requirement is a training program for policy makers in E-Governance (Senior Public Servants), politicians and IT task force members. The training program needs to be focused according to the requirements of the

policy makers at the top. Such programs can be need based and outsourced when required. In addition it should be made mandatory for all the stake holders in implementation and maintenance of e-governance services to have the general IT skills. There may be specific requirements for training in certain specific projects. Such programs can be need based and outsourced when required. A few suggestive programs include e-governance training, Building web interfaces for citizen interaction, Document management and workflow applications, security and PKI solutions, Office Automation, networking

**Usability Surveys for assessment of existing e-governance projects should be conducted.** There is a varying degree of development of e-governance among the different states. A few States have leapfrogged into a digital era whereas a few are yet to start with any initiative. There is a tremendous divergence in the extent of implementation of the concept of e-Governance. It is, therefore, not possible to come up with a framework for implementation of e-Governance which is straightaway applicable to all states and the Central Government. Therefore an e-readiness exerciseshould be carried out in all states, government departments to understand their level of acceptability of the e-governance

**Implementation of pilot projects and replicating the successful ones.** The pilot projects taken in various states should be accessed for their achievement levels. They should be classified as success or failure according to the desired output written down before implementation of the projects. The study should be carried out by an independent agency for the implementation agency the study should be carried out at each stage of implementation. Bottlenecks and causes of delays should be documented, even though they are removed later. The successful projects should be replicated over the nation with members drawn from the implementing team. The projects, which could not achieve the desired outcome, should be documented for possible causes of failure. Various bottlenecks and causes of delay should be identified.

Government must adopt the Best Practices in e-governance. The study of Best Practices will bring forward the best practices being followed nationally and internationally. The national and international Best Practices study will give a

great momentum to the process of E-Governance. The State Governments will not have to re-invent wheel every time and they can learn from the developments already made.

Manage and Update content on government websites efficiently and regularly.Content is the 'heart' of any IT project. The government agency has to keep in mind some of the important technical guidelines, while developing the software and computerization, to facilitate the future integration. The department also needs to address the security of transactions and messages. The process of content development encompasses a whole range of activities starting with a comprehensive study of the system and identification of the objectives. It ends up with delivery of the intended benefits to the citizens or other users of the IT System. The government agencies must ensure that the data on the sites is always updated and relevant.

Have clearly defined Interoperability policy.The e–governance architecture needs to ensure that the components are scalable and adaptable to the future requirements. It has also to ensure that the Local architecture fits into the State level and the same into National and Global architecture. Interoperability is a major criterion while defining the architecture.

Build National resource Database of e-governance projects.This would allow any organization planning an IT project to instantly ascertain whether any such project has already been implemented anywhere in the country. Intending implementers would know who the key people in similar projects are and how to reach them. It is well known that it is much easier to replicate a solution than to evolve it the first time around. So the lead-time to implement projects can be reduced substantially.

If a project is already in operation in a similar environment somewhere in the country, acceptance by all concerned is much faster and smoother elsewhere. So change management becomes much easier and the time and effort involved in such implementations. Due recognition would accrue to the pioneers who created the successes. It would enable others to learn from them if they wish.

CHAPTER 16

# INTELLECTUAL PROPERTY ISSUES

## INTRODUCTION TO INTELLECTUAL PROPERTY LAW

An important part of cyber law is intellectual property. Intellectual property can include areas like inventions, literature, music, and businesses. It now includes digital items that are offered over the internet. IP rights related to cyber law generally fall into the following categories:

1. Copyright. This is the main form of IP cyber law. Copyrights provide protection to almost any piece of IP you can transmit over the internet. This can include books, music, movies, blogs, and much more. Copyright is A form of state-sponsored protection provided to the authors of original works. Works can include literary, dramatic, musical, artistic, or other intellectual works, both published and unpublished.

2. Patents. Patents are generally used to protect an invention. These are used on the internet for two main reasons. The first is for new software. The second is for new online business methods. Patent refers to the grant of a property right to the inventor, issued by the authorities

3. Trademarks/Service Marks. Trademarks and service marks are used the same online as they are in the real world. Trademarks will be used for websites. Service marks are used for websites that provide services. Trademark refers to a word, name, symbol or device which is used in trade to indicate the source of goods to distinguish them from the goods of others.

4. Trade Secrets. Trade secret laws are used to protect multiple forms of IP. This includes formulas, patterns, and processes. Online businesses can use trade secret protections for many reasons. However, it does not prevent reverse engineering.

5. Domain Disputes. This is related to trademarks. Specifically, domain disputes are about who owns a web address. For instance, the person who runs a website may not be the person who owns it. Additionally, because domains are cheap, some people buy multiple domains hoping for a big payday.

6. Contracts. Most people don't think contracts apply online. This is not the case. For example, when you register for a website, you usually have to agree to terms of service. This is a contract.

7. Privacy. Online businesses are required to protect their customer's privacy. The specific law can depend on your industry. These laws become more important as more and more information is transmitted over the internet.

8. Employment. Some employee contract terms are linked to cyber law. This is especially true with non-disclosure and non-compete clauses. These two clauses are now often written to include the internet. It can also include how employees use their company email or other digital resources.

9. Defamation. Slander and libel law has also needed updating because of the internet. Proving defamation was not altered substantially, but it now includes the internet.

10. Data Retention. Handling data is a primary concern in the internet age. An area where this has become a big issue is in terms of litigation. In lawsuits, it is now common to request electronic records and physical records. However, there are no current laws that require keeping electronic records forever. This is not true for physical records.

11. Jurisdiction. Jurisdiction is a key part of court cases. Cybercrime has complicated this issue. If a cybercriminal is located in Minnesota and their victim is located in North Carolina, which state has jurisdiction? Different states have different rules about this issue. Also, it can depend on in what court, federal or state, a case was filed.

Protecting IP can be difficult over the internet. An example of this would be the popularity of pirated movies and music. Each business that relies on the internet needs to develop strategies for protecting their IP. Governments can also take part in this process. In 1999, India did just this by updating their IP laws.

## *The Problem*

Protecting IP can be difficult over the internet. An example of this would be the popularity of pirated movies and music. Each business that relies on the internet needs to develop strategies for protecting their IP. Governments can also take part in this process. In 1999, India did just this by updating their IP laws.

Everything in cyber-space is composed of bits, the binary code that is the foundation of computing. In their digital form, images, music, video, and text are perfectly reproducible; not just once, but an infinite number of times. There is no degradation to limit the value of duplicate copies. With digital media, all copies are originals.

The binary reality of digital media poses vexing problems for how works are used and reused, as well as the rights and responsibilities of producers and consumers under existing law. One of the virtues of the Web is its reach: the ability to widely distribute digital works faster and less expensively than ever before. There is great value in being able to communicate to millions of peo ple. The downside is that content owners have little control over the subsequent dissemination and use of their work. Too many consumers unaware or confused by expansive license agreements, or willing to dismiss them as overly restrictive or unfair, approach the Internet in the erroneous belief that every item that they encounter is in the public domain.

Intellectual property is a legal term that refers to industrial property and to copyright and related rights. Industrial property comprises the protection of patents, trademarks, industrial designs, and geographical indications. It also includes the protection of utility models against unfair competition or the protection of undisclosed information. Trade secrets are protected, as they are a type of property or asset, just as valuable as or even more valuable than physical or real property. The value of intellectual property assets relative to physical assets has increased because of the importance of technology and creative works in the modern economy. Intellectual property consists of new ideas, original expressions, distinctive names, and appearance that make products unique and valuable . Intellectual property is often traded (or licensed) in its own right without trading in the value of an underlying product or service, by means of patent or other intellectual property licenses from a rights owner to another.

The character of the intellectual property system is evolutionary and while the nature of the rights themselves remains relatively constant, the manner by which they are expressed and exchanged is constantly adapting to developments in the underlying technologies. The invention of, in turn, the printing press, phonograms, radio and television broadcasting, cable and satellite transmission, videocassette recorders, compact disc (CD) and digital versatile disc (DVD) technology and now, the Internet, has affected both the form and the substance of intellectual property rights. Intellectual property has gained importance in this digital environment as, increasingly, business assets

are reflected in intellectual as opposed to physical property. The value of many online companies, for example, may be found in their vast databases of customer information, which may be the subject of intellectual property protection.

This migration of intellectual property onto the Internet can be seen with respect to each species of rights . In the field of copyright, vast numbers of works of literature, film and art, and notably computer programs, have already been transferred to the digital environment. Software, protected as a form of intellectual property by patent and copyright law, underlies the operation of all digital technologies. Systems software, including utilities and operating systems, enable our computers to operate, while utilities software provides us with the programs that make the digital networks so useful. Much software is protected by intellectual property law, and yet its theft is endemic.

The copyright is created automatically when a qualifying work is created but it protects only the work itself and not the idea behind the work. This means that the copyright is only infringed by copying. So, if your competitor uses the ideas behind your successful e-commerce website to develop a very similar website independently, then it will not necessarily be infringing your copyright by doing so.

Textual works such as books and newspapers are ideally suited to digitization and, although online publishing of popular literature has had a mixed reception with a public accustomed to paper and ink, there is evidence of a growing demand for e-books. There has been real success in the online availability of science, technology and medical publications, where the demand for fee-based research has supported the e-publishing industry. Demand has also grown for the online collections of more than 7,300 libraries that have provided free remote access to the texts of hundreds of thousands of e-books.

In the field of fine art, indigenous craft and artifacts, numerous museums and art galleries have digitized their collections and made them available for viewing on the Internet.

Identity on the Internet also goes beyond the trademark system, because of the role played by the Internet domain name system, which facilitates the ability of users to navigate the network. Domain names are user-friendly addresses that correspond to the unique Internet Protocol numbers that connect our computers to the Internet and enable the network routing system to direct data requests to the correct addressee. Domain names were originally intended to perform a purely technical function in a user-friendly way, but because they are intuitive and easy to remember they now perform a function as business or personal identifiers. Most businesses, whether e-commercial or not, advertise their domain name to signal a Web presence. In this way, although, as such, not a form of intellectual property, domain names now perform an identifying functions similar to that of a trademark. Because of the way in which people and search engines operate, most businesses use their trademark or trade name as their domain name, and this has caused conflict with the advent of predatory practices. The patent system has also migrated to the Internet, as businesses have sought to recoup research and development costs in digital technologies by patenting their online business methods. In fact, the technology-intensive nature of e-commerce means that many of its constituent processes may be patentable subject matter so long as the legal criteria for patentability are met.

The global information society foreseen in the early days of the Internet has yet to become a worldwide reality, but the focus on information remains the key to the ecommerce economy. Although a good proportion of the information on the web is in the public domain, and freely available to use and copy, an increasingly significant amount is protected as intellectual property. The enthusiasm generated by the availability of so much online information, easily accessible through browsing and hyper linking, contributed to a general expectation that this information was free and its use uncontrolled. The intellectual property community has been addressing the challenge of this perception ever since, in an effort to determine and exert legal rights over digital content.

The intellectual property community, including film and music creators, software developers, authors and publishers, are now exploring ways in which to

make their products available online, while protecting their rights and recouping their investment. To some extent, the uptake of fee-based intellectual property services is dependent on the efficient management of these rights, as well as the availability of workable and secure methods of micro payments that would enable pay-per-unit purchases, and the building of consumer confidence in online payment security, privacy and consumer protection. At the same time, however, creators and intellectual property rights holders need to feel sure that they can protect their property from piracy and control its use, before they will be willing to make it available online.

The online distribution of audiovisual works has been held back until recently by the lack of bandwidth, which has prevented the relatively large data files required to transmit video to be downloaded or streamed at a speed or quality acceptable to consumers. While the technology is still developing to facilitate accessible video-on-demand and digital pay-per-view, the film industry is yet to match the progress of the music industry, and most legitimate film sites are web casters that distribute short made-for-online film and animation material which is largely experimental and available free of charge. As in the music industry, copyright owners in the film industry are also reluctant to release their audiovisual works online while there is a lack of adequate copy protection that could protect them from rampant piracy.

In the radio and web casting industry, Internet radio has been luring customers away from traditional media sources by providing access to thousands of global radio broadcasts in real time.

## *Existing laws*

Almost every country in the world has legislation on intellectual property rights protection, perhaps what to talk about should be the loopholes.

## *The Loopholes in the Intellectual Property system*

While the world is getting larger with its expanding cyber-space, the world intellectual property system is still at its infancy. Different countries or territories have different intellectual property rules, practices and procedures. Strategic e-intellectual property management has its defensive and proactive aspects. On the defensive side, one has to avoid infringing intellectual property rights. On the proactive side, one should manage its intellectual property by strategic acquisition, licensing and enforcement.

It is submitted that a key success factor in ecommerce is strategic e intellectual property management. Any member of the information society who loses sight or underestimates the impact of intellectual property on e- commerce may have to learn it the hard way, paying a high price for intellectual property infringement or lack of intellectual property protection.

The international exhaustion is not solely a legal issue; there are economic and political aspects which must be balanced. Arrangements may exist where a number of countries decide to form a single regional market, in effect defining a single regional territory. In such an arrangement, a requirement for freedom of movement of goods within a single market may lead to the acceptance of the legitimacy of parallel imports between countries which are party to the arrangement, provided that those countries together agree among themselves that such a restriction of the rights of a patentee is necessary in the realization of such a single market.

The following states do not apply a rule of international exhaustion of patents: Australia, Belgium, Brazil, Bulgaria, Czech Republic, Denmark, Egypt, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, the Netherlands, Paraguay, Portugal, Republic of Korea, Romania, Spain, Sweden, the United Kingdom, United States and Yugoslavia. In contrast, Argentina, Canada, Singapore and Venezuela do apply a rule of international exhaustion of patents.

Countries including the Member States of the European Economic Area (EEA), Bulgaria, Czechoslovakia, Hungary, Romania, the US and Yugoslavia do not

apply a rule of international exhaustion for trademarks. In contrast, Argentina, Australia, Brazil, Canada, Japan, Paraguay, Mexico, Singapore, Switzerland, Venezuela and Yugoslavia all allow international exhaustion.

There are obviously various approaches and a lack of uniformity in international exhaustion.

This question raises the distinction between the common law approach to exhaustion and the approaches of different countries. The common law approach is that a sale of goods is a contractual matter, and that treatment of Intellectual Property Rights (IPR) may be affected by the contract. In other countries, the treatment of IPR cannot be limited by contract. In a majority of countries, exhaustion is considered to be a matter governed by the legal effect of IPR, which are property rights having effect against all third parties. It is thus not possible for a contract between individuals to have any effect on the position. This is the legal theory, for example, in Brazil, Czech Republic, Paraguay and Yugoslavia. In contrast, in Japan (for patents at least) international exhaustion may be limited by contract and where there is a breach of contract, no exhaustion takes place. The Japanese position for patents is that if a patent owner fails to impose a contractual restriction on sale outside Japan then, irrespective of whether there is a parallel patent in the country of sale, the patentee is deemed to have waived his rights to prevent importation into Japan. In contrast, for trade-marks, the law is not clear. In Australia contracts may be effective in the case of patents, but not in the case of trademarks. In Canada it is necessary to bring a contractual restriction to the attention of a purchaser if it is to be effective. In Singapore contractual restrictions cannot be imposed to limit the effect of international exhaustion. In Japan the law differs for patents and trademarks.

Inventions are characteristically protected by patents. Inventions must also be protected by other types of rights, such as utility models or trade secrets. The patent system provides a framework for innovation and technological development by, on the one hand, granting an exclusive right to theowner of a patent to prevent others from commercially exploiting the patented invention for

a limited period and, on the other hand, balancing this right with a corresponding duty to disclose the information concerning the patented invention to the public. This information, which is stored in the patent documentation, is available to anyone and, is increasingly accessible online through Internet- based systems. The mandatory disclosure of the invention thus enriches the available pool of technological knowledge, facilitates technology transfer, and enhances the opportunities for creativity and innovation by others.

The patent system plays a vital role in e-commerce, and relies in a critical way on various computer and network technologies. However, the new technologies pose challenges to the conventional legal scheme for the patent system. It is expected that the number of these e-commerce-type patents may increase significantly, bearing in mind the potential for individuals, companies and national economies, as well as the global economy. Such patents are viewed by some as important for creating incentives and spurring investment in new digital technologies. But the subject matter of a patentable invention must have a technical character or involve technical teaching, (an instruction addressed to a person skilled in the art as to how to solve a particular technical problem using particular technical means).

Since the phenomena of digital networks and e-commerce are new and still emerging, the novelty of a business model in this area makes the requirements of patentability a tenuous task. That competition may be harmed in cyberspace if companies are able to obtain patents for basic business methods that already exist in non-cyber-space.

In addition to the question as to whether computer programs should be regarded as inventions under patent law, this broad scope of patentability has prompted a discussion of where the line is to be drawn between copyright and patent law protection for computer programs.

The Internet raises complex issues in jurisdictional and enforcement of rights, as patent protection is provided on a country-by-country basis, and the patent law of each country has application only within its borders, in accordance with the traditional principles of territoriality. For example, where patented software is

sold and delivered over the Internet internationally, any infringement action would require a consideration of the jurisdictional and choice-of-law issues. The first practical issue may be that of detection, since the unauthorized importation of such software by means of the Internet, unlike the importation of tangible goods, cannot be detected and stopped by customs authorities.

In the area of patents, one specific question may arise with respect to the law applicable to infringements when a patented invention consists of elements that are physically located in different territories. For example, in the case of process patents for a method to process and transfer certain data using computerized networks, distinct elements in the process could be performed in different territories. If an alleged infringer operates a system containing all of the claimed elements within the territory in which the invention is protected, there would be a straightforward claim for infringement. The question of applicable law (and jurisdiction) would be more difficult where a patented invention involves activities in several countries by several individuals.

Prior to the development of the Internet as a medium for commercial exchanges, consumers rarely entered into direct relationships with foreign vendors. Typically, foreign products were distributed through local importers from whom consumers residing in the territory would make purchases. As a result of the global presence that the Internet enables, this model will no longer apply in manyinstances. Consumers can place orders on, or performs downloads from, the sites of foreign vendors, thus entering into a direct contractual relationship with them. This shift in the business model has important legal reverberations from the consumer protection point of view. As consumer protection is regarded a matter of public policy in many countries, these questions have proven particularly vexing to solve.

## *The Suggested Solution*

The fundamental difficulty in coping with legal relationships involving foreign elements flows from the fact that the legal systems of more than one country may be involved. The application of the laws of one system, rather than that of

the other, will lead to different results. One solution to this problem consists of selecting the laws of one particular legal system to govern the legal relationship, from among the various potentially applicable legal systems.

A radically different solution consists of trying to remove the source of the problem, through a process of harmonization which eliminates the differences that exist between the laws of countries on a given issue. Harmonization can be achieved through negotiations between states, with treaties establishing uniform rules under a universal code and the subsequent modification of domestic laws in order to bring them in line with the treaty provisions.

# INTELLECTUAL PROPERTY LAW AND SEARCH ENGINES.

The widespread "search engines" in Internet allow to track down the information scattered through the web in a very quick way and just by typing simple questions. As a general definition can serve the one offered by the referee of the Court of Great Instance of Paris of 8th January 2001 (Cadremploi vs. Keljob; revoked by the sentence of the High Court of Paris of 25th May 2001): "a search engine is just a device which permits to look for information through criteria given to it and should not be used to collect other things but references, contents or parts of contents in order to the immediate reutilization in the frame of a commercial enterprise, created to that aim.

## *History of Search Engines.*

The first search engine was Archie, created in 1990 by Alan Emtage, a student at McGill University in Montreal. Archie was a tool for indexing FTP (File Transfer Protocol) archives through a searchable database of filenames as a method of storing and retrieving files online. Archie's operation was such a success it was later adapted and enhanced to generate new and more advanced search engines.

During the mid-1990's, new search tools emerged, introducing a complex system of search modifiers, enabling natural language searches, and grouping web pages by their underlying concepts to fine- tune a users' search results. Originally, search engine algorithms were based solely on the text of the webpage—determining its subject matter and relevance based on keywords discussed. Search engine capabilities, however, continued to expand, adding metadata (information about the page itself such as age, number of links, and authorship) into algorithms and assessing relevance based on the number of links.

The search engine market tended to fluctuate—many search engine companies emerged in the late 1990s, only to disappear a few years later; some search engines, however, asserted a strong presence in the market. Google, one of the most prominent Internet businesses, emerged as a leader in the search engine sector in 2000. Google's objective was to be the "perfect search engine,"—one that "understands exactly what [is] mean[t] and gives ... back exactly what [is] want[ed]—and based on its popularity it has generally achieved this objective. Although Google remains a prominent search engine, its competitors—Yahoo!, Bing, etc.—continue to vie for prominence in the online search engine market through innovation and expansion based on developments in search engine technology.

## *Functioning of Search Engines*

The technology search engines use is an important component to determining potential liability from legal issues. The methods for collecting, storing, and disseminating Internet-based content determine the scope of potential responsibility for a search engine

Search engines are intermediary tools to catalog websites using a process referred to as "crawling. Search engines gather the content through automated software by "crawling" through different web pages, copying the HTML code of each website found, and then retaining this in a temporary pool or "cache. The software compiles these different websites into a comprehensive index. Search results are generated from the search engine's index based on the search term

query submitted by the user. The heading and a snippet of each individual search result are indexed through computer- processed algorithms. By clicking the "cache" link of a webpage, the user views the most recent scanned and indexed snapshot of the website.

To avoid indexing certain content through a search engine's web-crawl, the content must be removed from the original website or be encrypted to prevent the web-crawl from locating the content. However, search engine indexing updates may not occur frequently given the voluminous data thatthe "crawler" must process and filter and therefore removal or encryption may not immediately remove the content from search engine results.

The potential challenges to search engine liability are based primarily on the technology used to operate a search engine. The crawling process, cache system, and dissemination method are all scrutinized to determine the culpability of search engines in particular circumstances.

## *Overview of Search Engine Liability.*

Search engines are unmistakably Internet-based operations; Internet-based laws for content providers, host providers, and online business operators, however, can be challenging to apply to search engines. Search engines are distinct from these other operations in both objective and technology, which requires courts and legislatures to address legal issues related to search engines from a different perspective.

Relevant case law emerged shortly after search engines rose to Internet prominence and primarily addressed the definition of search engines as distinct from other Internet- based entities. ACLU v. Renodefined the functionality and importance of web search engines as services that "allow users to search for Web sites that contain certain categories of information" and provide a list of links to relevant websites. Other early American cases noted additional distinctions between search engines and Internet-based businesses. **Lockheed Martin Corp. v. Network Solutions, Inc**. was a trademark infringement suit brought by a

company against the domain name registrar. The court held that keyword searches "often yield thousands of possible Web sites," and that "such a cumbersome process is rarely satisfactory to businesses seeking to use the Web as a marketing tool.

As Internet use expands, search engine law continues to grow. Search engine operators face increasing legal action related to intellectual property and data protection including third-party trademark infringement from advertising, copyright violation from search result displays, content aggregation from "crawling, and manipulation of search result rankings. This section examines search engine liability through a multi-jurisdictional review of general intellectual property rightsand defamation; it also explores the similar but distinct challenges generated by online advertisements.

## *Intellectual Property Issues*

Since the Internet is not bound by geographic constraints, legal issues concerning search engines are not bound by geographic constraints. The following cases and regulations demonstrate the pervasive search engine issues transcending jurisdictional boundaries. The most frequent types of claims against search engines arise from intellectual property violations and personal defamation suits. This section addresses search engine related intellectual property and defamation issues in the United States, the United Kingdom, and Europe.

Three main questions can be formulated about the intellectual property issues related to the search engines:

- Can the results of the searches be protected as autonomous databases?
- Are the search engines databases on their own?

- Does their operation imply an unlawful extraction and/or reuse of the information they collect from other web sites or databases or, on the contrary, is this a lawful use (right to mention)?

The answer to the first question is linked to the status granted to the creations or databases generated by computer means. This could be in relation to systematically presented data which may be easily retrieved or accessed by the individual user.

But, even if the results of the search engines are included into the notion of database, it would be necessary to solve the problem of the protection they deserve. The necessary element of the creation, as a result of a human activity, would impair the protection by means of the author's rights, since the requirement of the original creation would be missing.

But these results, and any database generated by a computer, could be protected by the sui generis right, provided that their production is the result of a material and proved investment; and for it, the value of the software necessary to generate the database and its operation would play a capital role against the rest of the resources used to obtain the final result. Anyway, if these results are to be protected, it would be advisable to make it clear in the general terms of use of the search engine, forcing their acceptance before offering the results of the search, as well as specifying the restrictions on the reuse of the lists of links.

To solve the other two issues, it would be necessary to refine the operation of the search engines according to their typology. To remove some irrelevant cases, it would be advisable to distinguish between the local or closed search engines — which browse their own web site without violating any intellectual property right and are a system to retrieve information without skipping from one page to the other— and the general or open search engines, which make inquiries in the webs of third parties and can be thematic (within a given field) or "panthematic" (covering any field). Note the difference between the six types of general or open search engines, which could be defined as follows:

1. The directories offer the possibility to access to multiple registered web sites summarized in different categories arranged in indexes of subjects visible to the user. The web sites are reviewed by the employees of this directory who include them according to their level of interest.The automatic search engines are software aimed at localizing, retrieving, indexing and updating the web pages on the Internet. The localization is done by means of ""spiders"', "robots"' or "crawlers"', which follow the links included in the web pages to increase continuously the information compiled. Each web page is integrated into a list of keywords using the words in the title of the web site, in its description and in the meta tags (or even in the text of the web page). The search engine offers its features to the user through a box where he/she can enter some words to request the system a list with the results following the internal index created, thus being a true database. It is also possible to offer the information in a directory or in an hybrid form.

2. The metaengines allow the user to use several search engines at the same time for a single search. Usually, they do not include their own database, rather they just forward the requests to a number of search engines, and then collect the resulting information and offer it to the user.

3. The search engines for search engines are a compilation of search engines, arranged by regions or subjects as a directory, which will also receive the question by words, and from which the user can access to the particular search involved.

4. The search services operate in a way similar to the search engines (and they even use them), but do not display immediately the results, rather they make customized inquiries according to the request and then forward the results to the user, either by e-mail or by means of an off-line version.

The user of any of these tools usually thinks that he/she is using a "database" but, from a technological and legal point of view, according to the sources of the information received and to the search procedure, the titleholders of the intellectual property rights affected can be several (as many as databases are successfully inquired). It is possible to draw some clear conclusions from the classification offered:

1. First, the pure search engines (directories or automatic search engines), provided that they fulfil the legal requirements involved (particularly the material investment, in terms of time or money) are true databases which can be at least protected by the sui generis right. The same applies to the search engines for search engines. Conversely, the search services cannot be included into this category if they do not have their own databases and just inquire the existing ones; and most of the times, the metaengines could not be included either.

2. Secondly, the arrangement of the search engines as a directory can enjoy an additional protection by means of the authors' rights if the selection or arrangement criteria are original ones, since they are a collection of links which can be arranged as a database; nevertheless, their level of originality should exceed the well-known general thematic distributions used by any web site (i.e., leisure, sports, education, health, etc.).

3. Thirdly, if a pure search engine or metaengine records or copies the web pages reviewed when it compiles their entries to offer them directly to the users, or if it uses the caching system (with automatic, both provisional and temporal, storage), besides of being liable for this reproduction or extraction, and in case it does not have an authorization. A number of laws require for protection of data bases against third parties.

A general answer rejecting that these tools imply a violation of the intellectual property rights on the basis of the possibility that the titleholder of a work or

performance on the Internet specifies that he/she does not want to become part of any index or search engine (he/she would authorize it, unless otherwise provided) is not realistic or legally justified. Apart from the legal problems implied by such a unilateral provision to be legally binding, the abovementioned operation of the search engines will ignore these notices, at least as regards the automatic search engines or the metaengines. The violation of the rights would have to be considered case by case, paying attention to the criterion of the unlawful use of a third party's effort and investment (the basis of the protection granted by the sui generis right and of the rules on unfair competition) and, by way of guidelines, to the three following ones:

The combination of the results of the search with the use of frames to offer them as their own results might imply a violation of the rights to the extraction and reuse of the creator of the database.

1. Since most of the web sites on the Internet are free for the users and obtain their funding from advertising, including the search engines, the skipping or removal of the advertising when they offer the information found could be a determining factor to get a court judgement. This would imply the application of the same criteria applied to the deep links.

2. Sometimes, despite the appearances, these are not true search engines (which do not violate, a priori, the intellectual property rights, since they just offer the typical links to other web pages found), but real unauthorized extractions from third parties' databases.

## *American Case Law on Search Engine Liability*

American courts have addressed a significant number of claims against search engines and have developed extensive jurisprudence on search engine liability, particularly related to intellectual property disputes and defamation.

Protecting intellectual property rights and promoting access to information are important issues in determining search engine liability. *Perfect 10,* involved an

intellectual property conflict over a search engine's capacity to assemble, organize, store, access, and display intellectual property protected "content." The plaintiff, Perfect 10, published a magazine and operated a subscription website; it registered the images it used with the United States Copyright Office. The defendant, Google, operated a search engine and indexed websites on the Internet via a web "crawler."

The court focused on whether a search engine could be liable for displaying "thumbnails" of copyrighted images on an "image search" and whether a search engine could be liable for displaying copyrighted images from another website through hyperlinks, The court also addressed whether Google directly infringed Perfect 10's distribution right by broadcasting the relevant images on the web. The court distinguished between "display" and "inline linking," while analyzing available precedents. The court held that Google did not infringe Perfect 10's right to distribution since infringement required *"actual* dissemination" (emphasis added) of the copyrighted material.

Defamation is another common basis for lawsuits brought against search engines. In ***Field v. Google,*** **Blake** Field filed a copyright infringement claim against Google Inc. for allowing Internet users' access to copies of 51 of his registered works, which violated Field's exclusive right to reproduce copies and distribute copies of those works. The court required Google to satisfy four elements for its estoppel defense. Because Google's "cached" links allow users to view pages that the user cannot easily access directly, the court held in favor of Google, noting that "if Google copies or distributes Field's copyrighted works by allowing access to them through 'cached' links, Google's conduct is fair use of those works as a matter of law.

The aforementioned cases and their progeny indicate the limitations on liability for search engines under American jurisprudence.

## *English Case Law on Search Engine Liability*

Courts in the United Kingdom addressed Internet law related to search engines similar to the United States. Although there are two preceding cases that provide the foundation for search engine liability in the United Kingdom, this section will focus on the contributions to this genre from a 2009 case.

In 2009, Metropolitan International Schools Limited brought a defamation case against Designtechnica **Corporation, Google UK Limited, and Google** Inc. This case established precedence for addressing Internet-based entities and provided a distinction between search engines and other Internet-based entities. This case also provided a rational basis for apportioning liability for online actions, and serves as a foundation for future cases addressing Internet activity and search engines.

The court held that the search engine operators exercised no control over Designtechnica's actions because a search yields a list of pages determined (automatically) relevant to the query. Thetechnology ranks the pages in order of "perceived" relevance, without human intervention; the search results to any given query depend on successful crawling, indexing, and ranking.

The court held that a search engine is "a different kind of Internet intermediary," which prevented the search engine from exercising complete control over the search terms and search results.[303] The court determined that Google was merely a conduit to information, not a publisher in its own right.

In the **Metropolitan case, Justice Eady** clearly states that the significance of notification to the proprietor of a search engine merits attention and in that regard, the Third Defendant is not in a position to "take down" the offending words in the way that the Claimant could have done. The opinion referenced search engines' responsibility to remove content after receiving a complaint about libelous material, though the speed and effectiveness of removal was not addressed.

Other courts and regulations lend additional support to the reasoning on search-engines liability based on broadcast content that violates local laws.

## *European Cases and Regulatory Frameworks on Search Engine Liability*

In civil law countries, court decisions related to search engines do not retain the same authority as in common law countries. There are, however, a few notable court decisions in Europe that demonstrate a comprehensive appreciation for the limits of search engine liability. In ***Palomo v. Google Inc***.[304]Spain's Court of First Instance heard a complaint regarding search result hyperlinks to websites with defamatory content. The court rejected the claim and held that the search engine was not liable for disseminating third party content. The court's rationale was that the search engine was unaware that the linked content was defamatory. The court also referenced the direction of European legislation indicating that there is no obligation for Internet intermediaries to supervise such content.

In ***SARL Publison System v SARL Google France***[305], claims were brought regarding an allegedly defamatory "snippet" appearing in the search engine results with a hyperlink to the primary site. The court held that a search engine was not obliged to consider the legality of a website that appears among the search results. Similarly in ***Jensen v. Google Netherlands,***[306] the court held that Google was not responsible for the outcome of a search (i.e. the claimant's name). The reasoning recognized that search engines bring up "technical, automatic and passive" results, independent from the knowledge of the search engine operator.

Internet legislation on the Internet also regulates search engine actions and liability in European countries. Bulgaria's Electronic Commerce Act, enacted in December 2006, removed liability from automated search engine services for contents where the transmission of the data has been already initiated, the data recipient has already been chosen, or where the data obtained is already chosen or altered.

The legislative framework in Romania has also been revised to protect search engine services from responsibility for content broadcasted by third parties. Article 15 of Law No. 365 on ElectronicCommerce provides protection to

search engine services unaware that the broadcasted information is illegal. If the search engine service is aware of the illegal broadcast it may avoid liability by removing or blocking access to the content.

Other jurisdictions can learn from these approaches when generating their own laws on search engine liability and Internet law.

## *Online Advertisements and Search Engine Liability*

Content provider liability also applies to online advertisements. A use that violates the rights of a third party concerns the advertiser rather than the search engine. The content and keywords of an advertisement are provided by the advertiser. A search engine generates list of advertisements based on keyword searches and acts as an intermediary listing the online advertisements for Internet users. When an Internet user performs a keyword search, the search engine displays the advertisements that correspond to those words. These are referred to as the 'natural' results of the search.[309] Therefore, the advertiser should be liable for an advertisement's content and keywords since the search engine exercises no control and has no obligation to monitor the content.

An automated process allows advertisers to create an advertisement by selecting the keywords, drafting the commercial message, and adding a link to their website. The advertiser is responsible for the keywords, categories and/or other channeling mechanisms; the advertisement produced by or for the advertiser; and the services or products in the advertisement. The search engine places the advertisement on the sponsored section of the results page. The short text that appears on each search result is automatically generated by computer processed algorithms created by third parties. Therefore, the Internet service provider that allows an advertiser to use a third party trademarked keyword and then displays the advertisement is not violating the trademark rights of a third party.

The Internet service provider cannot store data information and cannot control the data, and therefore, it cannot be responsible for the data kept upon the advertiser's request. A connection between a keyword and a search word shall

not be evaluated as if a search engine has the authority to control such data. Additionally, an Internet service provider that stores a keyword sign identical to a trademark and organizes the advertisement display on the basis of that keyword is not using that sign in the course of trade for its own goods or services.

Search engine are not liable for a third party's content and excessive monitoring expectations are unrealistic.

A landmark decision on this topic is the European Court of Justice's ***Google v. Louis Vuitton***decision.[312] The court held that an internet referencing service provider which stores, as a keyword, a sign identical with a trade mark and organizes the display of advertisements on the basis of that keyword does not use that sign[313], thereby not holding Google liable for trademark infringement. The court reasoned that the proprietor of a trademark is entitled to prohibit an advertiser from advertising, on the basis of a keyword identical with that trademark or goods or services identical with those for which that mark is registered.[314] Secondly, the court held that if an internet referencing service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored, that service provider (i.e. Google) cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.

## *Summary of Search Engine Liability*

These cases and regulations indicate a growing consensus on the extent of search engine liability. Because a search engine operator does not create, change, and upload the content on the Internet, it cannot be held liable for infringement. The individual who creates, changes, and uploads the content on the Internet (i.e. the content provider) would be the appropriate person to hold liable for infringement. The search engine operator also does not have any responsibility to monitor content and is not accountable for infringing the protected content

rights of third parties. Therefore, search engine operators are not liable under criminal or civil law for listing infringing content among search results.

The aforementioned cases and regulations establish a multi-jurisdictional framework for approaching search engine liability. This framework provides a useful tool for emerging market economies; as rising Internet use generates challenging legal issues, these courts and legislatures can adopt an approach that harmonizes with existing international jurisprudence on search engine liability.

# PROTECTION OF COMPUTER PROGRAMS

The laws which govern the protection of computer software fall under the domain of intellectual property. Intellectual property protection is generally granted for the benefit of both creator of the property and public welfare. There is a three step process linking the public welfare with intellectual property. The first step involves expanding the scope of legal protection offered to software creator. The second step is this kind of enhanced protection creates a reward system motivating further creativity. Finally, this expansion of inventive activity brings about the discovery of more ideas and faster advancement of technology. The end result of this process is that the public receives different range of software products.

The granting of intellectual property protection to computer programmes can be seen as a form of legal subsidization to a particular industry and technology. The intellectual property regimes that protect computer software have had a direct impact on the ownership and user regimes that have been established; the alternatives to proprietary software, open source and free software have been a philosophical and practical response to the existing legal regimes.

The persons seeking protection for their software related inventions follow the three important intellectual property rights for the protection of their programs are copyright, patent and trade secrets.(sometimes trade mark and trade dress law also apply for the protection of computer software).

## *Why Protect Computer Software*

"Computer software" also referred to as computer programs are the instructions executed by a computer. In other words, the explanations, instructions, commands and systems which have been developed in order to run the machine are called „computer software". Software comprises of the following one or more components: the source code itself which contains the programme's invaluable comments any literature that may be supplied with the package which could be in the form of manuals or explanatory material regarding the running of the programme. All these components require protection because the making of it involves the expenditure of skill, time and labour and therefore the resultant work should be protected from misappropriation.

Software has a market value. Computer software is subject to ferocious competition with a shorter life circle and is liable to be copied soon, as it is "read all on the face" technology. Because of its nature the owner of computer program will have two problems (i) economic problem and (ii) competition. Economic problem means, others can access it without payment to the creator. Competition means the competitors will make competing products based on the creation either by reserve engineering or blatant copying. Apart from protecting the economic interest of the owner the protection of software through appropriate IPR mechanism is considered necessary to encourage creativity, innovation and investment. As already mentioned software may be reproduced at no cost, some means of restricting the free copying and redistribution of software work is necessary to preserve an investment in a software product.

There is a divergence in views among various jurisdictions of the world as to what category of intellectual property may that is to be granted to protect computer software. Presently there are two principal modes of protection of software, copyright and patents. Copyright is most commonly used to protect computer program, because writing of a code is similar to any type of literary work. The copyright protection is extended to expression of ideas.

To establish intellectual property protection to computer software domestically and internationally the signatories of TRIPS Agreement, Berne convention, and WIPO Copyright Treaty (WCT) have agreed to protect copyright in a computer program until, at a minimum 50 years after the author (software writer) of the program dies. For citizens of more than 162 members of Berne convention countries, once protection is grated to a work in one member country that work is automatically protected with in the borders of all other signatory countries. However, it is the discretion of the states to given protection for computer program under copyright or patent laws.

## *Copyright law Protection of Computer Programs*

Copyright law and patent law provide different types of protection. Copyright protection extends only to expressions, and not to ideas, procedures, methods of operation or mathematical concepts as such, whereas a patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem.

Copyright protection is formality-free in countries party to the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention), which means that protection does not depend on compliance with any formalities such as registration or deposit of copies.

Copyright will automatically subsist in a 'work', provided the criteria for protection are satisfied.

These include:

(1) originality: this does not mean that the work has to involve creativity or artistic merit, but simply that a work 'originates from its author', i.e. it is the author's own intellectual creation or an expression of his/her 'independent' skill, labour and judgment;

(2) for certain types of work, the requirement to be recorded in a material form; and

(3) the presence of factors connecting the author or the work to the UK (or to a country party to international copyright treaties).

While copyright protection is conferred relatively easily, the scope of protection (and consequently the monopoly granted) is narrower if compared with that provided by trade marks or even more so patents. As observed by the Court of Justice of the European Union ('CJEU') in relation to computer programs (but it applies to all types of copyright works), 'copyright protection covers only the individual expression of the work and thus leaves other authors the desired latitude to create similar or even identical programs provided that they refrain from copying' (*SAS Institut Inc –v- World Programming Ltd, C-406/10)*. The rationale is that, doing otherwise, would 'make it possible to monopolize ideas [as opposed to the expression of ideas], to the detriment of technological progress and industrial development'.

# PATENT PROTECTION

A patent is generally granted after completing an examination procedure by a government agency. Copyright protection of computer software is established in most countries and harmonized by international treaties to that effect.[317] A patent allows you to forbid anyone to duplicate the functionality of the program, or any tricks or features in the program that were invented by you. However, this can be a very important affair, especially if a court case is necessary to enforce your right. Copyright will be most useful when others are making and distributing copies if your program, for example on a website or a CD. This can be prevented by copyright law, but you could also charge money for the act of distributing. Usually this is easier than going after them for patent infringement.[318]

Unlike the copyright law which merely protects the expression of an idea, patent law protects the concepts of the invention. Currently some countries protect computer software like any other invention as long as it is a proper subject for patent protection i.e. if it is a new and useful process involving an inventive step and capable of industrial application. The subjects which excluded from patent protection are laws of nature, natural phenomena, abstract ideas and

mathematical expressions of scientific truths. Mathematical and scientific expressions are denied patent protection because technology is suppressed against the desires of the authors of the constitution, if such patents are granted.[319]

Comparing to the protection given under patent law, the protection given by copyright and trade secrets has limited scope. The owner of the copyright over an item of software has the right to prevent any other person from copying the code as it is written but does not have the right to prevent the utilization of idea behind the code, providing that the person utilizing the idea must use in a manner that different from the arrangement of the code. The copyright law is also limited to prohibit unauthorized copying of the protected work but it does not prohibit all forms of copying. The expression of a method of operation and principles of a computer program cannot be protected by copyright. Functional aspects of a computer program are excluded from copying. A patent provides more secure protection than the copyright and the trade secret. It protects the "idea" or "functionality" of the software. Copying of an idea is very easy to do and anybody can describe it simply, that is might a patent is restricting from doing.[320]

If a computer software is merely an algorithm it should not be protected under patents. The term of algorithm is not defined in the patent act. If the invention is technical in nature it will entitled to get protection under patents. The mathematical algorithms which per se are not regarded as patentable subject matter universally, they are merely considered as abstract ideas or mental steps.[321]

# REFERENCES


1. **Aguilera, R. V. and Jackson, G. 2003**. 'The Cross-National Diversity of Corporate Governance: Dimensions and Determinants', Acade my of Management Review28, 447-465

2. FCC, Federal Communications Commission.(2009).About the Federal communications commission. Retrieved from http://www.fcc.gov/aboutus.html

**3.** IANA, Internet Assigned Numbers Authority.(2009).Introducing IANA. Retrieved from http://www.iana.org/about/

4. IETF, Internet Engineering Task Force. (2009).About the IETF. Retrieved from http://www.ietf.org/about/IEEE, Institute of Electrical and Electronics Engineers. (2009). Comcast claims they'll stop bittorrent throttling.

5. BroadbandDSLReports.com,1(25), Retrieved from http://www.dslreports.com/shownews/Comcast-Claims-Theyll-Stop-BitTorrent-Throttling-93022

6. International Telecommunication Union.(2009,December18).About ITU–ITU's History. Retrieved from http://www.itu.int/net/about/history.aspx

7. International Telecommunication Union. (2009,December18). The ITU mission: bringing the benefits of ICT to all the world's inhabitants. Retrieved from http://www.itu.int/net/about/mission.aspx


8. International Telecommunication Union.(2009,December18). About ITU. Retrieved from http://www.itu.int/net/about/index.aspx

9. International Telecommunication Union. (2009, December 18).ITU Landmark Dates. Retrieved from http://www.itu.int/net/about/landmarks.aspx

10. International Telecommunication Union - Telecom. (2009, December 18). IPTV Global Standards Initiative. Retrieved from http://www.itu.int/ITU-T/gsi/iptv/

11. International Electro technical Commission. (n.d.). Mission and Objectives. Retrieved from http://www.iec.ch/about/mission-e.html

12. International Electro technical Commission. (n.d.). 732 - Computer network technology. Retrieved from http://dom2.iec.ch/iev/iev.nsf/index?openform∂=732

13. International Organization for Standardization.(2008).Corporate governance of information technology. Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=51639

14. ISOC ,Internet Society.(2009).Introduction to ISOC. Retrieved from http://www.isoc.org/isoc/

15. Leiner, B, Cerf,V, Clark, D,etal.(1997).The past and future history of the internet. Communications of the ACM, 40(2), 102-108

16. Leiner, B, Cerf, V, Clark, D, et al. (2009). A brief history of the internet. Computer communicationreview,39(5), 22-31

17. Madden, J.(2009) Liskula Cohenv. Google,Inc. in the Supreme Court of New York. No.100012/09

18. Macmillan, T. 2003 ‘Tales of Power in Biotechnology Regulation: The EU Ban on BST’, Geoforum34(2):187–201

19. Network Overview: Internet Traffic Report. (2009,December27).Retrieved from http://www.internettrafficreport.com/

20. Porteus, L.(2005,November10).Who should control the Internet? Retrieved from http://www.foxnews.com/story/0,2933,175096,00.html

21. Postel ,J.(1972,December22).Internet-Drafts and RFCs. Retrieved from https://datatracker.ietf.org/doc/rfc433/

22. Raush, Gretchen. Personal interview. 9 Nov. 2009. Personal interview. DONE IN MLA - Could not find an APA Method for an interview

23. Raeburn, A. (n.d.). Development and growth of IEC technical committees: 1950 to 2006. Retrieved from http://www.iec.ch/about/history/overview/overview_1950-2006.html

24. Reporters Without Borders(2006). Internet Annual report.http://web.archive.org/web/20061126165543/http://www.rsf.org/print.php3?id_article=17177

25. Stoker, G. (1998). Governance as theory: Five propositions. International social science journal,50(1),17

26. UNESCAP, United Nations Economic and Social Commission for Asia and the Pacific s. (2009).What is good governance? Retrieved from http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/g/governance.asp

27. Van Atta, R.(n.d.).Fifty Years of Innovation and Discovery. Retrieved from http://www.darpa.mil/Docs/Intro_-_Van_Atta_200807180920581.pdf

28. Waldrop, M.(n.d.).DARPA and the Internet Revolution. Retrieved from http://www.darpa.mil/Docs/Internet_Development_200807180909255.pdf

29. Ward,M.(2002,March30).Wanted: New plantorun the net. Retrieved from http://news.bbc.co.uk/2/hi/science/nature/1898639.stm

30. Ware, J. (2006) Alberto R. Gonzales V. Google, Inc. In The United States District Court for the Northern District of California, San JoseDivision.CV 06-8006MISC JW

31. Zizic, B. (2000). Copyright Infringement Occurring over the Internet: Choice of Law Considerations. Master of laws thesis. Queen's University. Kingston, Ontario, Canada. http://www.collectionscanada.ca/obj/s4/f2/dsk2/ftp01/MQ54498.pdf

32. Cbc.ca,. (2015). Diane Finley breached conflict rules, federal ethics watchdog rules. Retrieved 11 March2015, from http://www.cbc.ca/news/politics/diane-finley-breached-conflict-rules-federal-ethics-watchdog-rules-1.2988913

33. Finley, K. (2014). Out in the Open: An Open Source Website That Gives Voters a Platform to Influence Politicians |WIRED. WIRED. Retrieved 23 March 2015,from http://www.wired.com/2014/05/democracy-os/

34. Jafarkarimi, H., Sim, A., Saadat doost, R., & Mei Hee, J. (2014). The Impact of ICT on Reinforcing Citizens Role in Government Decision Making (1st ed., pp. 642-645). International Journal of Emerging Technology and Advanced Engineering. Retrieved from http://www.ijetae.com/files/Volume4Issue1/IJETAE_0114_109.pdf

35. Mancini, P.(2014,October).PiaMancini: How to upgrade democracy for the Internet era[Videofile].Retrieved from http://www.ted.com/talks/pia_mancini_how_to_upgrade_democracy_for_the_internet_era/transcript?language=en

36. Poster, M. (1995). Cyber Democracy: Internet and the Public Sphere. Hnet.uci.edu. Retrieved 11 March 2015, from http://www.hnet.uci.edu/mposter/writings/democ.html

37. Postman, N. (1999). Building a bridge to the 18th century: How the past can improve our future. New York: Vintage Books. Rebar ,P.(2013).

38. Programming a Career in ICT. Retrieved from http://www.careeroptionsmagazine.com/wpcontent/uploads/2013/09/ICT_800x390.jpg

39. Stirland, s. (2008).Propelled By Internet,Barrack Obama Wins Presidency. Wired. Retrieved 11 March 2015, from http://www.wired.com/2008/11/propelled-by-in/Wasik, J. (2012). Voter Fraud: A Massive, Anti-Democratic Deception. Forbes. Retrieved 23 March 2015 ,from http://www.forbes.com/sites/johnwasik/2012/11/06/voter-fraud-a-massive-anti-democratic-deception/

40. Al-Alawi, A.I. and M.F. Abdelgadir, 2006. An empirical study of attitudes and opinions of computer crimes: A comparative study between U.K. and the Kingdom of Bahrain. J. Computer. Sci., 2: 229-235.

41. Direct Link Beebe, N.L and J.G.Clark,2005.Ahierarchical,objectives-based framework for the digital investigations process. Digital Invest. 2: '147-167.

42. Cross Ref|Direct Link|CSI, 2011.15 the annual computer crime and security survey. Computer SecurityInstitute.GDN, 2011. Cabinet push to fight cybercrimes. Gulf Daily News, Bahrain, September 19, 2011.http://gulf-daily-news.com/NewsDetails.aspx?storyid=313726.

43. GDN,2013.Helpsoughtforcybercrimecell.GulfDailyNews,Bahrain,February19,2013.http://www.gulf-daily-news.com/source/XXXV/336/pdf/page09.pdf.

44. Grewal, S.S., 2011. Fighting cyber crime. Gulf Daily News, Bahrain, May 03,2011. http://www.gulf-daily news.com/NewsDetails.aspx?storyid=305199.

45. Interpol, 2013. Enhancing international law enforcement cooperation and training focus of INTERPOL Chief's visitto Bahrain. February18, 2013. http://www.interpol.int/News-and-media/News/2013/PR015.

46. May, C.,2002. Computer forensic: The morse or clouseau approach. Comput. Fraud Security, 2002:14-17.

47. McDowell,B.,2012.Tech companies collaborate to fight phishing.http://www.itp.net/popup/print/587806.

48. Morris,R.,2003.Uncoveringauser's hidden tracks. Computer Fraud Security,2003:11-13

49. Direct Link Norton Cybercrime, 2011.The shocking scale of cyber crime: Report.http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

50. SPAM fighter News, 2006. Phishers target bank of Bahrain and Kuwait. SPAM fighter, Denmark.http://www.spamfighter.com/News-6307-Phishers-target-Bank-of-Bahrain-and-Kuwait.htm.

51. Sambidge,A.,2012.Bahrain'sgul fair says facebook page hacked.April10,2012.http://www.itp.net/588577-bahrains-gulf-air-says-facebook-page-hacked#.Ufm1053frIV.

52. Savona, E.U., 2012. Organized crime enablers, Global council on organized crime. World Economic Forum, July 2012. http://reports.weforum.org/organized-crime-enablers-2012/#chapter-enablers-of-cybercrime.

53. Teelink,S.andR.Erbacher,2006.Improving the computer forensic analysis process through visualization. Communication ACM.,49: 71-75.

54. Cross Ref| DirectLink| Trade Arabia, 2013. Cracks down on cyber crime. Trade Arabia Business News Information, Bahrain, January

12, 2013.
http://www.tradearabia.com/news/IT_228801.html.Wang, Y., J. Cannady and J. Rosenbulth, 2005. Foundations of computer forensics: A technology for the fight against computer crime. Computer. Law Security Report, 21:119-127.

55. Cros sRef|DirectLink| European Network and Information Security Agency. (2009).

56. Mell,P.& Grance,T. (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. Retrieved May 5, 2014 from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

57. Rohrmann, C. A. & Machado e Campos, M. (2009). Oscontratoseletronicos: Um estudo historico-comparativo dos direitos brasileiro e europeu. Revista da Faculdade de Direito Milton Campos, 18,2376).

58. Valenzuela, D.P. & Montoya ,J.D.B. (2012).Aspectos legales dela computacion emlanube.Bogota:Universidade Externadode Colombia.

59. Rohrmann, C.A.& Cunha, J.F.S.R. ,Some Legal Aspects of Cloud Computing Contracts.

60. Journal of International Commercial LawandTechnology,Vol.10 No.1(May,2015)

61. Avgerou, C.(2002).Information Systems and Global Diversity. Oxford, Oxford University Press.

62. [Bevir, M. and W. R. Rhodes (2004). "Interpreting British Governance." British Journal of Politics and International Relations 6: 129-164.

63. Braa, J., E. Monteiro, et al. (2004). "Networks of action: sustainable health information systems across developing countries."MIS Quarterly28(3).

64. Ciborra, C. (2003). Unveiling E-Government and Development: Governing at a distance in the new war. Department of Information Systems, Working Paper Series. London, London School of Economics and Political Science.

65. Ciborra, C. and D. D. Navarra (2005). "Good Governance, Development Theory and Aid Policy: Risks and Challenges of E-Government in Jordan."Journal of Information Technology for International Development 11(2).

66. DFID(2002).TheSignificance of Information and Communication Technologies for Reducing Poverty. London, Department forInternational Development.

67. Dobriansky, P.J.(2003)."Science, Technology, and Foreign Policy: The Essential Triangle: Remarks to the Council of Scientific Society Presidents."Retrieved 11 October,2004,

68. Force, D.(2001).Creating a Development Dynamic. New York, Digital Opportunity Task Force.

69. Foster,I.,C. Kesselman, etal.(2004)."The Physiology of the Grid: An Open Grid Services Architecture for Distributes System Integration."Retrieved 20th March,2004,

70. Intaj(2003).Jordan'sInformationSociety:afastgrowingsectorforatransformingnation.Beirut,Economicand Social Commission for Western Asia.

71. Data Protection Commission (Ireland), 'Case Study 1/01', available at: https://www.dataprotection.ie/docs/Case-Studv-1-01-Bank-and-Insurance- Company/121.htm

72. Privacy International, 'How do companies get our data?' available at: https://www.privacvinternational.org/feature/2048/how-do-data-companies-get-our-data

73. The Centre for Internet and Society, 'Aadhaar Act and its Non-compliance with Data Protection Lawin India', 14 April 2016, available at: https://cis-india.org/ internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection- law-in-india; and Usha Ramanathan, 'Aadhaar: from compiling a government database to creating a surveillance society',Hindustan Times, January 2018, available at: https://www.hindustantimes.com/opinion/aadhaar-from-compiling-a-govt-database-to-creating-a-surveillance-society/story-Jj36c6tVyHJMjOhCI8vnBN.html

74. Costica Dumbrava, 'European Information Systems In The Area Of Justice And Home Affairs: An Overview',European Parliamentary Research Service Blog,15 May 2017 ,available at: https://epthinktank.eu/2017/05/15/european-information-systems-in-the-area-of-justice-and-home-affairs-an-overview/

75. CJEU case of Osterreichischer Rundfunk C-138/01 2003

76. Commission National Informatique & Libertes, Compliance Package: Connected Vehicles and Personal Data, available (PDF) at: https://www.cnil.fr/sites/ default/flles/atoms/flles/cnil packvehiculesconnectesgb.pdf

77. Privacy International, Big Data - Explainer, available at: https://privacyinternational.org/explainer/1310/bigdata

78. Maria LaMagna,' The reason your loan application is rejected may have nothing to do with your credit score', MarketWatch', 29 March 2017, available at: https:// www.marketwatch.com/story/the-reason-your-loan-application-is-rejected-may-have- nothing-to-do-with-your-credit-score-2017-03-29: Anna Tims,' Equifax mistake with my credit score nearly lost mea mortgage' ,The Guardian,14February 2017, available at: https://www.theguardian.com/money/2017/feb/14/credit- rating-remortgage-equifax-experian-callcredit.

79. Anna Tims,‘ How credit score agencies have the power to make or break lives’,TheGuardian,17July2017,availableat: https://www.theguardian.com/money/2017/jul/17/credit-score- agencies-break-lives-lenders-no-mortgage

80. Court of Justice of the European Union, ‘The Court of Justice declares the Data Retention Directivetobe invalid’, Curia, available(PDF)athttps://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

81. Privacy International, Contesting Surveillance, available at https://www.privacyinternational.org/programmes/contesting-surveillance: and Privacy International, ChallengingData Exploitation, available at https://www. privacyinternational.org/programmes/challenging-data-exploitation

82. Foundation for Media Alternatives,‘National Privacy Commission to issue flnd in gson Comelec breach’ available at:http://www.fma.ph/?p=399

83. Folhade S. Paulo, 6 July 2016, available (Portuguese) at: http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados- de-pacientes-da-rede-publica.shtml

84. Paragraph 1of Article 5of the GDP Routlines the principles relating to processing of personal data.

85. Duncan Alfreds, ‘SA fails to make data breaches public - expert’, Fin24, 26 February 2016, available at https://www.fln24.com/Tech/Cyber-Security/sa-fails-to- make-data-breaches-public-expert-20160226

# APPENDIX 1

## ELECTRONIC TRANSACTIONS ACT 2011

ACTS
SUPPLEMENT No. 4 18th March, 2011.

ACTS SUPPLEMENT

*to The Uganda Gazette No. 19 Volume CIV dated 18th March, 2011.*

Printed by UPPC, Entebbe, by Order of the Government.

**Act 8** *Electronic Transactions Act* **2011**

# THE ELECTRONIC TRANSACTIONS ACT, 2011.

## ARRANGEMENT OF SECTIONS.

PART I—PRELIMINARY

*Section.*

*Section.*

# THE ELECTRONIC TRANSACTIONS ACT, 2011

**An Act to provide for the use, security, facilitation and regulation of electronic communications and transactions; to encourage the use of e-Government services and to provide for related matters.**

DATE OF ASSENT: 17th February, 2011.

*Date of Commencement:* See section 1.

BE IT ENACTED by Parliament as follows:

## PART I—PRELIMINARY

### 1. Commencement

This Act shall come into force on a date appointed by the Minister by statutory instrument and different dates may be appointed for the commencement of different provisions.

### 2. Interpretation.

(1) In this Act, unless the context otherwise requires—

"addressee", in respect of a data message, means a person who is intended by the person originating the data message to receive the data message, but not a person acting as an intermediary in respect of the data message;

"advanced electronic signature" means an electronic signature, which is—

(a) uniquely linked to the signatory;

(b) reliably capable of identifying the signatory;

(c) created using secure signature creation device that the signatory can maintain under his sole control; and

(d) linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable.

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of a data message in which the conduct or data messages of one or both parties is not reviewed by a natural person in the ordinary course of the natural person's business or employment;

"computer" means electronic, magnetic, optical, electrochemical, or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or a group of such interconnected or related devices;

"consumer" means a person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"currency point" has the value assigned to it in Schedule 1;

"data" means electronic representations of information in any form;

"data message" means data generated, sent, received or stored by computer means and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"data subject" means a person from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;

"e-Government services" includes a public service provided by computer means by a public body in Uganda;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of data messages;

"electronic record" means data which is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device and includes a display, printout or other output of that data;

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored and the procedure for recording and storing of electronic records;

"electronic signature" means data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicates the signatory's approval of the information contained in the data message; and includes an advanced electronic signature as well as secure signature;

"electronic transaction" means the exchange of information or data, the sale or purchase of goods or services, between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks;

"information" includes data,text,images,sounds,codes,computer programmes, software and databases;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the internet or any other information sharing system;

"information system services" includes a provision of connections, operation facilities, for information systems, the provision of access of information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

"Minister" means the Minister responsible for information and communications technology;

"originator" means a person by whom or on whose behalf, a data message is sent or generated prior to storage, but does not include a person acting as an intermediary in respect of that data message;

"person" includes any company or association or body of persons corporate or unincorporate;

"public body" includes the Government, a department, service or undertaking of the Government, Cabinet, Parliament, a court, local Government administration or a local council and any committee or commission thereof, an urban authority, a municipal council and any committee of any such council, any corporation, committee, board, commission or similar body whether corporate or incorporate established by an Act of Parliament relating to undertakings of public services or such

purpose for the benefit of the public or any section of the public to administer funds or property belonging to or granted by the Government or money raised by public subscription, rates, taxes, cess or charges in pursuance of any written law and any council, board, committee or society established by an Act of Parliament for the benefit, regulation and control of any profession;

"service provider" means—

(i) any public or private entity that provides to the users of its service the ability to communicate by means of a computer system, and

(ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

"third party", in relation to a service provider, means a subscriber to a service provided by the service provider or any other user of the service provider's services or a user of information systems.

(2) This Act shall be construed consistently with what is commercially reasonable under the circumstances as to achieve business sense.

**3. Application**

(1) This Act does not apply to the list of documents specified in Schedule 2.

(2) Nothing in this Act shall limit the operation of a law which expressly authorises, prohibits or regulates the use of electronic documents.

**4. Object of the Act**

(1) The object of this Act is to provide a legal and regulatory framework to—

(a) enable and facilitate electronic communication and transactions;

(b) remove and eliminate the legal and operational barriers to electronic transactions;

(c) promote technology neutrality in applying legislation to electronic communications and transactions;

(d) provide legal certainty and public confidence in the use of electronic communications and transactions;

(e) promote e-Government services through electronic communications and transactions with the Government, public and statutory bodies;

(f) ensure that electronic transactions in Uganda conform to the best practices by international standards;

(g) encourage investment and innovation in information communications and technology to promote electronic transactions;

(h) develops a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(i) promote the development of electronic transactions that are responsive to the needs of users and consumers; and

(j) foster economic and social prosperity.

PART II—FACILITATING ELECTRONIC TRANSACTIONS

**5. Legal effect of electronic records.**

(1) Information shall not be denied legal effect, validity or enforcement solely on the ground that it is wholly or partly in the form of a data message.

(2) Information incorporated into a contract that is not in the public domain is regarded as having been incorporated into a data message if the information is—

(a) referred to in a way that a reasonable person would have noticed the reference to the information or incorporation in the contract; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as the information is reasonably capable of being reduced into electronic form by the party incorporating it.

(3) Where—

(a) an act;

(b) a document; or

(c) information,

is required to be in writing, produced, recorded or retained, it may be written, produced, recorded or retained in electronic form.

(4) For purposes of subsection (3) the requirement for a document or information to be in writing is fulfilled if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner which is usable for subsequent reference.

**6. Use of electronic signature.**

Where a law requires a signature or provides for consequences where a document is not signed, the requirement is fulfilled if an electronic signature is used.

**7. Authenticity of data message.**

(1) Where a law requires information to be presented or retained in its original form, the requirement is fulfilled by a data message if—

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the authenticity of a data message shall be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of an endorsement and any change which arises in the normal course of communication, storage or display;
(b) in light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

**8. Admissibility and evidential weight of a data message or an electronic record**

(1) In legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message or an electronic record—

(a) merely on the ground that it is constituted by a data message or an electronic record;

(b) if it is the best evidence that the person adducing the evidence could reasonably be expected to obtain; or

(c) merely on the ground that it is not in its original form.

(2) A person seeking to introduce a data message or an electronic record in legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3) Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is fulfilled upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

(4) When assessing the evidential weight of a data message or an electronic record, the court shall have regard to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the authenticity of the data message was maintained;

(c) the manner in which the originator of the data message or electronic record was identified; and

(d) any other relevant factor.

(5) The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(6) For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of set standards, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

(7) This section does not modify the common law or a statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

**9. Retention of information or record.**

(1) Where a law requires that a document, record or information be retained, the requirement is fulfilled by retaining the document, record or information in electronic form if—

(a) the information contained in the electronic record remains accessible and can be used for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to accurately represent the information originally generated, sent or received;

(c) the information which is retained enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received; and

(d) the consent of the department or ministry of the Government, or the statutory corporation, which has supervision over the requirement for retaining the record, has been obtained.

(2) The obligation to retain a document, record or information in accordance with subsection (1) (c) shall not extend to information generated solely for the purpose of enabling a document, record or information to be sent or received.

(3) Subsection (1) may be fulfilled by using the services of a person other than the person who originated the document, record or information.

(4) Nothing in this section shall—

(a) affect a law which expressly provides for the retention of documents, records or information in the form of electronic records;

(b) preclude a department or ministry of the Government, a statutory corporation from specifying additional requirements for retaining electronic records that are subject to the jurisdiction of the department or ministry of the Government, or statutory corporation.

**10. Production of document or information.**

(1) For purposes of section 5(3), a requirement to produce a document or information is fulfilled if a person produces the document or information in electronic form if—

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained in the data message would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the authenticity of the information contained in a document is maintained if the information has remained complete and unaltered, except for—

(a) the addition of an endorsement; or

(b) an immaterial change, which arises in the normal course of communication, storage or display.

**11. Notarisation, acknowledgement and certification.**

(1) A requirement for a signature, statement or document to be notarised, acknowledged, verified or made under oath, is fulfilled if an advanced or secure electronic signature of a person authorised by law to sign or notarise the document is attached, incorporated or is logically associated with the electronic record.

(2) Where a person is required or permitted to provide a certified copy of a document which is in electronic form, the requirement is fulfilled if the person provides a printout certified to be a true copy of the document or information.

(3) Where a person is required or permitted to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is fulfilled if an electronic copy of the document is certified to be a true copy of the document and the certification is confirmed with an advanced electronic signature.

**12. Other requirements.**

(1) A requirement for multiple copies of a document to be submitted to a person at the same time is fulfilled by submitting a single data message which is capable of being reproduced by the person to whom the data message is submitted.

(2) Where a document is required to be sealed and the law does not prescribe the method or form in which it is to be the sealed, the document may be sealed by electronic means.

(3) For purposes of subsection (2) a document is sealed by electronic means if the document includes the advanced electronic signature of the person authorised to seal the document.

(4) Where a person is required or permitted to send a document or information by registered or certified mail, that requirement is fulfilled if an electronic copy of the document or information is sent to an authorised service provider and the document, is registered by the service provider and sent to the electronic address provided by the sender provided that such reproduction does not affect the integrity of the document.

**13. Automated transactions.**

(1) In an automated transaction—

(a) a contract may be formed where an electronic agent performs an action required by law in order to form a contract; or

(b) a contract may be formed by a party to the transaction using an electronic agent to enter into the contract.

(2) A party using an electronic agent to enter into a contract shall, subject to subsection (3), be bound by the terms of the contract irrespective of whether the party reviewed the actions of the electronic agent or the terms of the contract.

(3) A party interacting with an electronic agent to form a contract is not bound by the terms of the contract unless the terms are capable of being reviewed by a person representing that party before the formation of the contract.

(4) A contract shall not be formed under subsection (1) where a person interacts directly with the electronic agent of another party and the electronic agent makes a material error when creating a data message unless—

(a) the other party notifies the natural person of the error as soon as practicable after he or she has learnt of the error;

(b) the electronic agent provides the natural person with an opportunity to prevent or correct the error;

(c) the party takes reasonable steps, including steps that conform to the instructions of the natural person to return any performance received, or, if instructed to do so, to destroy that performance; and

(d) the party has not used or received any material benefit or value from the performance received from the natural person.

**14. Formation and validity of a contract.**

(1) A contract shall not be denied legal effect merely because it is concluded partly or wholly by means of a data message.

(2) A contract by means of a data message is concluded at the time when and the place where acceptance of the offer is received by the person making the offer.

**15. Time of dispatch of data message.**

(1) Subject to an agreement to the contrary, where a data message enters a single information system outside the control of the person originating the data message or a person who sent the message on behalf of the person originating the message, the dispatch of the message occurs when the data message enters the information system.

(2) Where a data message successively enters two or more information systems outside the control of the person originating the data message, unless otherwise agreed between the person originating the message and the addressee, the dispatch of the message occurs when the data message enters the first of the information systems.

**16. Time of receipt of data message.**

(1) Unless otherwise agreed between the person originating the data message and the addressee, the time of receipt of a data message is determined where the addressee designates an information system for receiving a data message the receipt of a data message occurs—

(a) at the time when the data message enters the designated information system; or

(b) if the data message is sent to an information system of the addressee which is not the designated information system, at the time when the data message is received by the addressee.

(2) Where the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Subsections (1) and (2) shall apply notwithstanding that the place where the information system is located is different from the place where the data message is received under section 17.

**17. Place of dispatch or receipt.**

(1) Unless otherwise agreed by the person originating a data message and the addressee, a data message is deemed to have been—

(a) dispatched at the place of business of the originator; and

(b) received at the place of business of the addressee.

(2) For the purposes of subsection (1) the person originating the data message or the addressee—

(a) has more than one place of business—

(i) and one of the places can more closely be associated with the transaction, the place of business which can be closely associated with the transaction is presumed to be the place of business;

(ii) but paragraph (a) does not apply, the principal place of business of the person originating the data message or the addressee is presumed to be the place of business;

(b) does not have a place of business, the place where the person originating the data message or the addressee ordinarily resides is presumed to be the place of business.

**18. Expression of interest.**

An expression of interest may be in the form of a data message and may be without an electronic signature as long as it is possible to infer the interest of the person from the data message.

**19. Attributing a data message to person originating the message.**

(1) A data message is attributed to the person who originated the data message if the message is sent by—

(a) the person originating the message;

(b) an agent of the person originating the message or a person who has the authority to act on behalf of the person originating the data message ; or

(c) an information system which is programmed by the person originating the message or on behalf of the person originating the message to operate automatically unless it is proved that the information system did not execute the programming properly.

(2) The addressee shall regard a data message as sent by the originator and to act on that assumption if—

(a) in order to ascertain whether the data message is sent by the person originating the message, the addressee properly applies a method previously agreed to by the person originating the message for that purpose;

(b) the data message received by the addressee resulted from the action of a person whose relationship with the originator enabled the person to gain access to a method used by the originator to identify electronic records as records of the originator; or

(c) the data message is sent by an agent of the originator.

(3) Subsection (2) shall not apply where—

(a) the addressee receives notice from the originator that the originator did not send the data message;

(b) the addressee knows or ought to have known, had he or she exercised reasonable care or used the agreed method, that the data message was not sent by the originator ;or

(c) in the circumstances it is unreasonable for the addressee to regard the data message as a message of the originator or to act on the assumption that the data message was sent by the originator.

(4) This section shall not affect the law of agency or the law on formation of contracts.

**20. Acknowledgement of receipt of data message.**

(1) Subject to this section, an acknowledgement of receipt of a data message is not necessary to give legal effect to the data message.

(2) Where the originator specifies that the data message is conditional on receipt of the acknowledgement, the data message is taken as not sent, until the acknowledgement is received by the originator.

(3) Where the originator specifies that the data message is conditional on receipt of an acknowledgement and the acknowledgement is not received by the originator within the time specified or agreed upon or, if no time has been specified or agreed upon, within a reasonable time, the originator may—

(a) give notice to the addressee stating that an acknowledgement has not been received and specify a reasonable time within which the acknowledgement should be received; and

(b) upon notice to the addressee, treat the data message as though it has never been sent or exercise any other rights that he or she may have in respect of the data message.

(4) Where the originator does not specify that the acknowledgement is to be given in a particular form or by a particular method, the acknowledgement may be given by—

(a) any communication from the addressee, automated or otherwise; or

(b) any conduct of the addressee which is sufficient to indicate to the originator that the addressee received the data message.

(5) Where the originator receives the acknowledgement of receipt from the addressee, unless there is evidence to the contrary it is presumed, that the addressee received the data message.

(6) The presumption in subsection (5) does not imply that the content of the electronic record corresponds to the content of the record received.

(7) Where the acknowledgement states that the related data message fulfilled the technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(8) Except in so far as it relates to sending or receiving of a data message, this section does not apply to the legal consequences that arise from the data message or from the acknowledgement of its receipt.

**21. Variation of conditions or requirements by agreement.**
Sections 16, 17, 18, 19 or 20 may be varied by an agreement made between the parties involved in generating, sending, storing or processing a data message.

PART III—E-GOVERNMENT SERVICES

**22. Electronic filing and issuing of documents.**
Where a law provides that a public body may—

(a) accept the filing of a document or requires that a document be created or retained;

(b) issue a permit, licence or an approval; or

(c) provide for the making of a payment,

the public body may,

(i) accept the document to be filed, created or retained in the form of a data message;

(ii) issue the permit, licence or approval in electronic form; or

(iii) make or receive payment by electronic means.

**23. Specific requirements by public body.**
(1) A public body may for the purposes of section 22 by notice in the *Gazette,* specify—

(a) the manner and format in which the data message shall be filed, created or retained;

(b) the manner and format in which the permit, licence or approval shall be issued;

(c) where the data message has to be signed, the type of electronic signature required;

(d) the manner and format in which the electronic signature shall be attached to or incorporated into the data message;

(e) the criteria that shall be met by an authentication service provider used by the person filing the data message or that the authentication service provider shall be a preferred authentication service provider;

(f) the appropriate control process and the procedure to ensure adequate integrity, security and confidentiality of a data messages or a payment; and

(g) any other requirements in respect of the data message or payment.

(2) For the purposes of subsection (1) (e) a relevant generic service provider shall be a preferred authentication service provider.

PART IV—CONSUMER PROTECTION

**24. Information to be provided by suppliers or sellers.**

(1) A person offering goods or services for sale, hire or exchange through an electronic transaction shall provide to the consumers on the web site or electronic communication where the goods or services are offered, the following—

(a) the full name and legal status of the person;

(b) the physical address and telephone number of the person;

(c) the web site address or e-mail address of the person;

(d) membership of any self-regulatory or accreditation bodies to which the person belongs or subscribes and the contact details of that body;

(e) any code of conduct to which that person subscribes and how the consumer may access that code of conduct electronically;

(f) in the case of a legal person, the registration number, names of directors and place of registration;

(g) the physical address where the person may be served with documents;

(h) a description of the main characteristics of the goods or services offered by the person which is sufficient to enable a consumer to make an informed decision on the proposed electronic transaction;

(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(j) the manner of payment;

(k) any terms or conditions of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;

(l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;

(m) the manner and period within which consumers may access and maintain a full record of the transaction;

(n) the return, exchange and refund policy of the person;

(o) any alternative dispute resolution code to which the person subscribes and how the code may be accessed electronically by the consumer;

(p) the security procedures and privacy policy of the person in respect of payment, payment information and personal information; and

(q) where appropriate, the minimum duration of the agreement in the case of agreements for the sale, hire, exchange or supply of products or services to be performed on an ongoing basis or recurrently;

(2) A person offering goods or services for sale, hire or exchange through an electronic transaction shall also provide a consumer with an opportunity—

(a) to review the entire electronic transaction;

(b) to correct any mistakes; and

(c) to withdraw from the transaction before placing an order.

(3) Where a person offering goods or services for sale, hire or exchange through an electronic transaction fails to comply with subsection (1) or (2), a consumer may cancel the transaction within fourteen days after receiving the goods or services under the transaction.

(4) Where a transaction is cancelled under subsection (3)—

(a) the consumer shall return the goods to the person who offered the goods or, where applicable, cease using the service; and

(b) the person selling or offering the goods or services shall refund all payments made by the consumer after deducting the direct cost of returning the goods.

(5) For the purposes of subsection (4) (b) the person offering the goods or services shall use a payment system which is secure according to the accepted technological standards at the time of the transaction.

(6) Where a person offering goods or services for sale, hire or exchange by electronic means fails to comply with subsections (4) (b) and (5) he or she is liable for the damage suffered by the consumer

(7) Subsection (3) does not apply to an electronic transaction—

(a) for financial services, including, investment services, insurance and reinsurance operations, banking services and securities;

(b) by way of an auction;

(c) for the supply of foodstuff, beverages or other goods intended for everyday consumption if they are supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day period referred to in section 25(1);

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods—

(i) are made to the specifications of the consumer;

(ii) are clearly personalised;

(iii) by reason of their nature cannot be returned; or

(iv) are likely to deteriorate or expire rapidly;

(g) where audio or video recordings or computer software is unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

**25. Cancelling electronic transaction after receipt of goods or services.**

(1) Subject to sub section (2), a consumer may cancel an electronic transaction and any related credit agreement for the supply of goods or services—

(a) within seven days after the date of receipt of the goods or services; or

(b) within seven days after the date of conclusion of the agreement.

(2) A consumer who returns goods after cancelling an electronic transaction under subsection (1) shall not be charged for the returning of the goods other than the direct cost of returning the goods

(3) Where payment for the goods or services has been effected before a consumer exercises the right to cancel the transaction under subsection (1), the consumer is entitled to a full refund of money paid within thirty days of the date of the cancellation.

(4) This section shall not be construed as prejudicing the rights of a consumer which are provided for in any other law.

**26. Unsolicited goods, services or communications.**

(1) A person who sends an unsolicited commercial communication to a consumer, shall provide—

(a) it at no cost;

(b) the consumer with the option to cancel his or her subscription to the mailing list of that person at no cost.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction to a fine not exceeding seventy two currency points or to imprisonment not exceeding three years or both.

(3) A person who sends an unsolicited commercial communication to a person who has advised the sender that he or she should not send the communication , commits an offence and is liable on conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

**27. Performance of electronic transaction.**.

(1) Where a person makes an order for goods or services by electronic means, unless otherwise agreed by the parties, the supplier shall execute the order within thirty days.

(2) Where the supplier fails to execute the order within thirty days or within the agreed period, the consumer may cancel the order after giving written notice of seven days.

(3) Where the supplier is not able to supply the goods or services, on the ground that the goods or services ordered are not available, he or she shall notify the consumer before the expiry of the agreed time and refund any payment made in respect of the goods or services within thirty days.

**28. Invalidity of provisions excluding consumer rights.**

A provision in an agreement, which excludes any rights provided for in this Part, is void.

PART V—LIMITATION OF LIABLITY OF SERVICE PROVIDERS

**29. Liability of a service provider**

(1) A service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on—

(a) the making, publication, dissemination or distribution of the material or a statement made in the material; or

(b) the infringement of any rights subsisting in or in relation to the material.

(2) This section shall not affect—

(a) an obligation in a contract;

(b) the obligation of a network service provider under a licencing or regulatory framework which is established by law; or

(c) an obligation which is imposed by law or a court to remove, block or deny access to any material.

(3) For the purposes of this section, provides access, in relation to third-party material, means providing the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access.

**30. Information location tools.**

Where a service provider refers or links users to a data message containing an infringing data message or infringing activity, the service provider is not liable for damage incurred by the user if the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;

(b) is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; or

(d) removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

**31. Notification of infringing data message or activity.**

(1) A person who complains that a data message or an activity relating to the data message is unlawful shall notify the service provider or his or her designated agent in writing and the notification shall include—

(a) the full name and address of the person complaining;

(b) the written or electronic signature of the person complaining;

(c) the right that has allegedly been infringed;

(d) a description of the material or activity which is alleged to be the subject of infringing activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephone and electronic contact details of the person complaining;

(g) a declaration that the person complaining is acting in good faith; and

(h) a declaration that the information in the notification is correct to his or her knowledge.

(2) A person who knowingly makes a false statement on the notification in subsection(1) is liable to the service provider for the loss or damage suffered by the service provider.

**32. Service provider not obliged to monitor data**

(1) For the purposes of complying with this Part, a service provider is not obliged to—

(a) monitor the data which the service provider transmits or stores; or

(b) actively seek for facts or circumstances indicating an unlawful activity,

(2) The Minister in consultation with the National Information Technology Authority—Uganda may by statutory instrument, prescribe the procedure for service providers to—

(a) inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service; and

(b) communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority

**33. Territorial Jurisdiction.**

(1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is outside or within Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

**34. Jurisdiction of courts.**

A court presided over by the Chief Magistrate or Magistrate Grade 1 has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the penalty or punishment in respect of any offence under this Act.

**35. Regulations.**

The Minister may, by statutory instrument make regulations for any—

(a) matter which is required to be prescribed;

(b) administrative or procedural matter which is necessary to give effect to this Act; or

(c) matter which is necessary and expedient to give effect to this Act.

**36. Power of the Minister to amend Schedule**

The Minister in consultation with the National Information Technology Authority- Uganda may, by statutory instrument, with the approval of Cabinet amend the Schedules.

SCHEDULE 1

*Section 2.*

Currency point

One currency point is equivalent to twenty thousand shillings.

SCHEDULE 2

*Section 3*

DOCUMENTS NOT COVERED BY THIS ACT:

(a) Will or codicil;
(b) Trust created by a will or codicil;
(c) Power of attorney;
(d) Document that creates or transfers an interest in property and requires regi
stration to be effective against third parties; and
(e) Negotiable instruments, including negotiable documents of title.

# APPENDIX 2

## ELECTRONIC SIGNATURES ACT 2011


10101
010

ACTS
SUPPLEMENT No. 4 18th March, 2011.

ACTS SUPPLEMENT

*to The Uganda Gazette No. 19 Volume CIV dated 18th March, 2011.*

Printed by UPPC, Entebbe, by Order of the Government.

**Act 7** *Electronic Signatures Act* **2011**

# THE ELECTRONIC SIGNATURES ACT, 2011.

## ARRANGEMENT OF SECTIONS

*Section.*

*Section.*

## THE ELECTRONIC SIGNATURES ACT, 2011.

**An Act to make provision for and to regulate the use of electronic signatures and to provide for other related matters.**

DATE OF ASSENT: 17th February, 2011.

*Date of Commencement:* See section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY

**1. Commencement**

This Act shall come into force on a date appointed by the Minister by statutory instrument.

**2. Interpretation**

In this Act, unless the context otherwise requires—

"accept a certificate" means—

(a) to manifest approval of a certificate, while knowing or having notice of its contents; or

(b) to apply to a certification service provider for a certificate, without revoking the application by delivering notice of the revocation to the licensed certification service provider and obtaining a signed, written receipt from the certification service provider, if the certification service provider subsequently issues a certificate based on the application;

"advanced electronic signature" means an electronic signature, which is—

(a) uniquely linked to the signatory;

(b) reliably capable of identifying the signatory;

(c) created using secure signature creation device that the signatory can maintain; and

(d) linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable;

"asymmetric cryptosystem" means an algorithm or series of algorithms, which provide a secure key pair;

"authorised officer" means the Controller or a police officer or a public officer performing any functions under this Act; and includes any public officer authorised by the Minister or by the controller to perform any functions under this Act;

"certificate" means a data message or other records confirming the link between a signatory and a signature creation data;

"certification service provider disclosure record" means an on-line and publicly accessible record that concerns a licensed certification service provider, which is kept by the Controller under subsection 21(5);

"certification practice statement" means a declaration of the practices, which a certification service provider employs in issuing certificates generally or employs in issuing a particular certificate;

"certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

"certify" means to declare with reference to a certificate, with ample opportunity to reflect and with a duty to apprise oneself of all material facts;

"confirm" means to ascertain through diligent inquiry and investigation;

"Controller" means National Information Technology Authority- Uganda;

"correspond", with reference to keys, means to belong to the same key pair;

"currency point" has the meaning assigned to it in the Schedule in this Act;

"digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine—

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) whether the message has been altered since the transformation was made;

"electronic signature" means data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature;

"electronic signature product" means configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures;

"forge a digital signature" means—

(a) to create a digital signature without the authorisation of the rightful holder of the private key; or

(b) to create a digital signature verifiable by a certificate listing as subscriber a person who either does not exist or does not hold the private key corresponding to the public key listed in the certificate;

"hold a private key" means to be able to utilise a private key;

"incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated;

"issue a certificate" means the act of a certification service provider in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate;

"key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates;

"licensed certification service provider" means a certification service provider to whom a licence has been issued by the Controller and whose licence is in effect;

"message" means a digital representation of information;

"Minister" means the Minister responsible for information and communication technology;

"notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person;

"person" includes any company or association or body of persons corporate or unincorporate;

"prescribed" means prescribed by or under this Act or any regulations made under this Act;

"private key" means the key of a key pair used to create a digital signature;

"public key" means the key of a key pair used to verify a digital signature and listed in the digital signature certificate;

"public key infrastructure" means a framework for creating a secure method for exchanging information based on public key cryptography;

"publish" means to record or file in a repository;

"qualified certification service provider" means a certification service provider that satisfies the requirements under section 23;

"recipient" means a person who receives or has a digital signature and is in a position to rely on it;

"recognised date or time stamp service" means a date/time stamp service recognised by the Controller under section 79;

"recognised repository" means a repository recognised by the Controller under section 77;

"recommended reliance limit" means the monetary amount recommended for reliance on a certificate under section 76;

"relying party" means a person that may act on the basis of a certificate or an electronic signature;

"repository" means a system for storing and retrieving certificates and other information relevant to digital signatures;

"revoke a certificate" means to make a certificate ineffective permanently from a specified time forward;

"rightfully hold a private key" means to be able to utilise a private key—

(a) which the holder or the holder's agents have not disclosed to any person in contravention of this act; and

(b) which the holder has not obtained through theft, deceit, eavesdropping or other unlawful means;

"security procedure" means a procedure for the purpose of—

(a) verifying that an electronic record is that of a specific person; or

(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgement procedures or similar security devices;

"secure signature creation device" means a signature creation device which meets the requirements laid down in section 4;

"signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents

"signature creation device" means configured software or hardware, used by the signatory to create an electronic signature;

"signature verification data" means unique data such as codes or public cryptographic keys, used for the purpose of verifying an electronic signature;

"signature verification device" means configured software or hardware, used for the purpose of verifying an electronic signature;

"signed" or "signature" and its grammatical variations includes any symbol executed or adapted or any methodology or procedure employed or adapted, by a person with the intention of authenticating a record, including an electronic or digital method;

"subscriber" means a person who—

(a) is the subject listed in a certificate;

(b) accepts the certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate;

"suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward;

"this Act" includes any regulations made under this Act;

"time-stamp" means—

(a) to append or attach to a message, digital signature or certificate a digitally signed notation indicating at least the date, time and identity of the person appending or attaching the notation; or

(b) the notation appended or attached;

"transactional certificate" means a certificate, incorporating by reference one or more digital signatures, issued and valid for a specific transaction;

"trustworthy system" means computer hardware and software which—

(a) are reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation; and

(c) are reasonably suited to performing their intended functions;

"valid certificate" means a certificate which—

(a) a licensed certification service provider has issued;

(b) has been accepted by the subscriber listed in it;

(c) has not been revoked or suspended; and

(d) has not expired,

but a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference;

"verify a digital signature" means, in relation to a given digital signature, message and public key, to determine accurately that—

(a) the digital signature was created by the private key corresponding to the public key; and

(b) the message has not been altered since its digital signature was created;

"writing" or "written" includes any handwriting, typewriting, printing, electronic storage or transmission or any other method of recording information or fixing information in a form capable of being preserved.

(2) For the purposes of this Act, a certificate shall be revoked by making a notation to that effect on the certificate or by including the certificate in a set of revoked certificates.

(3) The revocation of a certificate does not mean that it is destroyed or made illegible.

**3. Equal treatment of signature technologies.**

Nothing in this Act shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements for a signature in this Act or otherwise meets with the requirements of any other applicable law.

**4. Compliance with a requirement for a signature.**

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of all the circumstances, including any relevant agreement.

(2) Subsection (1) applies whether the requirement referred to in that subsection in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subsection (1) if—

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Subsection (3) does not limit the liability of any person—

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1),the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

**5. Conduct of the signatory.**

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall—

(a) exercise reasonable care to avoid unauthorised use of its signature creation data;

(b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if—

(i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle or which are to be included in the certificate.

**6. Variation by agreement.**

The provisions of this Act may be derogated from or their effect may be varied by agreement unless that agreement would not be valid or effective under any law.

**7. Conduct of the relying party.**

A relying party shall bear the legal consequences of his or her failure to—

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps—

(i) to verify the validity, suspension or revocation of the certificate; and

(ii) to observe any limitation with respect to the certificate.

**8. Trustworthiness.**

When determining whether or to what extent any systems procedures and human resources utilised by a certification service provider are trustworthy, regard may be had to the following factors—

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedure for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the state, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

**9. Conduct of the certification service provider.**

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall—

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate—

(i) the identity of the certification service provider;

(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise—

(i) the method used to identify the signatory;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signatory to give notice under section 4(1);

(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d) (v) are offered, provide a means for a signatory to give notice under section 4(1)(b) and, where services under paragraph d(vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of subsection (1).

**10. Advanced signatures.**

(1) An advanced electronic signature, verified with a qualified certificate, is equal to an autographic signature in relation to data in electronic form and has therefore equal legal effectiveness and admissibility as evidence.

(2) The advanced signature verification process shall ensure that—

(a) the data used for verifying the electronic signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of the verification and identity of the certificate holder is correctly displayed to the verifier;

(c) the verifier can reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are verified;

(e) the use of a pseudonym is clearly indicated;

(f) any security-relevant changes can be detected.

**11. Secure electronic signature.**

Where, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, an electronic signature is executed in a trustworthy manner, reasonably and in good faith relied upon by the relying party, that signature shall be treated as a secure electronic signature at the time of verification to the extent that it can be verified that the electronic signature satisfied, at the time it was made, the following criteria—

(a) the signature creation data used for signature creation is unique and its secrecy is reasonably assured;

(b) it was capable of being used to objectively identify that person;

(c) it was created in a manner or using a means under the sole control of the person using it, that cannot be readily duplicated or compromised;

(d) it is linked to the electronic record to which it relates in such a manner that if the record was changed to electronic signature would be invalidated;

(e) the signatory can reliably protect his or her signature creation data from unauthorised access.

**12. Presumptions relating to secure and advanced electronic signatures.**

(1) In any civil proceedings involving a secure electronic record, it shall be presumed, unless the contrary is proved, that the secure or advanced electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any civil proceedings involving a secure or advanced electronic signature, the following shall be presumed unless the contrary is proved—

(a) the secure or advanced electronic signature is the signature of the person to whom it correlates; and

(b) the secure or advanced electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(3) In the absence of a secure or advanced electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(4) The effect of presumptions provided in this section is to place on the party challenging the genuineness of a secure or advanced electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the court of the fact that the non-existence of the presumed fact is more.

PART III—SECURE DIGITAL SIGNATURES

**13. Secure digital signatures.**

When a portion of an electronic record is signed with a digital signature the digital signature shall be treated as a secure electronic signature in respect of that portion of the record, if—

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to a public key listed in the certificate; and

(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because—

(i) the certificate was issued by a certification service provider operating in compliance with regulations made under this Act;

(ii) the certificate was issued by a certification service provider outside Uganda recognised for the purpose by the Controller pursuant to regulations made under this Act;

(iii) the certificate was issued by a department or ministry of the Government, an organ of state of statutory corporation approved by the minister to act as a certification service provider on such conditions as the regulations may specify; or

(iv) the parties have expressly agreed between themselves to use digital signatures as a security procedure and the digital signature was properly verified by reference to the sender's public key.

**14. Satisfaction of signature requirements.**

(1) Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where—

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification service provider;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer—

(i) has breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(2) Notwithstanding any written law to the contrary—

(a) a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumbprint or any other mark; and

(b) a digital signature created in accordance with this Act shall be taken to be a legally binding signature.

(3) Nothing in this Act shall preclude a symbol from being valid as a signature under any other applicable law.

**15. Unreliable digital signatures.**

(1) Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.

(2) Where the recipient decides not to rely on a digital signature under this section, the recipient shall promptly notify the signer of its determination not to rely on a digital signature and the grounds for that determination.

**16. Digitally signed document taken to be written document.**

(1) A message shall be as valid, enforceable and effective as if it had been written on paper if—

(a) it bears in its entirety a digital signature; and

(b) that digital signature is verified by the public key listed in a certificate which—

(i) was issued by a licensed certification service provider; and

(ii) was valid at the time the digital signature was created.

(2) Nothing in this Act shall preclude any message, document or record from being considered written or in writing under any other applicable law.

**17. Digitally signed document deemed to be original document.**

A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

**18. Authentication of digital signatures.**

A certificate issued by a licensed certification service provider shall be an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgement appear with the digital signature and regardless of whether the signer physically appeared before the licensed certification service provider when the digital signature was created, if that digital signature is—

(a) verifiable by that certificate; and

(b) was affixed when that certificate was valid.

**19. Presumptions in adjudicating disputes.**

In adjudicating a dispute involving a digital signature, a court shall presume—

(a) that a certificate digitally signed by a licensed certification service provider and—

(i) published in a recognised repository; or

(ii) made available by the issuing licensed certification service provider or by the subscriber listed in the certificate, is issued by the licensed certification service provider which digitally signed it and is accepted by the subscriber listed in it;

(b) that the information listed in a valid certificate and confirmed by a licensed certification service provider issuing the certificate is accurate;

(c) that where the public key verifies a digital signature listed in a valid certificate issued by a licensed certification service provider—

(i) that digital signature is the digital signature of the subscriber listed in that certificate;

(ii) that digital signature was affixed by that subscriber with the intention of signing the message; and

(iii) the recipient of that digital signature has no knowledge or notice that the signer—

(aa) has breached a duty as a subscriber; or

(ab) does not rightfully hold the private key used to affix the digital signature; and

(d) that a digital signature was created before it was time-stamped by a recognised date or time stamp service utilising a trustworthy system.

PART IV—PUBLIC KEY INFRASTRUCTURE (PKI)

**20. Sphere of application.**

This Part applies to digital signatures or signatures that are able to use the public key infrastructure (PKI).

**21. Controller.**

(1) The Controller shall, in particular be responsible for monitoring and overseeing the activities of certification service providers and shall perform the functions conferred on the Controller under this Act.

(2) The Controller shall exercise its functions under this Act subject to such directions as to the general policy guidelines as may be given by the Minister.

(3) The Controller shall maintain a publicly accessible database containing a certification service provider disclosure record for each certification service provider, which shall contain all the particulars required under regulations made under this Act.

(4) The Controller shall publish the contents of the database in at least one recognised repository.

**22. Certification service providers to be licensed.**

(1) A person shall not carry on or operate or hold himself out as carrying on or operating, as a certification service provider unless that person has a valid licence issued under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both; and in the case of a continuing offence is in addition liable to a daily fine not exceeding ten currency points for each day the offence continues.

(3) The Minister may, on an application in writing being made in accordance with this Act, exempt a person operating as a certification service provider within an organisation from the requirement of a licence under this section where certificates and key pairs are issued to members of the organisation for internal use only; but the Minister shall not delegate that power to the Controller.

(4) The liability limits specified in Part IV shall not apply to an exempted certification service provider and Part V shall not apply in relation to a digital signature verified by a certificate issued by an exempted certification service provider.

**23. Qualifications of certification aservice providers.**

(1) The Minister in consultation with National Information Technolology Authority- Uganda shall, by regulations made under this Act, prescribe the qualifications required for certification service providers.

(2) The Minister in consultation with National Information Technolology Authority- Uganda may vary or amend the qualifications prescribed under subsection (1) but any such variation or amendment shall not be applied to a certification service provider holding a valid licence under this Act until the expiry of that licence.

**24. Functions of licensed certification service providers.**

(1) The function of a certification service provider shall be to issue a certificate to a subscriber upon application and upon satisfaction of the certification service providers requirements as to the identity of the subscriber to be listed in the certificate and upon payment of the prescribed fees and charges.

(2) The certification service provider shall, before issuing a certificate under this Act, take all reasonable measures to check for proper identification of the subscriber to be listed in the certificate.

**25. Application for licence.**

(1) An application for a licence under this Act shall be made in writing to the Controller in such form as may be prescribed.

(2) An application under subsection (1) shall be accompanied by such documents or information as may be prescribed and the Controller may, at any time after receiving the application and before it is determined, require the applicant to provide such additional documents or information as may be considered necessary by the Controller for the purposes of determining the suitability of the applicant for the licence.

(3) Where any additional document or information required under subsection (2) is not provided by the applicant within the time specified in the requirement or any extension granted by the Controller, the application shall be taken to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

**26. Grant or refusal of licence**.

(1) The Controller shall, on an application having been duly made in accordance with section 25 and after being provided with all the documents and information as he may require, consider the application and when he or she is satisfied that the applicant is a qualified certification service provider and a suitable licensee and upon payment of the prescribed fee, grant the licence with or without conditions or refuse to grant a licence.

(2) A licence granted under subsection (1) shall set out the duration of the licence and the licence number.

(3) The terms and conditions imposed under the licence may at any time be varied for just cause or amended by the Controller but the licensee shall be given a reasonable opportunity of being heard.

(4) The Controller shall notify the applicant in writing of his or her decision to grant or refuse to grant a licence within thirty days of receiving the application.

**27. Revocation of licence.**

(1) The Controller may revoke a licence granted under section 26 if satisfied that—

(a) the certification service provider has failed to comply with an obligation imposed upon it by or under this Act;

(b) the certification service provider has contravened any condition imposed under the licence, any provision of this Act or any other written law;

(c) the certification service provider has, either in connection with the application for the licence or at any time after the grant of the licence, provided the Controller with false, misleading or inaccurate information or a document or declaration made by or on behalf of the certification service provider or by or on behalf of a person who is or is to be a director, Controller or manager of the licensed certification service provider which is false, misleading or inaccurate;

(d) the certification service provider is carrying on its business in a manner which is prejudicial to the interest of the public or to the national economy;

(e) the certification service provider has insufficient assets to meet its liabilities;

(f) a winding up order has been made against the licensed certification service provider or a resolution for its voluntary winding-up has been passed;

(g) the certification service provider or its director, Controller or manager has been convicted of an offence under this Act in his or her capacity as; or

(h) the certification service provider has ceased to be a qualified certification service provider.

(2) Before revoking a licence, the Controller shall give the licensed certification service provider a notice in writing of his or her intention to revoke the licence and require the licensed certification service provider to show cause within thirty days as to why the licence should not be revoked.

(3) Where the Controller decides to revoke the licence, he or she shall notify the certification service provider of his or her decision by a notice in writing within 48 hours of making the decision.

(4) The revocation of a licence shall take effect where there is no appeal against the revocation, on the expiration of thirty days from the date on which the notice of revocation is served on the licensed certification service provider.

(5) Where an appeal has been made against the revocation of a licence, the certification service provider whose licence has been revoked shall not issue any certificates until the appeal has been disposed of and the revocation has been set aside by the Minister but nothing in this subsection shall prevent the certification service provider from fulfilling its other obligations to its subscribers during that period.

(6) A person who contravenes subsection (5) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both.

(7) Where the revocation of a licence has taken effect, the Controller shall, as soon as practicable, cause the revocation to be published in the certification service provider disclosure record he or she maintains for the certification service provider concerned and advertised in at least two English language national daily newspapers for at least three consecutive days.

**28. Appeal.**

(1) A person who is aggrieved by—

(a) the refusal of the Controller to license a certification service provider under section 26 or to renew a licence under section 35; or

(b) the revocation of a licence under section 27,

may appeal in writing to the Minister within thirty days from the date on which the notice of refusal or revocation is served on that person.

(2) The Minister shall, upon receipt of the appeal respond within thirty days.

(3) A person not satisfied with the Minister's decision may appeal to the High Court.

**29. Surrender of licence.**

(1) A certification service provider may surrender its licence by forwarding it to the Controller with a written notice of its surrender.

(2) The surrender shall take effect on the date the Controller receives the licence and the notice under subsection (1) or where a later date is specified in the notice, on that date.

(3) The licensed certification service provider shall, not later than fourteen days after the date referred to in subsection (2), cause the surrender to be published in the certification service provider disclosure record of the certification service provider concerned and advertised in at least two English language national daily newspapers for at least three days consecutive.

**30. Effect of revocation, surrender or expiry of licence.**

(1) Where the revocation of a licence under section 27 or its surrender under section 29 has taken effect or where the licence has expired, the licensed certification service provider shall immediately cease to carry on or operate any business in respect of which the licence was granted.

(2) Notwithstanding subsection (1), the Minister may, on the recommendation of the Controller, authorise the licensed certification service provider in writing to carry on its business for such duration as the Minister may specify in the authorisation for the purpose of winding up its affairs.

(3) Notwithstanding subsection (1), a licensed certification service provider whose licence has expired shall be entitled to carry on its business as if its licence had not expired upon proof being submitted to the Controller that the licensed certification service provider has applied for a renewal of the licence and that such application is pending determination.

(4) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding seventy two currency points or to imprisonment not exceeding ten years or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five currency points for each day the offence continues.

(5) Without prejudice to the Controller's powers under section 26, the revocation of a licence under section 27 or its surrender under section 29 or its expiry shall not affect the validity or effect of any certificate issued by the certification service provider concerned before such revocation, surrender or expiry.

(6) For the purposes of subsection (5), the Controller shall appoint another licensed certification service provider to take over the certificates issued by the certification service provider whose licence has been revoked or surrendered or has expired and the certificate shall, to the extent that they comply with the requirements of the appointed licensed certification service provider, be deemed to have been issued by that licensed certification service provider.

(7) Subsection (6) shall not preclude the appointed licensed certification service provider from requiring the subscriber to comply with its requirements in relation to the issue of certificates or from issuing a new certificate to the subscriber for the unexpired period of the original certificate except that any additional fees or charges to be imposed shall only be imposed with the prior written approval of the Controller.

**31. Effect of lack of licence.**

(1) The liability limits specified in Part IV shall not apply to unlicensed certification service providers.

(2) Part V shall not apply in relation to an electronic signature, which cannot be verified by a certificate issued by a licensed certification service provider.

(3) In any other case, unless the parties expressly provide otherwise by contract between themselves, the licensing requirements under this Act shall not affect the effectiveness, enforceability or validity of any digital signature.

**32. Return of licence.**

(1) Where the revocation of a licence under section 27 has taken effect or where the licence has expired and no application for its renewal has been submitted within the period specified or where an application for renewal has been refused under section 35, the licensed certification service provider shall within fourteen days return the licence to the Controller.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding seventy two eight currency points or to imprisonment not exceeding three years or to both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five currency points for each day the offence continues and the court shall retain the licence and forward it to the Controller.

**33. Restricted licence.**

(1) The Controller may classify licences according to specified limitations including—

(a) maximum number of outstanding certificates;

(b) cumulative maximum of recommended reliance limits in certificates issued by the licensed certification service provider; and

(c) issuance only within a single firm or organisation.

(2) The Controller may issue licences restricted according to the limits of each classification.

(3) A licensed certification service provider that issues a certificate exceeding the restrictions of its licence commits an offence.

(4) Where a licensed certification service provider issues a certificate exceeding the restrictions of its licence, the liability limits specified in Part IV shall not apply to the licensed certification service provider in relation to that certificate.

(5) Nothing in subsection (3) or (4) shall affect the validity or effect of the issued certificate.

**34. Restriction on use of expression "certification service provider".**

(1) Except with the written consent of the Controller, a person shall not being a licensed certification service provider, assume or use the expressions "certification service provider" or "licensed certification service provider", as the case may be or any derivative of those expressions in any language or any other words in any language capable of being construed as indicating the carrying on or operation of such business, in relation to the business or any part of the business carried on by that person or make any representation to that effect in any bill head, letter, paper, notice, advertisement or in any other manner.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one hundred sixty eight currency points or to imprisonment not exceeding seven years or to both.

**35. Renewal of licence.**

(1) A licensed certification service provider shall submit an application to the Controller in such form as may be prescribed for the renewal of its licence at least thirty days before the date of expiry of the licence and the application shall be accompanied by such documents and information as may be required by the Controller.

(2) The prescribed fee shall be payable upon approval of the application.

(3) Where a licensed certification service provider has no intention of renewing its licence, the licensed certification service provider shall, at least thirty days before the expiry of the licence, publish the intention in the certification service provider disclosure record of the certification service provider concerned and advertise such intention in at least two English language national daily newspapers for at least five consecutive days.

(4) Without prejudice to any other grounds, the Controller may refuse to renew a licence where the requirements of subsection (1) have not been complied with.

**36. Lost license.**

(1) Where a certification service provider has lost its license, it shall immediately notify the Controller in writing of the loss.

(2) The certification service provider shall, as soon as practicable, submit an application for a replacement license accompanied by all such information and documents as may be required by the Controller together with the prescribed fee.

**37. Recognition of other licenses.**

(1) The Controller may recognise, by order published in the *Gazette,* certification service providers licensed or otherwise authorised by entities outside Uganda that satisfy the prescribed requirements.

(2) Where a license or other authorisation of an entity is recognised under subsection (1)—

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification service provider licensed or otherwise authorised by such an entity shall have effect in the same manner as a recommended reliance limit specified in a certificate issued by a certification service provider of Uganda; and

(b) Part IV shall apply to the certificates issued by the certification service provider licensed or otherwise authorised by such entity in the same manner as it applies to a certificate issued by a certification service provider of Uganda.

**38. Performance audit.**

(1) The operations of a certification service provider shall be audited a least once a year to evaluate its compliance with this Act.

(2) The audit shall be carried out by an internationally recognised computer security professional or a certified public accountant having expertise in the relevant field.

(3) The qualifications of the auditors and the procedure for an audit shall be as may be prescribed by regulations made under this Act.

(4) The Controller shall maintain and publish, the date and result of the audit in the certification service provider disclosure record he or she maintains for the certification service provider concerned.

**39. Activities of certification service providers.**

(1) A certification service provider shall only carry on such activities as may be specified in its license.

(2) A certification service provider shall carry on its activities in accordance with this Act and any regulations made under this Act.

**40. Requirement to display license.**

A certification service provider shall at all times display its license in a conspicuous place at its place of business and on its website.

**41. Requirement to submit information on business operations.**

(1) A licensed certification service provider shall submit to the Controller such information and particulars including financial statements, audited balance sheets and profit and loss accounts relating to its entire business operations as may be required by the Controller within the time he or she may determine.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding twenty four currency points or imprisonment not exceedingone year or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two currency points for each day the offence continues.

**42. Notification of change of information.**

(1) A certification service provider shall, before making an amendment or alteration to any of its constituent documents or before any change in its director or chief executive officer, furnish the Controller particulars in writing of any proposed amendment, alteration or change.

(2) A licensed certification service provider shall immediately notify the Controller of any amendment or alteration to any information or document which has been furnished to the Controller in connection with the licence.

**43. Use of trustworthy systems.**

(1) A certification service provider shall only use a trustworthy system—

(a) to issue, suspend or revoke a certificate;

(b) to publish or give notice of the issuance, suspension or revocation of a certificate; and

(c) to create a private key, whether for itself or for a subscriber.

(2) A subscriber shall only use a trustworthy system to create a private key.

**44. Disclosures on inquiry.**

(1) A certification service provider shall, on an inquiry being made to it under this Act, disclose any material certification practice statement and any fact material to either the reliability of a certificate, which it has issued or its ability to perform its services.

(2) A certification service provider may require a signed, written and reasonably specific inquiry from an identified person and payment of the prescribed fee, as conditions precedent to effecting a disclosure required under subsection (1).

**45. Prerequisites to issue of certificate to subscriber.**

(1) A certification service provider may issue a certificate to a subscriber where the following conditions are satisfied—

(a) the certification service provider has received a request for issuance signed by the prospective subscriber; and

(b) the certification service provider has confirmed that—

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber has duly authorised the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(2) The requirements of subsection (1) shall not be waived or disclaimed by the certification service provider, the subscriber or both.

**46. Publication of issued and accepted certificate.**

(1) Where the subscriber accepts the issued certificate, the certification service provider shall publish a signed copy of the certificate in a recognised repository, as the certification service provider and the subscriber named in the certificate may agree, unless a contract between the certification service provider and the subscriber provides otherwise.

(2) Where the subscriber does not accept the certificate, a certification service provider shall not publish it or shall cancel its publication if the certificate has already been published.

**47. Adoption of more rigorous requirements permitted.**
Nothing in sections 31 and 32 shall preclude a certification service provider from conforming to standards, certification practice statements, security plans or contractual requirements more rigorous than, but nevertheless consistent with, this Act.

**48. Suspension or revocation of certificate for faulty issuance.**

(1) Where after issuing a certificate a certification service provider confirms that it was not issued in accordance with sections 31 and 32, the certification service provider shall immediately revoke it.

(2) A certification service provider may suspend a certificate which it has issued for a reasonable period not exceeding forty-eight hours as may be necessary for an investigation to be carried out to confirm the grounds for a revocation under subsection (1).

(3) The certification service provider shall immediately notify the subscriber of a revocation or suspension under this section.

**49. Suspension or revocation of certificate by order.**

(1) The Controller may order the certification service provider to suspend or revoke a certificate where the Controller determines that—

(a) the certificate was issued without compliance with sections 31 and 32; and

(b) the non-compliance poses a significant risk to persons reasonably relying on the certificate.

(2) Before making a determination under subsection (1), the Controller shall give the licensed certification service provider and the subscriber a reasonable opportunity of being heard.

(3) Notwithstanding subsections (1) and (2), where in the opinion of the Controller there exists an emergency that requires an immediate remedy, the Controller may, after consultation with the Minister, suspend a certificate for a period not exceeding forty-eight hours.

**50. Warranties to subscriber.**

(1) By issuing a certificate, a certification service provider warrants to the subscriber named in the certificate that—

(a) the certificate contains no information known to the certification service provider to be false;

(b) the certificate satisfies all the requirements of this Act; and

(c) the certification service provider has not exceeded any limits of its licence in issuing the certificate.

(2) A certification service provider shall not disclaim or limit the warranties under subsection (1).

**51. Continuing obligations to subscriber.**

Unless the subscriber and certification service provider otherwise agree, a certification service provider, by issuing a certificate, promises to the subscriber—

(a) to act promptly to suspend or revoke a certificate in accordance with Part IV; and

(b) to notify the subscriber within a reasonable time of any facts known to the licensed certification service provider, which significantly affect the validity or reliability of the certificate once it is issued.

**52. Representations upon issuance.**

By issuing a certificate, a certification service provider certifies to all who reasonably rely on the information contained in the certificate that—

(a) the information in the certificate and listed as confirmed by the licensed certification service provider is accurate;

(b) all information foreseeable and material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) the subscriber has accepted the certificate; and

(d) the certification service provider has complied with all applicable laws governing the issue of the certificate.

**52. Representations upon publication.**
By publishing a certificate, a certification service provider certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the licensed certification service provider has issued the certificate to the subscriber.

**54. Implied representations by subscriber.**
By accepting a certificate issued by a certification service provider, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that—

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) all representations made by the subscriber to the certification service provider and material to information listed in the certificate are true; and

(c) all material representations made by the subscriber to a certification service provider or made in the certificate and not confirmed by the certification service provider in issuing the certificate are true.

**55. Representations by agent of subscriber.**
By requesting on behalf of a principal the issue of a certificate naming the principal as subscriber, the requesting person certifies in that person's own right to all who reasonably rely on the information contained in the certificate that the requesting person—

(a) holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(b) has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

**56. Disclaimer or indemnity limited.**

A person shall not disclaim or contractually limit the application of this part, nor obtain indemnity for its effects, if the disclaimer, limitation or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

**57. Indemnification of certification service provider by subscriber.**

(1) By accepting a certificate, a subscriber undertakes to indemnify the issuing licensed certification service provider for any loss or damage caused by issue or publication of the certificate in reliance on—

(a) a false and material representation of fact by the subscriber; or

(b) the failure by the subscriber to disclose a material fact, if the representation or failure to disclose was made either with intent to deceive the certification service provider or a person relying on the certificate or with negligence.

(2) Where the certification service provider issued the certificate at the request of one or more agents of the subscriber, the agent or agents personally undertake to indemnify the certification service provider under this section, as if they were accepting subscribers in their own right.

(3) The indemnity provided in this section shall not be disclaimed or contractually limited in scope.

**58. Certification of accuracy of information given.**

When obtaining information from a subscriber which is material to the issue of a certificate, the certification service provider may require the subscriber to certify the accuracy of the relevant information under oath or affirmation.

**59. Duty of subscriber to keep private key secure.**
By accepting a certificate issued by a certification service provider, the subscriber named in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorised to create the subscriber's digital signature.

**60. Property in private key.**
A private key is the personal property of the subscriber who rightfully holds it.

**61. Fiduciary duty of a certification service provider.**
Where a certification service provider holds the private key corresponding to a public key listed in a certificate which it has issued, the certification service provider shall hold the private key as a fiduciary of the subscriber named in the certificate and may use that private key only with the subscriber's prior written approval, unless the subscriber expressly and in writing grants the private key to the licensed certification service provider and expressly and in writing permits the licensed certification service provider to hold the private key according to other terms.

**62. Suspension of certificate by certification service provider.**
(1) Unless the certification service provider and the subscriber agree otherwise, the licensed certification service provider, which issued a certificate, which is not a transactional certificate, shall suspend the certificate for a period not exceeding forty-eight hours—

(a) upon request by a person identifying himself as the subscriber named in the certificate or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee or member of the immediate family of the subscriber; or

(b) by order of the Controller under section 35.

(2) The certification service provider shall take reasonable measures to check the identity or agency of the person requesting suspension.

**63. Suspension of certificate by Controller**.

(1) Unless the certificate provides otherwise or the certificate is a transactional certificate, the Controller may suspend a certificate issued by a certification service provider for a period of forty-eight hours, if—

(a) a person identifying himself or herself as the subscriber named in the certificate or as an agent, business associate, employee or member of the immediate family of the subscriber requests suspension; and

(b) the requester represents that the certification service provider, which issued the certificate, is unavailable.

(2) The Controller may require the person requesting suspension to provide evidence, including a statement under oath or affirmation regarding his or her identity and authorisation and the unavailability of the issuing licensed certification service provider and may decline to suspend the certificate in his or her discretion.

(3) The Controller or other law enforcement agency may investigate suspensions by the Controller for possible wrongdoing by persons requesting suspension.

**64. Notice of suspension.**

(1) Upon suspension of a certificate by a certification service provider, the certification service provider shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the certification service provider shall publish signed notices of the suspension in all those repositories.

(3) Where any repository specified no longer exists or refuses to accept publication or if no such repository is recognised under section 69 the certification service provider shall also publish the notice in a recognised repository.

(4) Where a certificate is suspended by the Controller, the Controller shall give notice as required in this section for a certification service provider if the person requesting suspension pays in advance any prescribed fee required by a repository for publication of the notice of suspension.

**65. Termination of suspension initiated by request.**

A certification service provider shall terminate a suspension initiated by request—

(a) where the subscriber named in the suspended certificate requests termination of the suspension, only if the certification service provider has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorised to terminate the suspension; or

(b) where the licensed certification service provider discovers and confirms that the request for the suspension was made without authorisation by the subscriber.

**66. Alternate contractual procedures.**

(1) The contract between a subscriber and a licensed certification service provider may limit or preclude requested suspension by the certification service provider or may provide otherwise for termination of a requested suspension.

(2) Where the contract limits or precludes suspension by the Controller when the issuing licensed certification service provider is unavailable, the limitation or preclusion shall be effective only if notice of it is published in the certificate.

**67. Effect of suspension of certificate.**

Nothing in this Part shall release the subscriber from the duty under section 47 to keep the private key secure while a certificate is suspended.

**68. Revocation on request.**

(1) A licensed certification service provider shall revoke a certificate, which it issued but which is not a transactional certificate—

(a) upon receiving a request for revocation by the subscriber named in the certificate; and

(b) upon confirming that the person requesting revocation is that subscriber or is an agent of that subscriber with authority to request the revocation.

(2) A certification service provider shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity of the person requesting the revocation or of the agent.

**69. Revocation on subscriber's demise.**

A licensed certification service provider shall revoke a certificate which it issued—

(a) upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead; or

(b) upon presentation of documents effecting a dissolution of the subscriber or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

**70. Revocation of unreliable certificates.**

(1) A licensed certification service provider may revoke one or more certificates, which it issued if the certificates are or become unreliable regardless of whether the subscriber consents to the revocation and notwithstanding any provision to the contrary in a contract between the subscriber and the licensed certification service provider.

(2) Nothing in subsection (1) shall prevent the subscriber from seeking damages or other relief against the licensed certification service provider in the event of wrongful revocation.

**71. Notice of revocation.**

(1) Upon revocation of a certificate by a licensed certification service provider, the licensed certification service provider shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

(2) Where one or more repositories are specified, the licensed certification service provider shall publish signed notices of the revocation in all such repositories.

(3) Where any repository specified no longer exists or refuses to accept publication or if no such repository is recognised under section 69, the licensed certification service provider shall also publish the notice in a recognised repository.

**72. Effect of revocation request on subscriber.**

Where a subscriber has requested for the revocation of a certificate, the subscriber ceases to certify as provided in Part IV and has no further duty to keep the private key secure as required under section 59—

(a) when notice of the revocation is published as required under section 71; or

(b) where forty eight hours have lapsed after the subscriber requests for the revocation in writing, supplies to the issuing licensed certification service provider information reasonably sufficient to confirm the request and pays any prescribed fee, whichever occurs first.

**73. Effect of notification on certification service provider.**

Upon notification as required under section 71, a certification service provider shall be discharged of its warranties based on issue of the revoked certificate and ceases to certify as provided in sections 22 and 24 in relation to the revoked certificate.

**74. Expiration of certificate.**

(1) The date of expiry of a certificate shall be specified in the certificate.

(2) A certificate may be issued for a period not exceeding three years from the date of issue.

(3) When a certificate expires, the subscriber and licensed certification service provider shall cease to certify as provided under this Act and the licensed certification service provider shall be discharged of its duties based on issue in relation to the expired certificate.

(4) The expiry of a certificate shall not affect the duties and obligations of the subscriber and licensed certification service provider incurred under and in relation to the expired certificate.

**75. Reliance limit.**

(1) A licensed certification service provider shall, when issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed certification service provider may specify different limits in different certificates as it considers fit.

**76. Liability limits for certification service providers.**

Unless a licensed certification service provider waives the application of this section, a licensed certification service provider—

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification service provider complied with the requirements of this Act;

(b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either—

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification service provider is required to confirm; or

(ii) failure to comply with sections 31 and 32 when issuing the certificate.

**77. Recognition of repositories.**

(1) The Controller may recognise one or more repositories, after determining that a repository to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognition of repositories shall be as prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised repositories in such form and manner as he or she may determine.

**78. Liability of repositories.**

(1) Notwithstanding any disclaimer by the repository or a contract to the contrary between the repository and a licensed certification service provider or a subscriber, a repository shall be liable for a loss incurred by a person reasonably relying on an electronic signature verified by the public key listed in a suspended or revoked certificate, if loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation and the repository had failed to publish the notice when the person relied on the digital signature.

(2) Unless waived, a recognised repository or the owner or operator of a recognised repository—

(a) shall not be liable for failure to record publication of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(b) shall not be liable under subsection (1) in excess of the amount specified in the certificate as the recommended reliance limit;

(c) shall not be liable for misrepresentation in a certificate published by a certification service provider;

(d) shall not be liable for accurately recording or reporting information which a licensed certification service provider, a court or the Controller has published as required or permitted under this Act, including information about the suspension or revocation of a certificate; and

(e) shall not be liable for reporting information about a certification service provider, a certificate or a subscriber, if the information is published as required or permitted under this Act or is published by order of the Controller in the performance of his or her licensing and regulatory duties under this Act.

**79. Recognition of date or time stamp services.**

(1) The Controller may recognise one or more date or time stamp services, after determining that a service to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognising of date or time stamp services shall be as may be prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised date or time stamp services in a form and manner as he may determine.

PART V—MISCELLANEOUS

**80. Prohibition against dangerous activities**

(1) A certification service provider, whether licensed or not, shall not conduct its business in a manner that creates an unreasonable risk of loss to the subscribers of the certification service provider, to persons relying on certificates issued by the certification service provider or to a repository.

(2) The Controller may publish in one or more recognised repositories brief statements advising subscribers, persons relying on digital signatures and repositories about any activities of a certification service provider, whether licensed or not, which create a risk prohibited under subsection (1).

(3) The certification service provider named in a statement as creating or causing a risk may protest the publication of the statement by filing a brief written defence.

(4) On receipt of a protest made under subsection (3), the Controller shall publish a written defence together with the Controller's statement and shall immediately give the protesting certification service provider notice and a reasonable opportunity of being heard.

(5) Where, after a hearing, the Controller determines that the publication of the advisory statement was unwarranted, the Controller shall revoke the advisory statement.

(6) Where, after a hearing, the Controller determines that the advisory statement is no longer warranted, the Controller shall revoke the advisory statement.

(7) Where, after a hearing, the Controller determines that the advisory statement remains warranted, the Controller may continue or amend the advisory statement and may take further legal action to eliminate or reduce the risk prohibited under subsection (1).

(8) The Controller shall publish his decision under subsection (5), (6) or (7), as the case may be, in one or more recognised repositories.

**81. Obligation of confidentiality**

(1) Except for the purpose of this Act or for any prosecution for an offence under any written law or under an order of court, a person under any powers conferred under this Act, shall not obtain access to any electronic record, book, register, correspondence, information, document, other material or grant access to any other person.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one hundred twenty currency points or imprisonment for a term not exceeding five years or both.

**82. False information.**

A person who knowingly makes, orally or in writing, signs or furnishes any declaration, return, certificate or other document or information required under this Act which is false or misleading in any particular way commits an offence and is liable, on conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment for a term not exceeding five years or both.

**83. Offences by body corporate.**

(1) Where a body corporate commits an offence under this Act, a person who at the time of the commission of the offence is a director, manager, secretary or other similar officer of the body corporate or was purporting to act in that capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management—

(a) may be charged severally or jointly in the same proceedings with the body corporate; and

(b) where the body corporate is convicted of the offence, such a person shall be deemed to have committed an offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves—

(i) that the offence was committed without his knowledge, consent or connivance; and

(ii) that he took all reasonable precautions and had exercised due diligence to prevent the commission of the offence.

(2) Where a person is liable under this Act to a punishment or penalty for any act, omission, neglect or default, he or she is liable to the same punishment or penalty for every such act, omission, neglect or default of any employee or agent of his or of the employee of such agent, if the act, omission, neglect or default was committed—

(a) by his employee in the course of his employment;

(b) by the agent when acting on his behalf; or

(c) by the employee of such agent in the course of his employment by such agent or otherwise on behalf of the agent.

**84. Authorised officer.**
An authorised officer may exercise the powers of enforcement under this Act.

**85. Power to investigate.**
(1) The Controller may investigate the activities of a certification service provider material to its compliance with this Act.

(2) For the purposes of subsection (1), the Controller may issue orders to a certification service provider to further its investigation and secure compliance with this Act.

(3) Further, in any case relating to the commission of an offence under this Act, any authorised officer carrying on an investigation may exercise all or any of the special powers in relation to police investigation in all cases given by the Criminal Procedure Code.

**86. Search by warrant.**
(1) If it appears to a Magistrate, upon written information on oath and after such inquiry as he or she considers necessary, that there is reasonable cause to believe that an offence under this Act is being or has been committed on any premises, the Magistrate may issue a warrant authorising any police officer not below the rank of Inspector or any authorised officer named in the warrant, to enter the premises at any reasonable time by day or by night, with or without assistance and if need be by force, to search for and seize—

(a) copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed;

(b) any signboard, card, letter, pamphlet, leaflet, notice or other device representing or implying that the person is a licensed certification service provider; and

(c) any other document, article or item that is reasonably believed to furnish evidence of the commission of that offence.

(2) A police officer or an authorised officer conducting a search under subsection (1) may, if in his or her opinion it is reasonably necessary to do so for the purpose of investigating into the offence, search any person who is in or on those premises.

(3) A police officer or an authorised officer making a search of a person under subsection (2) may seize, detain or take possession of any book, accounts, document, computerised data, card, letter, pamphlet, leaflet, notice, device, article or item found on that person for the purpose of the investigation being carried out by that officer.

(4) A female person shall not be searched under this section except by another female person.

(5) Where, by reason of its nature, size or amount, it is not practicable to remove any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item seized under this section, the seizing officer shall, by any means, seal that book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item in the premises or container in which it is found.

(6) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (5) or removes any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item under seal or attempts to do so commits an offence.

**87. Search and seizure without warrant.**

If a police officer not below the rank of Inspector in any of the circumstances referred to in section 86 has reasonable cause to believe that by reason of delay in obtaining a search warrant under that section the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, that officer may enter the premises and exercise in, upon and in respect of the premises all the powers referred to in section 86 in as full and ample a manner as if he or she were authorised to do so by a warrant issued under that section.

**88. Access to computerised data.**

(1) A police officer conducting a search under section 86 or 87 shall be given unlimited access to computerised data whether stored in a computer or otherwise.

(2) For the purposes of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data.

**89. List of things seized.**

(1) Except as provided in subsection (2), where any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item is seized under section 86 or 87, the seizing officer shall prepare a list of the things seized and immediately deliver a copy of the list signed by him or her to the occupier of the premises which have been searched or to his or her agent or servant, at those premises.

(2) Where the premises are unoccupied, the seizing officer shall post a list of things seized conspicuously on the premises and leave a copy with the local authorities.

**90. Obstruction of authorised officer.**

A person who obstructs, impedes, assaults or interferes in any way with any authorised officer in the performance of his functions under this Act commits an offence.

**91. Additional powers**.

An authorised officer may, for the purposes of the execution of this Act, to do all or any of the following—

(a) require the production of records, accounts, computerised data and documents kept by a licensed certification service provider and to inspect, examine and copy any of them;

(b) require the production of any identification document from a person in relation to any case or offence under this Act;

(c) make such inquiry as may be necessary to ascertain whether the provisions of this Act have been complied with.

**92. General penalty.**

(1) A person who commits an offence under this Act for which no penalty is expressly provided is liable, on conviction, to a fine not exceeding seventy two currency points or to imprisonment for a term not exceeding three years or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two currency points for each day the offence continues.

(2) For the purposes of this section, "this Act" does not include the regulations made under this Act.

**93. Institution and conduct of prosecution.**

(1) A prosecution under this Act shall not be instituted except by or with the consent of the Director of Public Prosecution, but a person charged with such an offence may be arrested or a warrant for his or her arrest issued and executed and the person may be detained or released on police bond, not withstanding that the consent of the Director of Public Prosecution to the institution of a prosecution for the offence has not yet been obtained, but no further or other proceedings shall be taken until that consent has been obtained.

(2) An officer of the Controller duly authorised in writing by the Director of Public Prosecutions may conduct the prosecution for any offence under this Act.

**94. Jurisdiction to try offences.**
Notwithstanding any written law to the contrary, a Magistrate Grade I shall have jurisdiction to try an offence under this Act and to impose the full punishment for the offence.

**95. Protection of officers.**
An action or prosecution shall not be brought, instituted or maintained in a court against the Controller or any officer duly authorised under this Act for or on account of or in respect of any act ordered or done for the purpose of carrying into effect this Act.

**96. Limitation on disclaiming or limiting application of Act.**
Unless it is expressly provided for under this Act, a person shall not disclaim or contractually limit the application of this Act.

**97. Regulations**.
(1) The Minister may on the recommendation of the Controller make regulations for all or any of the following purposes—

(a) prescribing the qualification requirements for certification service providers;

(b) prescribing the manner of applying for licences and certificates under this Act, the particulars to be supplied by an applicant, the manner of licensing and certification, the fees payable there for, the conditions or restrictions to be imposed and the form of licences and certificates;

(c) regulating the operations of licensed certification service provider;

(d) prescribing the requirements for the content, form and sources of information in certification service provider disclosure records, the updating and timeliness of such information and other practices and policies relating to certification service provider disclosure records;

(e) prescribing the form of certification practice statements;

(f) prescribing the qualification requirements for auditors and the procedure for audits;

(g) prescribing the requirements for repositories and the procedure for recognition of repositories;

(h) prescribing the requirements for date and time stamp services and the procedure for recognition of date and time stamp services;

(i) prescribing the procedure for the review of software for use in creating digital signatures and of the applicable standards in relation to digital signatures and certification practice and for the publication of reports on such software and standards;

(j) prescribing the forms for the purposes of this Act;

(k) prescribing the fees and charges payable under this Act and the manner for collecting and disbursing the fees and charges;

(l) providing for such other matters as are contemplated by or necessary for giving full effect to, the provisions of this Act and for their due administration.

(2) Regulations made under subsection (1) may prescribe any act in contravention of the regulations to be an offence and may prescribe in relation to the offence, penalties not exceeding a fine of seventy two currency points or imprisonment for three years or both.

**98. Compensation.**
Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

**99. Power of Minister to amend the Schedule.**
The Minister may, with the approval of Cabinet, by statutory instrument, amend the Schedule to this Act.

**100. Savings and transitional provisions.**

(1) A certification service provider that has been carrying on or operating as a certification service provider before the commencement of this Act shall, not later than three months from the commencement, obtain a licence under this Act.

(2) Where a certification service provider referred to in subsection (1) fails to obtain a licence after the period prescribed in subsection (1), it shall be taken to be an unlicensed certification service provider and the provisions of this Act shall apply to it and a certificate issued by it accordingly.

(3) Where a certification service provider referred to in subsection (1) has obtained a licence in accordance with this Act within the period prescribed in subsection (1), all certificates issued by that certification service provider before the commencement of this Act, to the extent that they are not inconsistent with this Act, shall be taken to have been issued under this Act and shall have effect accordingly.

SCHEDULE

*Section 2*

CURRENCY POINT

One currency point is equivalent to twenty thousand shillings.

# APPENDIX 3

## THE COMPUTER MISUSE ACT 2011

**ACTS**
**SUPPLEMENT No. 2** **14th Febuary, 2011.**

**ACTS SUPPLEMENT**

*to The Uganda Gazette No. 10 Volume CIV dated 14th February, 2011.*

Printed by UPPC, Entebbe, by Order of the Government.

**Act 2** *Computer Misuse Act* **2011**

# THE COMPUTER MISUSE ACT, 2011.

## ARRANGEMENT OF SECTIONS.

PART I—PRELIMINARY.

*Section.*

*Section.*

## THE COMPUTER MISUSE ACT, 2011

**An Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters**.

DATE OF ASSENT: 1st November, 2010.

*Date of Commencement:* See Section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY.

**1. Commencement.**
This Act shall come into force on a date appointed by the Minister by statutory instrument

**2. Interpretation.**
In this Act, unless the context otherwise requires—

"access" means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective;

"application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;

"authorised officer" has the meaning assigned to it in section 28;

"child" means a person under the age of eighteen years;

"computer" means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices;

"computer output" or "output" means a statement, information or representation, whether in written, printed, pictorial, graphical or other form—

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced from a computer;

"computer service" includes computer time, data processing and the storage retrieval of data;

"content" includes components of computer hardware and software;

"currency point" means the value of a currency point specified in the Schedule;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(a) causes any loss;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data" means electronic representations of information in any form;

"data message" means data generated, sent, received or stored by computer means; and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"electronic device", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"electronic record" means data which is recorded or stored on any medium in or by a computer or other similar device, that can be read or perceived by a person or a computer system or other similar device and includes a display, printout or other out put of that data;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;

"information system services" includes a provision of connections, operation facilities, for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer or acquiring the substance, meaning or purport of such a function;

"Minister" means the Minister responsible for information and communications technology;

"person" includes any company or association or body of persons corporate or unincorporate;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"traffic data" means any computer data relating to communication by means of a computer system generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

PART II—GENERAL PROVISIONS.

**3. Securing access.**

A person secures access to any program or data held in a computer if that person—

(a) views, alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses or destroys it; or

(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

**4. Using a program.**

A person uses a program if the function he or she causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

**5. Authorised access.**

Access by a person to any program or data held in a computer is authorised if—

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access that program or data from any person who is charged with giving that consent.

**6. References.**

(1) A reference to a program or data held in a computer includes a reference to any program or data held in any removable storage medium and a computer may be regarded as containing any program or data held in any such medium.

(2) A reference to a program includes a reference to part of a program.

**7. Modification of contents.**

A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer connected to it result into—

(a) a program, data or data message held in the computer concerned being altered or erased; or

(b) a program, data or data message being added to its contents.

**8. Unauthorised modification.**

Modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from a person who is entitled.

PART III—INVESTIGATIONS AND PROCEDURES.

**9. Preservation Order.**

(1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.

**10. Disclosure of preservation Order.**

The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.

**11. Production Order.**

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling—

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

PART III—COMPUTER MISUSE OFFENCES.

**12. Unauthorised access.**

(1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a manner that causes the program or data to be modified, damaged, destroyed or rendered ineffective, commits an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence.

(4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data, commits an offence.

(5) A person who accesses any information system so as to constitute a denial including a partial denial of service to legitimate users commits an offence.

(6) The intent of a person to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

**13. Access with intent to commit or facilitate the commission of a further offence.**

(1) A person who commits any acts specified under section 12 with intent to—

(a) commit any other offence; or

(b) facilitate the commission of any other offence,

commits an offence.

(2) The offence to be facilitated under subsection (1)(b) may be one committed by the person referred to in subsection (1) or by any other person.

(3) It is immaterial for the purposes of this section whether the act under this section is committed on the same occasion as the offence under section 12 or on any future occasion.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

**14. Unauthorised modification of computer material.**

(1) A person who—

(a) does any act which causes an unauthorised modification of the contents of any computer; and

(b) has the requisite intent and the requisite knowledge at the time when he or she does the act,

commits an offence.

(2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer and by doing so—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent under subsection (1)(b) need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification that the person intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind specified in subsection (2) is intended to be permanent or temporary.

(6) A person who commits an offence under this section is liable on conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

**15. Unauthorised use or interception of computer service.**

(1) Subject to subsection (2), a person who knowingly—

(a) secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device whether similar or not; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

**16. Unauthorised obstruction of use of computer.**

A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

**17. Unauthorised disclosure of access code.**

(1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

**18. Unauthorised disclosure of information.**

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

**19. Electronic fraud.**

(1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) For the purposes of this section "electronic fraud" means deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

**20. Enhanced punishment for offences involving protected computers.**

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 12, 14, 15 or 16, the person convicted of an offence is, instead of the punishment prescribed in those sections, liable on conviction, to imprisonment for life.

(2) For the purposes of subsection (1), a computer is treated as a "protected computer" if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for—

(a) the security, defence or international relations of Uganda;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2).

**21. Abetment and attempts.**

(1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

(2) Any person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

**22. Attempt defined.**

(1) When a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

(2) It is immaterial—

(a) except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention; or

(b) that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.

**23. Child pornography.**

(1) A person who—

(a) produces child pornography for the purposes of its distribution through a computer;

(b) offers or makes available child pornography through a computer;

(c) distributes or transmits child pornography through a computer;

(d) procures child pornography through a computer for himself or herself or another person; or

(e) unlawfully possesses child pornography on a computer,

commits an offence.

(2) A person who makes available pornographic materials to a child commits an offence.

(3) For the purposes of this section "child pornography" includes pornographic material that depicts—

(a) a child engaged in sexually suggestive or explicit conduct;

(b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or

(c) realistic images representing children engaged in sexually suggestive or explicit conduct.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

**24. Cyber harassment.**

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

(2) For purposes of this section cyber harassment is the use of a computer for any of the following purposes—

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.

**25. Offensive communication.**

Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both.

**26. Cyber stalking.**

Any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

**27. Compensation.**

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

PART V—MISCELLANEOUS.

**28. Searches and seizure.**

(1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—

(a) that an offence under this Act has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises,

the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.

(2) An authorised officer may seize any computer system or take any samples or copies of applications or data—

(a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant.

(4) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (3).

(5) An authorised officer executing a search warrant referred to in subsection (3), may—

(a) at any time search for, have access to and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant;

(b) require a person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant; and

(c) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorties in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (5), an authorised officer shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.

(7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers under this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

(8) A computer system seized or samples or copies of applications or data taken by the authorised officer shall be returned within seventy two hours unless the authorised officer has applied for and obtained an order in an inter party application for extension of the time.

(9) In this section—

"authorised officer" means a police officer who has obtained an authorising warrant under subsection (1); and

"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hover craft.

**29. Admissibility and evidential weight of a data message or an electronic record.**

(1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message or an electronic record—

(a) merely on the ground that it is constituted by a data message or an electronic record;

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain; or

(c) merely on the ground that it is not in its original form.

(2) A person seeking to introduce a data message or an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3) Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

(4) When assessing the evidential weight of a data message or an electronic record, the court shall have regard to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the authenticity of the data message was maintained;

(c) the manner in which the originator of the data message or electronic record was identified; and

(d) any other relevant factor.

(5) The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds on which to doubt the authenticity of the electronic records system;

(b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(6) For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of any set standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

(7) For the avoidance of doubt, this section does not modify the common law or a statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

**30. Territorial jurisdiction.**

(1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

(3) For the purposes of this Act, this section applies if, for the offence in question—

(a) the accused was in Uganda at the material time; or

(b) the computer, program or data was in Uganda at the material time.

**31. Jurisdiction of courts.**

A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.

**32. Power of Minister to amend Schedule**

The Minister may by statutory instrument with the approval of the Cabinet, amend the Schedule to this Act.

SCHEDULE

*Section 2.*

Currency point

One currency point is equivalent to twenty thousand shillings.

**Cross reference**

Magistrates Courts Act, Cap.16.

# APPENDIX 4

## THE UGANDA COMMUNICATIONS ACT 2013

ACTS
SUPPLEMENT No. 1 18th January, 2013.

ACTS SUPPLEMENT

*to The Uganda Gazette No. 4 Volume CVI dated 18th January, 2013.*

Printed by UPPC, Entebbe, by Order of the Government.

**Act 1** *Uganda Communications Act* **2013**

# THE UGANDA COMMUNICATIONS ACT, 2013.

## ARRANGEMENT OF SECTIONS.

*Section*

*Section.*

*Section.*

*Section.*

# THE UGANDA COMMUNICATIONS ACT, 2013.

**An Act to consolidate and harmonise the Uganda Communications Act and the Electronic Media Act; to dissolve the Uganda Communications Commission and the Broadcasting Council and reconstitute them as one body known as the Uganda Communications Commission; and to provide for related matters.**

DATE OF ASSENT: 23rd December, 2012.

*Date of Commencement:* See section 1.

BE IT ENACTED By Parliament as follows:

## PART I—PRELIMINARY.

**1. Commencement.**

(1) Subject to subsection (2), this Act shall come into force upon the date of its publication in the Gazette.

(2) Part X of this Act shall come into force within one year from the date of publication in the Gazette, on the date appointed by the Minister by statutory instrument.

**2. Interpretation.**

In this Act, unless the context otherwise requires—

"authorised", in relation to an officer or employee of the Commission, means authorised by the Executive Director to exercise the powers or perform the duties in respect of which an authorised person is required;

"Board" means the Board established under section 9;

"broadcaster" means a licensed person who packages and distributes or distributes television or radio programmed services for reception by subscribers or the public, regardless of the technology;

"broadcasting" means the transmission of sound, video or data, intended for simultaneous reception by the public;

"cinematograph theatre" means any building, structure, tent or other erection of whatever nature or any place or land in or on which a cinematograph or video exhibition is presented to the public either gratuitously or for reward;

"Commission" means the Uganda Communications Commission established under section 4;

"communications" means telecommunications, data communication, radio communications, postal communications and includes broadcasting;

"communications services" means services performed consisting of the dissemination or interchange of audio, visual or data content using postal, radio, or telecommunications media, data communication, and includes broadcasting;

"content" means any sound, text, still picture, moving picture or other audiovisual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically;

"currency point" has the value assigned to it in Schedule 1;

"data" means electronic representations of information in any form;

"dominant position" means a position of market power enjoyed by an operator, which enables the operator to prevent effective competition being maintained in the relevant market by giving it the power to behave, to an appreciable extent, independently of its competitors and customers;

"Executive Director" means the Executive Director of the Commission appointed under section 16;

"eligible person" means a person who—

(a) has not been adjudged bankrupt or has not entered into a composition or a scheme of arrangement with his or her creditors; or

(b) has not been convicted of an offence whose penalty exceeds six months imprisonment or a fine exceeding twelve currency points or both;

"emission of electromagnetic energy" includes the deliberate radiation or reflection of electromagnetic energy by means of any apparatus designed or specially adapted for that purpose whether the reflection is continuous or intermittent;

"electronic media" means communication of any message to the public by means of any electronic apparatus;

"exhibition" means a display of art, video or data to the public, with or without sound by means of any electronic apparatus;

"franking machine" means a machine for the purposes of making impressions on postal articles to denote prepayment of postage and includes any metre or metres and any franking or date stamping dies or incidental dies;

"licence" means a licence issued under this Act;

"Minister" means the Minister responsible for information and communications technology;

"operator" means a person licensed to provide a communication or broadcasting service;

"person" includes any individual, company, association, or body of persons corporate or unincorporate;

"postal article" includes any letter, postcard, newspaper, book, document, pamphlet, pattern, sample packet, small packet, parcel package or other article tendered for dispatch or specified in the International Postal Union or in the licence of an operator;

"postal services" means the services performed and facilities provided in connection with—

(a) the collection, transmission and delivery by land, water or air of postal articles;

(b) the issue of postage stamps and the use of franking machines;

(c) the issue and payment of money from one place to another or address commonly referred to as money ordering;

"producer" includes a person who is at any given time, in charge of programme production and transmission to the public by means of any electronic apparatus;

"radio communication" means the transmitting or receiving over paths which are not provided by any material substance constructed or arranged for that purpose, of electromagnetic energy of a frequency not exceeding three million megahertz being energy which either—

(a) serves for the conveyance of messages, sound or visual images, whether messages are actually received by any person or not, or for the actuation or control of machinery or apparatus; or

(b) is used in connection with the determination of position, bearing or distance, or for the gaining of information as to the presence, absence, position or motion of any object or objects of any class;

"radio communications apparatus" or "radio communications station" means any apparatus or station, as the case may be, for transmitting or receiving of radio communication other than a domestic radio set and where—

(a) that radio communications apparatus or station cannot lawfully be used without a radio communications licence or without an exemption under section 23;

(b) radio communication in the form of messages, audio or visual images is received or transmitted by that apparatus or station;

(c) an apparatus is electrically coupled with another apparatus or station for the purpose of enabling any person to receive or transmit messages, sound or visual images;

"radio communications services" means services performed and the facilities provided in connection with communication by means of radio communications apparatus;

"telecommunication" means the emission, transmission or reception through the agency of electricity or electromagnetism of any sounds, signals, signs, writing, images or intelligence of any nature by wire, radio, optical or other electromagnetic systems whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception;

"telecommunications apparatus" or "telecommunication station" means any apparatus or equipment used or intended to be used in connection with the transmission of communications by means of electricity from one place to another place either along a wire joining those two places or partly by wire from each of those two places and partly by radio communication;

"telecommunications line" means any wire, cable, equipment, tower, mast, antenna, tunnel, hole, pit trench, pole or other structure or thing used or intended to be used in connection with a telecommunications system;

"telecommunications service" means a service consisting of the conveyance or reception of any sounds, signs, signals, writing or images by wire, optical or other electronically guided media systems whether or not the signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other process by any means in the course of their transmission, emission or reception;

"telecommunications system" means a system for the conveyance through the agency of electric, magnetic, electromagnetic, electrochemical, electromechanical or light energy of—

(a) speech, music, data and other sounds;

(b) visual images;

(c) signals serving for the importance, whether as between persons and things, of any matter otherwise than in the form of sounds, visual images; or

(d) signals serving for the actuation or control of machinery or apparatus; and

including telecommunications apparatus situated in the Republic of Uganda;

"tribunal" means the Uganda Communications Tribunal established under section 60;

"wire" includes optical cable.

**3. Objectives of the Act.**

The objectives of this Act are to develop a modern communications sector, which includes telecommunications, broadcasting, radio communications, postal communications, data communication and infrastructure by—

(a) establishing one regulatory body for communications in accordance with international best practice;

(b) enhancing national coverage of communications services

(c) expanding the existing variety of communications services available in Uganda to include modern and innovative communications services;

(d) reducing the direct role of Government as an operator in the communications sector and minimising the subsidies paid by the Government to the communications sector;

(e) encouraging the participation of the private sector in the development of the communications sector;

(f) introducing, encouraging and enabling competition in the communications sector through regulation and licensing of competitive operators to achieve rapid network expansion, standardisation as well as operation of competitively priced and quality services; and

(g) establishing and administering a fund for the development of rural communications and information and communication technology in the country.

PART II—UGANDA COMMUNICATIONS COMMISSION

**4. Establishment of Uganda Communications Commission**

(1) There is established the Uganda Communications Commission.

(2) The Commission is a body corporate with perpetual succession and a common seal and may for the purposes of discharging its functions under this Act—

(a) acquire, hold or dispose of movable and immovable property;

(b) sue and be sued in its corporate name;

(c) do all acts and things that a body corporate may lawfully do.

(3) The seal of the Commission shall be authenticated in accordance with Schedule 2.

**5. Functions of the Commission**

(1) The functions of the Commission are—

(a) to implement the objectives of this Act;

(b) to monitor, inspect, licence, supervise, control and regulate communications services;

(c) to allocate, license, standardize and manage the use of the radio frequency spectrum resources in a manner that ensures widest variety of programming and optimal utilization of spectrum resources;

(d) to process applications for the allocation of satellite orbital locations;

(e) to regulate rates and charges for communications services with a view to protecting consumers from excessive tariffs and to prevent unfair competitive practices.

(f) to establish, amend, administer and enforce a national numbering plan and electronic addresses plan; and assign numbers and electronic addresses;

(g) to conduct, or authorise any person to conduct, technical evaluations relating to communications services;

(h) to coordinate and collaborate with the relevant national and international organisations in matters relating to communications;

(i) to set national standards and ensure compliance with national and international standards and obligations laid down by international communication agreements and treaties to which Uganda is a party;

(j) to receive, investigate and arbitrate complaints relating to communications services, and take necessary action;

(k) to promote and safeguard the interests of consumers and operators as regards the quality of communications services and equipment;

(l) to promote research into the development and use of new communications techniques and technologies, including those which promote accessibility of persons with disability and other members of society to communications services;

(m) to improve communications services generally and to ensure equitable distribution of services throughout the country;

(n) to promote competition, including the protection of operators from acts and practices of other operators that are damaging to competition, and to facilitate the entry into markets of new and modern systems and services;

(o) to regulate interconnection and access systems between operators and users of telecommunications services;

(p) to advise the Government on communications policies and legislative measures in respect of providing and operating communications services;

(q) to represent Uganda's communications sector at national and international fora and organizations relating to its functions and to coordinate the participation of any interested groups;

(r) to collaborate with educational institutions in order to promote specialised education in the field of communications;

(s) to establish and administer a fund for the development of rural communications and information and communication technology in the country;

(t) to advise the Minister on the administration of this Act;

(u) establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators;

(v) to regulate value added services provided by communications operators;

(w) to operate and manage the Uganda Institute of Information and Communications Technology;

(x) to set standards, monitor and enforce compliance relating to content; and

(y) to encourage and promote infrastructure sharing amongst licensees and to provide regulatory guidelines

(z) to carry out any other function that is related to the functions of the Commission.

(2) The Commission shall submit to the Minister quarterly reports on the performance of its functions.

(3) The Minister may at any time request the Commission for a report of its performance.

(4) The Commission shall submit an annual performance report to the Minister within three months prior to the end of each year.

(5) The Minister shall lay the annual report of the Commission before Parliament.

**6. Powers of the Commission.**

(1) The Commission may in the exercise of its functions—

(a) charge fees for services provided by the Commission;

(b) institute a levy on the gross annual revenue from operators in accordance with section 68;

(c) collect the revenue determined by the Minister in respect of the internationl incoming telecommunications traffic;

(d) impose a fine on a person who unlawfully possesses, installs, connects or operates any communications equipment or apparatus, or unlawfully provides or performs any communications services;

(e) classify communications services and licenses.

(2) The Commission may in accordance with this Act, confiscate any apparatus which is possessed, installed, connected or operated unlawfully.

(3) The owner of an apparatus confiscated by the Commission may appeal to the tribunal against the confiscation.

**7. Powers of the Minister.**

(1) The Minister may, in writing, give policy guidelines to the Commission regarding the performance of its functions.

(2) The Commission shall comply with the policy guidelines given by the Minister under this section.

**8. Independence of the Commission.**

Subject to this Act, the Commission shall exercise its functions independently of any person or body.

**9. Board of the Commission.**

(1) The Commission shall be governed by a Board.

(2) The Board shall consist of the following—

(a) a person with experience and knowledge in tele-communications, broadcasting or postal communications, who shall be the chairperson;

(b) a representative of professional engineers recommended by the Institute of Professional Engineers;

(c) one prominent lawyer who is a member of the Uganda Law Society;

(d) a person knowledgeable in the field of economics, financial management and public administration;

(e) a representative of the Ministry responsible for information and communications technology, who shall be an ex-officio member;

(f) the Executive Director;

(g) a representative of consumers recommended by the Uganda Consumers Association; and

(h) one eminent person of good repute and proven integrity representing the public.

(3) All members of the Board shall be appointed by the Minister with approval of Cabinet, one of whom shall be a person with disability and at least three of whom shall be women.

(4) A member of the Board shall hold office on the terms and conditions specified in the instrument of appointment.

(5) A member of the board shall hold office for three years and shall be eligible for reappointment for only one further term.

**10. Disqualification from appointment.**
A person shall not be appointed to the Board who—

(a) is engaged in an organization which operates or provides communications services, directly or indirectly, as owner, shareholder, partner or otherwise;

(b) is engaged in the manufacture or distribution of communications equipment in Uganda, directly or indirectly, as owner, shareholder, partner or otherwise;

(c) has a financial or proprietary interest in an organization referred to in paragraph(a) or (b);

(d) is insolvent;

(e) is incapacitated by mental or physical illness that renders the person incapable of performing the functions of a member of the Board;

(f) is otherwise unable or unfit to discharge the functions of a member of the Board.

**11. Vacating office of member of the Board.**

(1) A member of the Board shall vacate office, if the member—

(a) is declared insolvent;

(b) is convicted of a criminal offence in respect of which a penalty of imprisonment of six months or more is imposed without the option of a fine;

(c) is continuously and persistently unable to discharge the functions of the office of a member of the Board;

(d) subsequently becomes disqualified from being a member under section 10.

(e) fails to disclose to the Commission any interest that member has in a contract or proposed contract connected with the Commission or any other matter;

(f) misbehaves or abuses the office of a member of the Board.

(2) The Minister shall determine that a member vacates office under subsection (1).

(3) A member of the Board may resign from office in writing to the Minister.

(4) Where a member resigns, dies or is removed from office under this section, the Minister shall within three months and in accordance with section 9, appoint another person to replace the member, and to hold office for the remainder of the term of that member.

**12. Meetings of the Board.**

(1) The Board shall meet at least once every three months for the purposes of discharging its functions.

(2) The meetings of the Board shall be conducted in accordance with Schedule 3.

**13. Remuneration of members of the Board.**

The members of the Board may be paid remuneration or allowances approved by the Minister in consultation with the Ministers responsible for public service and finance.

**14. Committees of the Board.**

(1) The Board may appoint committees—

(a) to inquire into and advise the Board on any matter concerning the functions of the Commission;

(b) to exercise the powers or perform a function of the Commission.

(2) The Board shall establish a contents committee to oversee content matters under the Act.

(3) A committee appointed under subsection (1) shall consist of a chairperson and other members of the Board, as the Board may determine.

(4) A committee may invite any person to attend any of its meetings and may co-opt any person to the committee but that person shall not vote on any matter before the committee.

(5) Members of a committee appointed under this section may be paid allowances as the Board may, with the written approval of the Minister, determine.

(6) Subject to any direction given by the Board, a committee appointed under this section may regulate its own procedure.

PART III—SECRETARIAT AND STAFF OF THE COMMISSION

**15. Secretariat of the Commission.**

(1) The Commission shall have a secretariat which shall be responsible for the day-to-day operations of the Commission and implementing the decisions of the Board.

(2) The secretariat shall be headed by a full time Executive Director.

**16. Executive Director.**

(1) The Executive Director shall be appointed by the Minister on the recommendation of the Board.

(2) A person shall not be appointed executive director unless that person has relevant knowledge, qualification and considerable experience in either communications, economics, finance, law or administration.

(3) The Executive Director shall hold office for five years, and shall be eligible for reappointment for only one further term.

(4) A person shall cease to hold the office of Executive Director if that person—

(a) resigns;

(b) is declared insolvent;

(c) is convicted of a criminal offence in respect of which a penalty of imprisonment of six months or more is imposed without the option of a fine;

(d) is removed from office by the Minister on the recommendation of the Board for—

(i) continuously and persistently being unable to discharge the functions of the office Executive Director;

(ii) failing to disclose to the Commission any interest in a contract or proposed contract or any other matter connected to the Commission; or

(iii) misbehavior or abuse of office.

**17. Duties of the Executive Director.**

(1) Subject to this Act and to the general supervision of the Board, the Executive Director is the chief executive officer of the Commission and is responsible for—

(a) implementing the policies and programmes agreed upon by the Commission;

(b) managing the funds and property of the Commission;

(c) administering, organizing and supervising the staff of the Commission;

(d) keeping the Board informed of the activities of the Commission;

(e) keeping record of all the transactions of the Commission.

(2) In the performance of his or her duties, the Executive Director is answerable to the Board.

**18. Secretary to the Commission.**

(1) There shall be a secretary to the Commission who shall be appointed by the Board on the terms and conditions specified in the instrument of appointment.

(2) The secretary shall be responsible for taking all the minutes of the meetings of the Board.

(3) The secretary shall perform all other duties and functions that the Board or the Executive Director may assign to the secretary.

(4) The secretary shall, in the discharge of his or her duties, be answerable to the Executive Director.

**19. Other officers and staff of the Commission.**

(1) There shall be officers and staff of the Commission as may be necessary for the effective performance of the functions of the Commission.

(2) The officers and staff of the Commission shall be appointed by the Board on such terms and conditions as the Board shall determine.

**20. Protection of members of the Board and officers of the Commission.**

A member of the Board or an officer of the Commission or a person acting on the directions of the Board or of an officer of the Commission is not personally liable for any act or omission done or omitted to be done in good faith in the exercise of functions under this Act.

PART IV—LICENSING OF COMMUNICATIONS

*Radio, telecommunications and other communications licences*

**21. Licence for radio communications**

A person shall not, without a licence issued by the Commission—

(a) establish or use any radio station or provide radio communication services;

(b) sell, let, hire or otherwise dispose of any radio communications apparatus;

(c) manufacture, possess, install, connect or operate any radio communications apparatus or interference-causing apparatus.

**22. Licence for telecommunications.**
A person shall not, establish a telecommunications station, provide telecommunications services or construct, maintain or operate telecommunications apparatus without a licence issued by the Commission.

**23. Exemption from requirement for licence.**
Notwithstanding sections 21 and 22, a licence is not required for communications apparatus—

(a) exempted by regulations made under this Act;

(b) for use by the police, the armed forces or any other services directly used by the State in the performance of official functions, which comply with technical requirements specified by the Commission.

*Management and use of frequency spectrum*

**24. Licence to use frequency spectrum.**
The Commission shall exclusively issue licences for—

(a) radio broadcasting or communications apparatus and spectrum use;

(b) possession and operation of radio broadcasting or communications apparatus;

(c) broadcasting and communications as the Commission may consider appropriate.

**25. Management of radio spectrum.**

(1) Notwithstanding any other law, the Commission is exclusively responsible for—

(a) planning, monitoring, managing and allocating the use of the radio spectrum;

(b) establishing technical requirements and standards in respect of—

(i) radio communications apparatus;

(ii) interference-causing apparatus or any class of that apparatus;

(c) negotiating with the International Telecommunications Union or its affiliated bodies on matters relating to radio spectrum.

(2) For the purposes of section 5(1)(c), the Commission may, through spectrum refarming, withdraw spectrum where the Commission is satisfied that the spectrum is not utilized optimally or efficiently.

*Installation of television and radio stations.*

**26. Installation of television and radio stations.**

(1) A person shall not install or operate a television station, radio station or any related broadcasting apparatus without a licence issued by the Commission.

(2) The Commission shall, before issuing a licence under this section, take into account—

(a) proof of existence of adequate technical facilities;

(b) the location of the station and geographical area to which broadcast is to be made;

(c) social, cultural and economic values; and

(d) the environmental impact assessment.

(3) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one thousand five hundred currency points or imprisonment not exceeding five years or both.

(4) For the purposes of sub section (3), in the case of a corporate body, any or all the persons who are authorized to sign any document on behalf of the corporate body may be held liable for the contravention.

*Broadcasting licence, right to broadcast and broadcasting standards*

**27. Broadcasting licence.**

(1) A person shall not broadcast without a broadcasting license issued by the Commission.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding twenty five currency points or imprisonment not exceeding one year or both.

**28. Right to broadcast.**

(1) A person shall not, take any action which is not authorized under this Act or other law, on account of the content of a programme, to prevent the broadcasting of a programme.

(2) Subsection (1) does not absolve a person from complying with any law which prohibits—

(a) the broadcasting of pornographic material and obscene publications; or

(b) any broadcasting which infringes upon the privacy of any

individual.

**29. Duties of a licensee and producer.**

The holder of a licence or a producer of a broadcasting station or disseminating apparatus shall—

(a) ensure that what is broadcast is not contrary to public morality;

(b) retain a record of all that is broadcast, for not less than sixty days.

**30. Disqualification of a producer.**

A person shall not be appointed a producer of a broadcasting station if that person—

(a) is less than eighteen years of age;

(b) is of unsound mind;

(c) is not ordinarily resident in Uganda;

(d) does not possess the requisite qualifications prescribed by the Media Council.

**31. Minimum broadcasting standards.**

A person shall not broadcast any programme unless the broadcast or programme complies with Schedule 4.

**32. Ethical broadcasting standards**

(1) Subject to this Act, the ethical broadcasting standards which apply to broadcasters are the professional code of ethics specified in the First Schedule to the Press and Journalist Act.

(2) The standards referred to in subsection (1) may be modified by the Commission to accord with this Act.

PART V—POSTAL SERVICES

**33. Licensing of postal services.**

(1) A person shall not convey, deliver or distribute postal articles

without a licence issued under this Act.

(2) A person shall not require a licence to convey, deliver or distribute the following postal articles—

(a) articles for delivery to another person or persons to whom they are directed, without hire, reward or other profit or advantage for receiving, carrying or delivering them;

(b) articles solely concerning goods or other property sent by land, water or air, and delivered with the goods or property to which the letters relate without hire, reward, profit or advantage for receiving them, and the articles are open to inspection and have subscribed on them the words "consignee's articles" or other words to that effect.

**34. Subcontracting by a licensee.**

(1) In the case of postal services, a licensee may use a subcontractor to perform the services subject to the licensee's responsibility to comply with all obligations and conditions under the licence and this Act.

(2) The liability of a subcontractor of a licensee under subsection (1) in the collection, transmission or delivery of any postal article or for loss or delay of or damage to the article or any other loss or damage in relation to the performance of postal services shall be the same as the liability of the licensee.

(3) Subsection (2) does not affect the liability of the subcontractor to the licensee.

**35. Protection of postal articles.**

(1) A person engaged in postal services shall protect any postal article and ensure that an employee of that person does not—

(a) open the article;

(b) know or disclose the contents of a postal article;

(c) deliver an article in the course of transmission to a person other than the addressee, without the consent of the addressee;

(d) permit that article to be opened or delivered to a person other than the addressee, without the consent of the addressee, or permit anyone other than the addressee to know or to disclose the contents of a postal article.

(2) Any person who negligently or knowingly fails to comply with subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment for a period not exceeding five years or both on the first conviction; and a fine not exceeding two hundred and forty currency points or imprisonment for a period not exceeding ten years or both on a subsequent conviction.

(3) Subsection (1) does not apply to an article opened or disposed of under—

(a) the law regulating customs;

(b) any other law prohibiting or regulating the importation or exportation of an article;

(c) any regulation permitting the opening of a postal article for the purposes of ascertaining details pertaining to the sender or addressee which are necessary in order to return or deliver the postal article.

**36. Limitation of liability of a licensee.**

(1) The liability of a holder of a licence for—

(a) the loss, misdelivery or delay of or damage to, any postal

article in the course of transmission by the licensee;

(b) the interception, detention or disposal of any postal article in accordance with this Act; or

(c) the wrong payment of a money order,

shall not exceed that provided for by regulations made by the Commission, the contract governing the service contracted or the Universal Postal Union.

(2) The holder of a licence shall give notice to the public regarding the type of liability under subsection (1) which applies to the licensee.

PART VI—VIDEO AND CINEMA OPERATORS

**37. Licence for cinematograph theatre or video library.**

(1) A person shall not operate a cinematograph theatre or a video or film library without a licence issued by the Commission.

(2) The Commission shall issue the licence on terms and conditions the Commission may consider necessary.

(3) The Commission shall, before issuing a licence under this section consider whether, at the place or premises of the applicant, there is adequate provision for the safety, health or convenience of the persons attending a video or cinematograph exhibition.

(4) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding twelve months or both.

PART VII—GENERAL PROVISIONS RELATING TO LICENCES.

**38. Application for a licence.**

(1) An application for a licence under this Act shall be made to the Commission in the prescribed form.

(2) Before granting a licence, the Commission shall, take into account the following—

(a) whether the applicant is an eligible person;

(b) the capability of the applicant to operate a system or service for which a licence is sought;

(c) the objectives of this Act;

(d) whether the grant of the licence is in the public interest.

(3) A licence under this section shall—

(a) be issued upon payment of the fees prescribed for the licence;

(b) state the terms and conditions upon which it is granted;

(c) specify the services to be provided by the operator;

(d) where applicable, specify the network to be operated.

(4) The Commission shall grant the licence within sixty days from the date of application.

(5) Where the Commission refuses to grant the licence, it shall within fourteen days provide a written explanation to the applicant, giving reasons for the refusal.

**39. Terms and conditions of a licence.**

(1) The Commission shall prescribe the terms and conditions of all operators licensed under this Act.

(2) A licence may include the provision of services to rural or sparsely populated areas or other specified areas and other conditions specified in Schedule 6.

(3) An operator shall provide the service for which that operator has obtained a licence.

(4) For the purposes of this section, the conditions may include—

(a) in the case of a licence to establish a radio communication station, the specifications as to the positions and nature of the station, the purpose for and circumstances in which and the persons by whom the station may be installed or used;

(b) in the case of any other telecommunication licence, specifications as to the apparatus which may be installed or used, the places where, the purposes for, the circumstances in which and the persons by whom an apparatus may be used; and

(c) in the case of a postal services licence, specifications as to the services to be performed, the place of postal services and the geographical spread of the services and places.

**40. Modification of licence.**

(1) The Commission may, upon reasonable grounds, modify the conditions of any licence if the Commission considers it necessary to achieve the objectives of this Act, or is in the public interest, taking into account the justified interests of operators and the principles of fair competition and equality of treatment.

(2) Before modifying any condition of a licence, the Commission shall give the operator notice of not less than sixty days, stating the reasons for the intended modification and giving the operator an opportunity to make any representation.

(3) The Commission shall give an operator reasonable time within which to comply with the modification of the licence.

(4) A person aggrieved by a decision of the Commission may appeal to the tribunal.

**41. Suspension and revocation of licence.**

(1) The Commission may suspend or revoke a licence issued under this Act, on the following grounds—

(a) serious and repeated breach of the licence conditions;

(b) any fraud or intentional misrepresentation by the operator applying for the licence;

(c) where the operator is engaged in or is supporting activities amounting to a treasonable offence under the Penal Code Act; or

(d) where the operator has ceased to be an eligible person.

(2) After consideration of any representations by the operator, the Commission may—

(a) prescribe time during which the operator is required to remedy the offending act or conduct;

(b) require the operator to pay a fine not exceeding the equivalent of ten percent of its gross annual revenue.

(3) The Commission shall give the operator written notice of not less than sixty days specifying the reasons for the intended suspension or revocation, during which the operator may make representations to the Commission.

(4) Where the Commission is of the opinion that the measures under subsection (3) are not sufficient, the Commission may—

(a) suspend the licence for a specified period; or

(b) revoke the licence.

**42. Transfer of licence.**

(1) A licence issued by the Commission shall not be transferred without the written consent of the Commission.

(2) An operator may apply to the Commission in the prescribed manner for consent to transfer a licence.

(3) An application under subsection (2) shall be accompanied by an application for grant of a licence by the person to whom the operator intends to transfer the licence.

(4) The Commission shall in considering an application for the transfer of a licence have regard to the same terms and conditions as those that apply to the grant of a new licence, but the Commission may in its discretion refuse to grant the application under this section.

(5) For the purposes of this section—

(a) "transfer of licence" includes the acquisition of control of the licence holder;

(b) "control" as used with respect to any person shall mean the possession, directly or indirectly, of the power to direct or cause the direction of the management of that person, whether through the ownership of shares, voting, securities, partnership or other ownership interests, agreement or otherwise.

(6) The Commission shall grant its consent to transfer a licence within forty five days from the date of application.

(7) Where consent is not granted under this section, the Commission shall within fourteen days provide a written explanation, giving reasons for the refusal.

**43. Lapse and renewal of a licence.**

(1) An application for the renewal of a licence shall be made at least two months before the expiration of the licence.

(2) In considering an application for a renewal of a licence, the

Commission shall have regard to the performance of the operator during the duration of the licence.

(3) The Commission shall renew a licence within thirty days from the date of application.

(4) Where a licence is not renewed under this section, the Commission shall within fourteen days, provide a written explanation, giving reasons for the refusal.

**44. Annual report on operations of licensee.**

Every licensee shall, at the end of each year of business, prepare and submit to the Commission in the prescribed form, a report on the operations and services of the licensee and the extent to which the conditions of the licence are followed.

PART VIII—INVESTIGATION AND INSPECTIONS.

**45. Investigation of complaints.**

The Commission may investigate any matter within its functions under this Act which relates to—

(a) communications services or apparatus provided or supplied in Uganda; and

(b) any representation made to the Commission by or on behalf of a person whom the Commission considers to have an interest in the matter which is the subject of the representation.

**46. Power to institute inquiries.**

(1) The Commission may appoint any person or committee to inquire into and report to the Commission on any matter pending before the Commission.

(2) The Commission shall institute an inquiry where the Commission is directed to do so by the Minister.

(3) The Commission may give to a person or committee

appointed under this section, directions regarding the procedures for conducting the inquiry.

**47. Report on investigations.**

(1) A person or committee appointed to carry out inquiries under section 46 shall submit a report to the Commission in a form and manner that the Commission may direct.

(2) Where an inquiry is instituted in accordance with the direction of the Minister, the Commission shall submit a copy of the report to the Minister.

**48. Directions to remedy breach.**

Where as a result of an investigation the Commission is satisfied that an operator has breached a condition of a licence or an obligation under this Act, it may direct the operator in writing to remedy the breach or to do such act or acts as the Commission may specify in the direction, in accordance with the procedures specified in section 41.

**49. Appointment of inspectors.**

(1) The Commission may appoint inspectors for the purposes of verifying compliance with this Act and the decisions of the Commission.

(2) An inspector shall, when exercising powers under this Act, produce the instrument of appointment and identification when required to do so by any person.

**50. Powers of an inspector.**

(1) Subject to subsection (3), an inspector may—

(a) enter and inspect at any reasonable time any place owned by or under the control of an operator in which the inspector believes on reasonable grounds to be any document, information or apparatus relevant to the enforcement of this Act and examine the document,

information or apparatus or remove it for examination or reproduction;

(b) enter any place in which the inspector believes that there is radio apparatus or interference-causing apparatus, and examine any radio apparatus, logs, books, reports, data, records, documents or other information, and remove the information, document, apparatus or equipment for examination or reproduction;

(c) make reasonable use of any copying equipment or means of communication located at the place.

(2) The inspector shall sign for any information, document, article, apparatus or equipment removed by the inspector under this section and shall leave a copy of the signed record with the operator.

(3) Where a place referred to under subsection (1) is a dwelling house, an inspector shall not enter that dwelling house without the consent of the occupant, unless—

(a) under the commission of a warrant issued under section 51; or

(b) where by reason of exigent circumstances, it would not be practical for the inspector to obtain a warrant.

(4) For the purposes of subsection (3)(b), "exigent circumstances" include circumstances in which the delay arising from obtaining a warrant would result in danger to human life or safety, loss or destruction of evidence.

(5) The owner or person in charge of a place entered by an inspector shall give the inspector all reasonable assistance to enable the inspector to carry out the inspector's duties under this Act.

**51. Search warrant.**

(1) Where on application, a magistrate is satisfied by information on oath that—

(a) entry to a dwelling house is necessary for the purpose of performing any duty of an inspector under this Act; and

(b) entry to a dwelling house has been refused or is likely to be refused,

the magistrate may issue a warrant authorising the inspector named in the warrant to enter that dwelling house, subject to conditions specified in the warrant.

(2) In executing a warrant issued under this section, an inspector shall not use force unless accompanied by a police officer, and unless the use of force is specifically authorised in the warrant.

(3) For the purposes of this section, "magistrate" means a Magistrate not below a Magistrate Grade I.

PART IX—FAIR COMPETITION AND EQUALITY OF TREATMENT.

**52. Commission to promote fair competition.**

The Commission shall, in the performance of its functions under this Act, promote, develop and enforce fair competition and equality of treatment among all operators in any business or service relating to communication.

**53. Unfair competition prohibited.**

(1) An operator shall not engage in any activities, which have, or are intended or are likely to have, the effect of unfairly preventing, restricting or distorting competition in relation to any business activity relating to communications services.

(2) For the purposes of subsection (1) the acts or omissions include—

(a) any abuse by an operator, independently or with others, of

a dominant position which unfairly excludes or limits competition between the operator and any other party;

(b) entering into an agreement or engaging in any concerted practice with any other party, which unfairly prevents, restricts or distorts competition; or

(c) effecting anticompetitive changes in the market structure and, in particular, anticompetitive mergers and acquisitions in the communications sector.

**54. Exceptions to fair competition.**

The Commission may, in writing, allow an operator to carry on any act or omission prohibited under section 53 where the Commission is satisfied that, the act or omission—

(a) contributes to—

(i) the improvement of any goods or services;

(ii) the promotion of communications services in Uganda in accordance with this Act; and

(b) does not—

(i) impose on the parties restrictions which are not indispensable to attaining the objective specified under paragraph (a); and

(ii) give the parties the ability to substantially reduce competition in respect of the goods or services in question.

**55. Breach of fair competition.**

(1) The Commission may, by its own motion, investigate any operator who commits any act or omission in breach of fair competition.

(2) A person may complain to the Commission against a breach of fair competition by an operator.

(3) The Commission shall, if it appears that a breach of competition has been committed, investigate the act or omission and give written notice to the operator stating—

(a) that the Commission is investigating a possible breach of fair competition;

(b) the reasons for the suspicion of a contravention or breach, including any matter of facts or law which are relevant to the investigation;

(c) further information required from the operator in order to complete the investigation; and

(d) where appropriate, the steps to be taken in order to remedy the breach.

(4) The operator may, within thirty days from the date of the notice, make representations in response to the notice.

(5) Any person affected by the contravention or breach of fair competition may make a representation to the Commission in relation to the contravention or breach.

(6) The Commission shall, after considering any representations of the operator or any other person, fix a date on which to make a decision on the matter.

(7) The Commission may, upon satisfaction that an operator is competing unfairly—

(a) order the operator to stop the unfair competition;

(b) require the operator to pay a fine not exceeding ten percent of the annual turnover of the operator;

(c) declare any anticompetitive agreements or contracts null and void.

(8) Subsection (6) shall not affect in any way the right of a person to take any other action against the operator under this Act or any other law.

(9) Any person aggrieved by the decision of the Commission under this section may appeal to the tribunal.

(10) This section shall not limit or in any way affect the obligations of an operator under any condition of a licence.

**56. Denial of access or service.**

An operator shall not deny access or service to a customer except for nonpayment of dues or for any other just cause.

**57. Equality of treatment.**

An operator shall provide equal opportunity for access to the same type and quality of service to all customers in a given area at substantially the same rates, limiting variations to available or appropriate technologies required to serve specific subscribers.

**58. Interconnection of network facilities.**

(1) A telecommunications operator may, with the approval of the Commission, enter into an agreement with any other operator for the purpose of connecting its network facilities with the network facilities of that other operator on terms and conditions that the operators may agree.

(2) The operators referred to in subsection (1) shall submit to the Commission an application for approval of an interconnection agreement accompanied by a copy of the proposed interconnection agreement.

(3) Upon receipt of the application and proposed interconnection

agreement, the Commission shall within thirty days respond to the application in writing.

(4) Where the Commission does not respond to the application in the time specified in subsection (3), the Commission shall be taken to have approved the application.

(5) The Commission—

(a) shall, within ninety days from the receipt of an application of an operator or within such other reasonable period in the circumstances; or

(b) may, on its own motion,

impose an interconnection agreement on two operators if a negotiated agreement is not possible or if the Commission determines that such agreement promotes fair competition.

(6) Before imposing an interconnection agreement between two or more operators, the Commission shall give each operator thirty days' notice stating the reasons for the intended imposition, and giving the operators opportunity to make representations.

(7) The Commission shall issue minimum guidelines in accordance with which telecommunications operators shall negotiate interconnection agreements.

**59. Maximum interconnection rates.**

(1) Notwithstanding section 58, the Commission may fix maximum interconnection rates.

(2) For the purposes of determining the rate under subsection (1), the Commission shall take into account—

(a) accessibility and affordability of the communications

services to all parts of the society;

(b) fair treatment and competition among the operators

PART X—UGANDA COMMUNCATIONS TRIBUNAL.

**60. Establishment of Uganda Communications Tribunal.**

(1) There is established a tribunal known as the Uganda Communications Tribunal.

(2) The tribunal shall consist of a judge and two other persons appointed by the President on the recommendation of the Judicial Service Commission.

(3) The judge shall be the chairperson of the tribunal.

(4) The chairperson or a member of the tribunal shall hold office for four years, and shall be eligible for reappointment.

(5) The tribunal may, in the discharge of its functions, be assisted by not more than four technical advisers appointed by the tribunal from technical persons identified by the Minister.

(6) A technical adviser shall be appointed for a specific assignment after which the appointment shall lapse.

**61. Funds of the tribunal.**

The funds of the tribunal shall consist of—

(a) money appropriated by Parliament from time to time for enabling the tribunal to perform its functions;

(b) grants, gifts or donations from the Government or other sources acceptable to the Minister and the Minister responsible for finance; or

(c) funds provided to the tribunal by the Commission under section 71.

**62. Disqualification from appointment to the tribunal.**

A person shall not be appointed to the tribunal or as a technical adviser who—

(a) is engaged in a communications company or organisation which operates communications systems or provides services or is engaged in the manufacture or distribution of communications equipment in Uganda, as an owner, shareholder, partner or otherwise, whether directly or indirectly;

(b) has a financial or proprietary interest in an organisation referred to in paragraph (a) or in the manufacture or distribution of communications apparatus anywhere in Uganda;

(c) is an undischarged bankrupt or has made any arrangement with creditors;

(d) is incapacitated by mental or physical illness; or

(e) is otherwise unable or unfit to discharge the functions of office of a member of the tribunal or technical adviser.

**63. Vacating office of member of the tribunal.**

(1) The office of a member of the tribunal shall fall vacant if—

(a) the member is continuously and persistently unable to perform the functions of the office;

(b) the member engages in misbehaviour or abuse of office;

(c) the member is subsequently disqualified from membership in accordance with section 62;

(d) the member fails to disclose to the tribunal any interest in a contract or proposed contract or any other matter before the tribunal.

(2) A vacancy under subsection (1)(a) shall be determined by the President on the recommendation of the Minister.

(3) A member of the tribunal may resign office by notification in writing to the President.

(4) A technical adviser shall cease to be a technical adviser if he or she—

(a) is subsequently disqualified from appointment in accordance with this section;

(b) fails to disclose to the tribunal any interest in the communications sector or in a contract or other matter before the Commission or the tribunal;

(c) subsequently acquires any material interest in the communications sector.

(5) A vacancy under sub-section (4) shall be determined by the Minister on the recommendation of the Commission.

(6) A technical advisor may resign office by notification in writing to the Minister.

**64. Jurisdiction of the tribunal.**

(1) The tribunal shall have jurisdiction to hear and determine all matters relating to communications services arising from decisions made by the Commission or the Minister under this Act.

(2) For the avoidance of doubt, the jurisdiction of the tribunal does not include the trial of any criminal offence.

**65. Powers of the tribunal.**

(1) The tribunal shall in the exercise of its jurisdiction under this Act have all powers of the High Court.

(2) For the purposes of this section the law applicable to a civil action in the High Court shall, with the necessary modifications, apply to proceedings before the tribunal.

(3) Judgments and orders of the tribunal shall be executed and enforced in the same manner as judgments and orders of the High Court.

(4) Any person aggrieved by a decision of the tribunal may within thirty days from the date of the decision or order appeal to the Court of Appeal.

(5) The law applicable to appeals from the High Court in civil matters shall, with the necessary modifications or the written adjustments as the Chief Justice may direct, apply to appeals from the Commission to the tribunal and from the tribunal to the Court of Appeal.

PART XI—UGANDA POST LIMITED

**66. Uganda Post Limited.**

(1) Uganda Post Limited shall provide reserved postal services, exclusively and the postal services that the company is required to provide, as mandatory postal services, at uniform prices and conditions.

(2) The Uganda Post Limited shall, exclusively, be responsible for producing and issuing postage stamps, prestamped envelopes, aerograms and international reply coupons bearing the official national coat of arms or the words "Republic of Uganda", "Uganda" or "Uganda Post".

(3) The Uganda Post Limited may, subject to such conditions as it may determine and without prejudice to the provisions of this Act or any regulations made under this Act, license the use by any person of franking machines.

PART XII—FINANCIAL PROVISIONS

**67. Funds of the Commission.**

(1) The funds of the Commission shall consist of—

(a) money appropriated by Parliament for the purposes of the Commission;

(b) licence fees and money paid to the Commission for services rendered;

(c) money collected from the levy on the gross annual revenue of operators charged in accordance with section 68;

(d) revenue collected from license in respects of internationl incoming telecommunications traffic;

(e) money borrowed by the Commission;

(f) loans, grants, gifts or donations from Government and other sources made with the approval of the Minister, the Minister responsible for finance and Parliament.

(2) The Minister shall by statutory instrument determine the percentage of revenue received by operators from internationl incoming telecommunications traffic to be collected by the Commission.

**68. Levy on gross annual revenue of operators**

(1) The Commission may levy a charge on the gross annual revenue of operators licenced under this Act.

(2) The levy in subsection (1) shall be the percentage specified in schedule 5.

(3) For avoidance of doubt, the levy in subsection (2) shall not be less than two percent.

(4) The levy shall be shared between information and communication technology development and rural communication in the ratio of one to one.

**69. Power to open and operate bank accounts**

(1) The Commission shall open and maintain bank accounts as are necessary for the performance of the functions of the Commission.

(2) The bank accounts shall be operated in a manner determined by the Board.

**70. Estimates of income and expenditure**

(1) The Board shall, not less than two months before the beginning of each financial year, prepare and submit to the Minister for approval, a budget containing the estimates of income and expenditure of the Commission for the next financial year.

(2) The Commission shall not incur any expenditure exceeding the budget without the approval of the Minister.

**71. Application of Commission funds**

Subject to section 70 (2), the funds of the Commission may be applied to the payment—

(a) or discharge of expenses, obligations, including international obligations, or liabilities incurred in connection with the performance of the functions or exercise of the powers of the Commission;

(b) of any remuneration or allowances payable under this Act.

**72. Investment of surplus funds**

(1) The Board shall declare to the Minister any surplus funds that the Commission may have at the end of the financial year.

(2) Any funds of the Commission not immediately required for

any purpose under this Act, may be invested—

(a) on a fixed deposit account with a bank approved by the Board;

(b) in treasury bills and securities of the Government;

(c) in any other manner determined by the Board with the approval of the Minister, other than in the business licensed under this Act.

**73. Financial year of Commission.**

The financial year of the Commission is the period of twelve months beginning on the 1st day of July in each year, and ending on the 30th day of June in the next calendar year.

**74. Accounts.**

The Commission shall—

(a) keep proper books of accounts and all records relating to the transactions and affairs of the Commission;

(b) within three months after the end of the financial year, prepare annual financial statements for the preceding financial year; and

(c) within three months after the end of each financial year, submit the annual accounts to the Auditor General.

**75. Audit.**

(1) The Auditor General or an auditor appointed by the Auditor General shall, in each financial year, audit the accounts of the Commission.

(2) The Auditor General or an auditor appointed by the Auditor General shall within three months after receipt of the accounts submit to the Minister and Parliament a report on the audited accounts of the Commission.

PART XIII—OFFENCES AND PENALTIES.

**76. Unlawful opening of postal article.**

A person who—

(a) opens or permits to be opened any postal article otherwise than in accordance with this Act or any other law;

(b) knowingly reveals, discloses or in any way makes known the content of information in relation to a postal article opened under this Act or otherwise than in accordance with this Act or any other law;

(c) knowingly destroys, detains or secrets any mail bag or postal article otherwise than in accordance with this Act or any other law;

(d) knowingly permits any unauthorised person to interfere with any mail bag or postal article;

(e) fraudulently or with intent to deceive, prepares, alters, secrets or destroys any document used for the purposes of postal services,

commits an offence and is liable to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

**77. Issuing money order with fraudulent intent.**

A person who with intent to defraud or without a licence under this Act issues any money order or valuable security commits an offence and is liable on conviction to a fine not exceeding twelve currency points or to imprisonment not exceeding six months or both.

**78. Offences and penalties for unlicensed persons.**

Any person who establishes, installs, maintains, provides or operates—

(a) a radio communication station;

(b) a telecommunications system or service; or

(c) a postal service,

without a licence issued under this Act, commits an offence and is liable on conviction to a fine not exceeding ninety six currency points and in the case of a continuing offence, to a further fine not exceeding fifteen currency points for each day or part of a day during which the offence continues after conviction.

**79. Interception and disclosure of communication.**

(1) Any operator of a communications service or system, or employee of an operator of a communications service or system who—

(a) unlawfully intercepts any communication between other persons sent by means of that service or system;

(b) unlawfully interferes with or obstructs any radio communication; or

(c) unlawfully discloses any information in relation to a communication of which that operator or employee is aware,

commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

(2) Any person who without lawful excuse, intercepts, makes use of or divulges any communication except where permitted by the originator of the communication, commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

(3) For the purpose of sub-clause (2) where the conviction is a subsequent conviction, the person shall on conviction be liable to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

**80. Interception of Government communication.**

An operator of communications services or employee of an operator who intentionally intercepts, disrupts, denies accessibility to or diverts government communication commits an offence and is liable on conviction to a fine not exceeding ninety six currency points or imprisonment not exceeding forty eight months or both.

**81. Sending false distress signals.**

Any person who knowingly sends, transmits or causes to be sent or transmitted any false or fraudulent distress signal, message, call or radiogram of any kind commits an offence and is liable on conviction to a fine not exceeding thirty currency points and in the case of a second conviction to a fine not exceeding ninety six currency points, or to imprisonment not exceeding forty eight months or both.

**82. Offences in respect of radio communications.**

A person who—

(a) installs, operates or possesses a radio communications apparatus except in accordance with this Act; or

(b) without lawful excuse manufactures, imports, distributes, leases, offers for sale, sells, installs, modifies, operates or possesses any apparatus or device or its component under circumstances that give rise to a reasonable interference to another apparatus, device or component or if that apparatus device or component has been used, or is or was intended to be used, for the purposes of contravening this Act,

commits an offence and is liable on conviction to a fine not exceeding

one hundred and twenty currency points or imprisonment not exceeding five years or both and on a subsequent conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years.

**83. Protection of telecommunication installations.**

(1) A person who—

(a) prevents or obstructs the transmission or delivery of any message; or

(b) damages, removes or tampers with any installation or plant or any part of it belonging to an operator,

commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both and on a subsequent conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

(2) In addition to the penalty under subsection (1), the court may order the person convicted to make good any damage occasioned.

**84. False advertisement.**

A person who, without a licence, advertises or places a notice, mark or word at any place which notice, advertisement, mark or word signifies, implies or may reasonably lead the public to believe that the advertiser or other person is a holder of a licence under this Act commits an offence and is liable on conviction to a fine not exceeding ninety six currency points or imprisonment not exceeding four years or both and in case of a continuing offence, to a further fine not exceeding forty eight currency points for each day during which the offence continues after conviction.

**85. General penalty.**

Any person convicted of an offence under this Act for which no penalty is expressly provided is liable to a fine not exceeding ninety six currency points or imprisonment not exceeding four years or both.

PART XIV—MISCELLANEOUS.

**86. Powers of the Commission in a state of emergency.**

(1) The Commission may, during a state of emergency in the interest of public safety—

(a) direct any operator to operate a network in a specified manner in order to alleviate the state of emergency;

(b) take temporary possession of any communication station within Uganda, and any apparatus which may be installed and used in the station, for a specified period not exceeding six months;

(c) in writing direct a licensed person, to intercept or detain a postal article, class or description of postal articles in the course of transmission within Uganda and deliver it to an officer specified in the order.

(2) The officer to whom the article is delivered under subsection (1)(c) shall dispose of the article in the manner specified by the Commission.

(3) A proclamation by the President under article 110 of the Constitution is conclusive proof of the existence of a state of emergency.

**87. Transfer of assets and liabilities.**

All assets, rights and liabilities relating to communications services to which Uganda Communications Commission or Broadcasting Council were entitled or subject, before the commencement of this Act, shall vest in the Commission.

**88. Transfer of service contracts.**

Employees of Uganda Communications Commission and

Broadcasting Council immediately before the commencement of this Act whose services are transferred to the Commission shall transfer to the Commission on similar or better terms than those enjoyed by those employees before the transfer.

**89. Pension fund and retired and redundant employees.**

(1) All former employees of the Uganda Communications Commission or Broadcasting Council who at the commencement of this Act are receiving retirement benefits and pensions from the Uganda Communications Commission or Broadcasting Council shall continue to be paid by the Commission.

(2) All employees of Uganda Communications Commission or Broadcasting Council who become redundant as a result of the implementation of section 88 shall be paid the calculated and ascertained retirement benefits and pension due to them under the Uganda Communications Act or the Electronic Media Act respectively.

(3) The contributory pension fund established under the Uganda Communications Act shall continue in force in accordance with this Act.

**90. Agreements and licences by the Commission or Broadcasting Council.**

All valid—

(a) licences issued by Uganda Communications Commission or Broadcasting Council before the commencement of this Act; and

(b) any other agreements entered into by Uganda Communications Commission or Broadcasting Council before the commencement of this Act,

shall remain valid and only be modified by the Commission within one year from the time the Commission commences operations to the extent that any provisions of the agreements or licences are inconsistent with this Act.

**91. Pending court proceedings or orders of court.**

(1) Any pending court proceedings, court actions, judgments or court orders which were enforceable by or against Uganda Communications Commission immediately before the commencement of this Act, and are connected with the assets vested in the Commission or the functions of the Commission, shall be enforceable by or against the Commission as they would have been enforced by or against the Uganda Communications Commission, immediately before the commencement of this Act.

(2) Any pending court proceedings, judgment or order against the Attorney General arising out of matters connected with the Broadcasting Council, shall continue against the Attorney General until they are disposed of or satisfied.

**92. Service of notices on the Commission.**

Any notice or other document required to be served on the Commission may be served by—

(a) delivery to the Executive Director or any authorised employee;

(b) delivery at the office of the Executive Director and obtaining evidence of receipt; or

(c) courier delivery to the Executive Director.

**93. Regulations.**

(1) The Minister may, after consultation with the Commission and with the approval of Parliament, by statutory instrument, make regulations for better carrying into effect the provisions of this Act.

(2) Without prejudice to subsection (1) the Minister may make

regulations relating to—

(a) fees payable upon the grant or renewal of a licence;

(b) the classification or categories of licences;

(c) the use of any communications station, apparatus or licence;

(d) obligations for permitting and facilitating the inspection of any communications station, apparatus or licence;

(e) anti competitive practices;

(f) energy regulation requirements to be complied with by any person who uses, sells, other than for export, or lets on hire any apparatus generating, designed to generate or liable to generate, fortuitous electromagnetic energy at frequencies that may be specified;

(g) the exhibition at any communications station of notices that may be specified in the regulations;

(h) the use on board any vessel or aircraft other than a vessel or aircraft registered or licensed in Uganda, within the limits of Uganda and the territorial waters adjacent to Uganda, of communications apparatus on that vessel or aircraft, and the importation, acquisition, manufacture, sale, letting on hire or other disposition of communications apparatus of any kind, or the use or installation of that apparatus;

(i) the requirements of the communications services to be provided by a licensee, in terms of quantitative and quality criteria;

(j) the specifications of reserved and mandatory services to be provided for by an operator under this Act;

(k) the way the consumer will be informed about the range of

commercial services and the conditions under which they are provided;

(l) prescribing conditions to be observed in the erection, alteration or equipment of cinematograph theatres;

(m) prescribing conditions to be observed in relation to safety from fire or otherwise of any cinematograph theatre or the control of person attending the theatre;

(n) the conditions under which a licensee can apply for compensation for loss-incurring operations as the result of the operator's obligation imposed on the operator by the Commission regarding the provision of uneconomic services in pursuance of the objectives of this Act;

(o) the retention of records relating to programmes or broadcasts;

(p) the obligations of proprietors, producers or broadcaster in respect of public broadcasts;

(q) the licensing and management of telecommunication numbering and orbital slots;

(r) the regulation of community broadcasting.

(3) Regulations made shall be laid before Parliament.

(4) Regulations made under this section may provide in respect of any contravention of the regulations for the imposition of a fine not exceeding forty eight currency points or imprisonment not exceeding twenty four months or both.

(5) The Executive Director may by notice require anybody who, in his or her opinion is not complying with the regulations made under this section, to discontinue the use, sale or letting on hire, as the

case may be, the apparatus in question, or to use, sell or let on hire the apparatus subject to conditions that may be specified in the notice.

**94. Amendment of Cap. 49**

The Stage Plays and Public Entertainment Act is amended—

(a) in section 1by substituting for paragraph (a) the following—

"(a) Commission means the Uganda Communications Commission established under the Uganda Communications Act, 2013.";

(b) by substituting for any reference to "council" in that Act, a reference to "Commission".

**95. Amendment of Schedules.**

The Minister may, with the approval of Cabinet, by statutory instrument amend the Schedules to this Act.

**96. Repeal and saving.**

(1) The Electronic Media Act, Cap. 104 and the Uganda Communications Act, Cap. 106 are repealed.

(2) Notwithstanding subsection (1), any statutory instrument made under the Electronic Media Act or the Uganda Communications Act which is in force immediately before the commencement of this Act, shall remain in force until revoked under this Act.

———

## SCHEDULES

SCHEDULE 1.

*Section 2*

Currency point

One currency point is equivalent to twenty thousand shillings

SCHEDULE 2

*Section 4*

**Seal of the Commission.**

1. The common seal of the Commission shall be determined by the Commission and shall be kept in the custody of the Executive Director.

2. The common seal shall, when affixed to any document, be authenticated by the signatures of the chairperson and the Executive Director.

3. In the absence of the chairperson or when the chairperson is unable to perform this function, two other members of the Commission appointed for that purpose shall sign in the place of the chairperson.

4. A person performing the functions of Executive Director shall sign in the absence of the Executive Director.

5. A contract or instrument which if entered into or executed by a person not being a body corporate would not be required to be under seal may be entered into or executed without seal on behalf of the Commission by the Executive Director or any other person authorised in that behalf by the Commission.

6. Every document purporting to be—

(a) an instrument issued by the Commission and sealed with the common seal of the Commission and authenticated in the manner prescribed in paragraphs 2 to 4; or

(b) a contract or instrument entered into or executed under paragraph

5,

shall be received in evidence as such an instrument without further proof unless the contrary is proved.

SCHEDULE 3

*Section 12*

**Meetings of the Board.**

**1. Meetings of the Board.**

(1) Meetings of the Board shall be convened by the chairperson, and the Commission shall meet for the transaction of business at such places and times as may be decided upon by the Board but in any case shall meet at least once every three months.

(2) The chairperson or, in the absence of the chairperson, a member appointed by the Board to act in the chairperson's place may at any time call a special meeting of the Board and shall call a special meeting upon a written request by a majority of the members of the Board.

(3) The chairperson shall preside at every meeting of the Board.

(4) In the absence of the chairperson, the members present may appoint a member from among themselves to preside at that meeting.

**2. Quorum.**

The quorum at a meeting of the Board shall be four members.

**3. Decisions of the Board.**

(1) All questions proposed at a meeting of the Board shall be decided by a simple majority of the votes of the members present and voting; and in case of an equality of votes, the person presiding shall have a casting vote in addition to that person's deliberative vote.

(2) A decision may be made by the Board without meetings but by circulation of the relevant papers among the members and by the expression of the views of the majority of the members in writing; however, any member shall be entitled to require that the decision be deferred and the matter on which a decision is sought be considered at a meeting of the Board.

**4. Board may co-opt members.**
The Board may invite any person to attend any of its meetings as a consultant and may co-opt any person to the Board but that person shall not vote on any matter before the Board.

**5. Declaration of interest.**
(1) Any member of the Board having pecuniary or other interest, directly or indirectly in any contract or proposed contract or other matter before the Board shall, at that meeting, declare the nature of such interest and shall not take part in any discussion or vote on that matter; and if the chairperson directs, the person shall withdraw from that meeting.

(2) The failure of any member of the Board to disclose an interest in any contract or proposed contract or any other matter before the Board will cause the decision of the Board to be voidable at the instance of the other members of the Board, and that member shall be liable to be relieved of his or her duties.

(3) For purposes of determining whether there is a quorum, a member withdrawing from a meeting or who is not taking part under subparagraph (1) shall be treated as being present.

**6. Board may regulate its procedure.**
Subject to this Act, the Board may regulate its own procedure and may make rules regarding the holding of meetings, notice to be given, the keeping of minutes or any other matter relating to its meetings.

SCHEDULE 4

*Section 31*

**Minimum broadcasting standards.**

A broadcaster or video operator shall ensure that—

(a) any programme which is broadcast—

(i) is not contrary to public morality;

(ii) does not promote the culture of violence or ethnical prejudice among the public, especially the children and the youth;

(iii) in the case of a news broadcast, is free from distortion of facts;

(iv) is not likely to create public insecurity or violence;

(v) is in compliance with the existing law;

(b) programmes that are broadcast are balanced to ensure harmony in such programmes;

(c) adult-oriented programmes are appropriately scheduled;

(d) where a programme that is broadcast is in respect to a contender for a public office, that each contender is given equal opportunity on such a programme;

(e) where a broadcast relates to national security, the contents of the broadcast are verified before broadcasting.

SCHEDULE 5

*Section 68*

**Rate of percentage of gross annual revenue payable by operators**

The rate of gross annual revenue payable by an operator to the Commission under section 68 shall not be less than 2 percent and shall not exceed 2.5 percent.

SCHEDULE 6

*Section 39*

**Conditions of a licence.**

1. A licence issued under this Act may include the following conditions—

(a) the payment of sums of money calculated as a proportion of the rate of the annual turnover of the operator's licensed system or otherwise;

(b) the payment by the operator of a contribution toward any loss incurred by another operator as a result of such other operator's obligation imposed on the operator by the Commission regarding the provision of uneconomic service in pursuance of the objectives of this Act;

(c) the provision of services to disadvantaged persons;

(d) interconnection of an operator's telecommunications system with any other system and permitting the connection of telecommunications apparatus to an operator's system;

(e) prohibiting an operator from giving undue preference to or from exercising undue discrimination against any particular person or class of persons, including any operator;

(f) furnishing the Commission with such documents, accounts, returns or such other information as the Commission may require for the performance of its functions under this Act;

(g) requiring an operator to publish in such manner as may be specified in the licence a notice stating the charges and terms and conditions that are to be applicable to facilities and services provided;

(h) provision of service on priority service to the Government or specified organisations;

(i) requiring an operator to ensure that an adequate and satisfactory information system, including billing, tariff, directory information and directory inquiry services, is provided to customers;

(j) conditions specifying the criteria for setting tariffs;

(k) requiring an operator to comply with such technical standards or requirements, including service performance standards, as may be specified in the licence;

(l) any other condition as the Commission may consider appropriate or expedient.

2. It is a condition of every licence issued under this Act that the licensee shall—

(a) comply with all relevant international conventions or instruments to which Uganda is a party;

(b) in the case of a broadcaster, allocate time for the coverage of national events and functions.

3. A licence shall not be used for a purpose other than that for which it is issued.

**Cross References**
Electronic Media Act, Cap. 104.
Uganda Communications Act, Cap. 106.
The Stage Plays and Public Entertainments Act, Cap. 49.
Press and Journalist Act, Cap. 105.

# APPENDIX 5

## THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY ACT 2009

ACTS
SUPPLEMENT No. 3 31st July, 2009.
ACTS SUPPLEMENT
*to The Uganda Gazette No. 36 Volume CII dated 31st July, 2009.*
Printed by UPPC, Entebbe, by Order of the Government.

**Act 4** *National Information Technology Authority, Uganda Act* **2009**

# THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA ACT, 2009.

## ARRANGEMENT OF SECTIONS

*Section*

*Section*

# THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA ACT, 2009.

**An Act to provide for the establishment of the National Information Technology Authority, Uganda and to provide for its objects, functions, composition, management and finances; and other related matters.**

DATE OF ASSENT: 15th July, 2009.

*Date of Commencement:* See section 1.

BE IT ENACTED by Parliament as follows—

PART I—PRELIMINARY

**1. Commencement.**
This Act shall come into force on a date appointed by the Minister by statutory instrument.

**2. Interpretation.**
In this Act, unless the context otherwise requires—

"authorised officer" means a person appointed as an authorised officer under section 18 and includes a computer scientist, network administrator, systems administrator, systems analyst, data base administrator, software engineer, programmer, information technology security administrator, electronic engineer, communications engineer and a telecommunication specialist;

"Authority" means the National Information Technology Authority, Uganda established by section 3;

"Board" means the Board of Directors appointed under section 7;

"Chairperson" means the Chairperson of the Board appointed under section 7;

"currency point" has the value assigned to it in Schedule 1 to this Act;

"data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose;

"Executive Director" means the chief executive of the Authority, appointed under section 16;

"e-Commerce" means the distribution, buying, selling, marketing and servicing of products or services over electronic systems such as the internet or other computer networks;

"e-Government" is the use of information and communication technologies to deliver public services in a convenient, efficient customer-oriented, and cost-effective way;

"e-Readiness survey" means a survey undertaken to establish the ability to use information technologies;

"e-Transaction" means the exchange of information or data, the sale or purchase of goods or services between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks;

"e-waste" means any form of waste that is accumulated as a result of hardware used in information technology;

"information technology" means the science of collecting and using information by means of computer systems and refers to computers, ancillary or peripheral equipment such as printers and scanners, software and firmware services including support services, and related resources and includes any equipment or interconnected systems that are

used in the acquisition, storage, manipulation or processing, management, movement, control, display, transmission or reception of data or information;

"information technology survey" means an operation in which enumerations, inspections, studies, examinations, reviews, inquiries or analyses are carried out to collect or gather information and data on matters related to information technology;

"member" means a member of the Board of Directors appointed under section 7;

"Minister" means the Minister responsible for information technology.

PART II—ESTABLISHMENT, OBJECTS, FUNCTIONS AND POWERS OF THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA.

**3. Establishment of the Authority.**

(1) There is established an autonomous body known as the National Information Technology Authority, Uganda (NITA—U).

(2) The Authority shall be a body corporate with perpetual succession and a common seal, and shall be capable of suing and being sued in its corporate name and, subject to this Act, may borrow money, acquire and dispose of property and do or suffer any other thing a body corporate may lawfully do or suffer.

(3) The Authority shall be an agency of Government and shall be under the general supervision of the Minister.

**4. Objects of the Authority.**

The objects of the Authority are—

(a) to provide high quality information technology services to Government;

(b) to promote standardisation in the planning, acquisition, implementation, delivery, support and maintenance of information technology equipment and services, to ensure uniformity in quality, adequacy and reliability of information technology usage throughout Uganda;

(c) to provide guidance and other assistance as may be required to other users and providers of information technology;

(d) to promote cooperation, coordination and rationalisation among users and providers of information technology at national and local level so as to avoid duplication of efforts and ensure optimal utilisation of scarce resources;

(e) to promote and be the focal point of co-operation for information technology users and providers at regional and international levels; and

(f) to promote access to and utilisation of information technology by the special interest groups.

**5. Functions of the Authority.**

The functions of the Authority are—

(a) to provide first level technical support and advice for critical Government information technology systems including managing the utilisation of the resources and infrastructure for centralised data centre facilities for large systems through the provision of specialised technical skills;

(b) to identify and advise Government on all matters of information technology development, utilisation, usability, accessibility and deployment including networking, systems development, information technology security, training and support;

(c) to co-ordinate, supervise and monitor the utilisation of information technology in the public and private sectors;

(d) to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals;

(e) to create and manage the national databank, its inputs and outputs;

(f) to set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organisation, sustenance, disposal, risk management, data protection, security and contingency planning;

(g) to regulate the electronic signature infrastructure and other related matters as used in electronic transactions in Uganda;

(h) to promote and provide technical guidance for the establishment of e-Government, e-Commerce and other e-Transactions in Uganda;

(i) in liaison with other relevant institutions, to regulate the information technology profession in Uganda in order to ensure its effective utilisation promotion and development;

(j) to act as an authentication center for information technology training in Uganda in conjunction with the Ministry responsible for Education;

(k) to provide advice on information technology project management services to Government;

(l) to provide for information management service through acting as a records management facility and an information depository;

(m) to provide guidance on the establishment of an infrastructure for information sharing by Government and related stakeholders;

(n) to provide guidance in information technology audit services to Government;

(o) to undertake and commission research as may be necessary to promote the objects of the Authority;

(p) to arbitrate disputes arising between suppliers of information technology solutions and consumers;

(q) to protect and promote the interests of consumers or users of information technology services or solutions;

(r) to undertake any other activity necessary for the implementation of the objects of the Authority.

**6. Powers of the Authority.**

In carrying out the functions specified in section 5, the Authority shall have the following powers—

(a) to carry out regular e-Readiness surveys to ascertain the status of information technology in Uganda;

(b) to establish a repository of information technology standards, and for the registration and classification of documentation related to locally developed and imported information technology solutions;

(c) to establish a mechanism for collaboration and promotion of partnerships between various categories of players in the information technology sector;

(d) to regulate and certify information technology education in Uganda in consultation with the Ministry responsible for Education or its agencies;

(e) to charge fees for services provided by the Authority.

PART III—THE BOARD AND ITS FUNCTIONS

**7. The Board.**

(1) There is established a Board of Directors as the governing body of the Authority, which shall consist of the following members—

(a) the Chairperson;

(b) the Executive Director;

(c) the Commissioner responsible for information technology in the Ministry responsible for information technology;

(d) four other nominees, at least one of whom shall be an eminent Ugandan with expertise in information technology.

(2) The Chairperson and the members of the Board mentioned in subsection (1) (d) shall be appointed by the Minister, with the approval of Cabinet.

(3) In making the appointments to the Board, the Minister shall take into consideration gender equity.

(4) The Executive Director shall be the secretary to the Board.

**8. Qualifications for appointment to the Board.**

The Chairperson and the members of the Board mentioned in section 7 (1) (d) shall be appointed from among persons who qualify for appointment by virtue of their professional qualifications, knowledge and experience in disciplines relevant to the functions of the Authority.

**9. Tenure of office of members of the Board.**

The Chairperson and the members of the Board mentioned in section 7 (1) (d) shall hold office on such terms and conditions as may be specified in the instrument of appointment, for a period of three years which may be renewed for one further term.

**10. Powers of Minister to suspend or terminate appointment of members of the Board.**

(1) The Minister may, at any time suspend or terminate the appointment of the Chairperson or a member of the Board mentioned in section 7 (1) (d) for—

(a) abuse of office;

(b) corruption;

(c) incompetence;

(d) any physical or mental incapacity that renders a person incapable of performing the duties of that office;

(e) failure to attend three consecutive Board meetings without reasonable grounds;

(f) conviction of an offence involving moral turpitude;

(g) being adjudged bankrupt by a court of law;

(h) any other reasonable ground.

(2) A member of the Board other than the Executive Director may resign from the Board by giving notice in writing to the Board, of not less than one month.

**11. Functions of the Board.**

The Board shall—

(a) formulate policy guidelines for the Authority;

(b) monitor the implementation of the plans and programmes of the Authority;

(c) approve the annual budget and action plan of the Authority;

(d) appoint the staff of the Authority;

(e) determine the structure and staffing levels of the Authority and the terms of service of the staff of the Authority;

(f) establish rules and procedures for—

(i) the appointment, career development and disciplining of staff;

(ii) the management of the finances and assets of the Authority; and

(iii) the procurement of goods and services for the Authority and for the disposal of the assets of the Authority, in accordance with the Public Procurement and Disposal of Public Assets Act, 2003;

(g) submit a quarterly report to the Minister, on the activities of the Authority and any other reports as may be deemed necessary;

(h) perform any other functions as may be approved by the Minister in writing, on the recommendation of the Board.

**12. Meetings of the Board.**

(1) Schedule 2 shall have effect in relation to the meetings of the Board and to other matters provided for in it.

(2) The Board may co-opt any person to participate in its deliberations, but a person so co-opted shall not have a right to vote.

**13. Conditions of service of members of the Board.**

The Minister shall, in consultation with the Minister responsible for finance, determine the terms and conditions of service of the members of the Board, except for the Executive Director.

PART IV—SECRETARIAT

**14. Secretariat.**

The Authority shall have a Secretariat headed by an Executive Director and shall consist of directorates covering the following areas—

(a) planning, research and development;

(b) technical services;

(c) e-Government services;

(d) finance and administration;

(e) regulation and legal services;

(f) any other area approved by the Minister.

**15. Functions of the Secretariat.**

The Secretariat shall—

(a) be the source of official information and data relating to information technology in Uganda;

(b) implement Government and national information technology policies, strategies and action plans;

(c) be the custodian of the national information technology policies, strategies and action plans;

(d) coordinate and monitor information technology initiatives in the public and private sectors;

(e) perform any other duties as the Board may instruct from time to time.

**16. Executive Director.**

(1) The Executive Director shall be appointed by the Minister on the recommendation of the Board.

(2) A person to be appointed Executive Director shall be a person with considerable practical, professional and administrative experience in information and communication technology.

(3) The Executive Director shall hold office for five years and is eligible for re-appointment for one more term.

(4) The terms and conditions of service of the Executive Director shall be determined by the Board and approved by the Minister and shall be specified in the instrument of appointment.

(5) Subject to the general supervision and direction of the Board, the Executive Director shall be the accounting officer of the Authority and shall be responsible for—

(a) the management and operations of the Authority;

(b) the management of the funds, property and business of the Authority;

(c) the administration, organisation and control of the officers and staff of the Authority; and

(d) the promotion, training and disciplining of the officers and staff of the Authority in accordance with their terms and conditions of appointment.

(6) The Executive Director shall be a full time employee of the Authority.

(7) The Executive Director shall on appointment, take and subscribe before the Board, the oath of office and secrecy, specified in Schedule 3.

(8) The Minister may, after consultation with the Board, terminate the appointment of the Executive Director for—

(a) abuse of office;

(b) corruption;

(c) incompetence;

(d) physical or mental incapacity that renders the Executive Director incapable of performing the duties of that office;

(e) failure to attend three consecutive Board meetings without reasonable grounds;

(f) conviction of an offence involving moral turpitude;

(g) being adjudged bankrupt by a court of law;

(h) any other reasonable ground.

**17. Other officers and staff of the Authority.**

(1) The Board may, on the advice of the Executive Director, appoint directors to head the directorates specified in section 14.

(2) A director appointed under subsection (1) shall hold office for five years and is eligible for re-appointment for one more term.

(3) The terms and conditions of service of the directors shall be determined by the Board and specified in their instruments of appointment.

(4) The Board may, on the advice of the Executive Director, appoint other officers and staff of the Authority, as may be necessary for the effective performance of the functions of the Authority.

(5) The officers and staff appointed under subsection (4) shall hold office on such terms and conditions as the Board may determine and specify in their instrument of appointment.

(6) A director appointed under subsection (1), shall on appointment, take and subscribe before the Board, the oath of office and secrecy specified in Schedule 3.

(7) An officer appointed under subsection (4), shall on appointment, take and subscribe before the Executive Director, the oath of office and secrecy provided in Schedule 3.

(8) The Board shall be responsible for the discipline and management of the officers and staff.

**18. Authorised officers.**

(1) The Board may, from time to time appoint authorised officers for the purposes of carrying out information technology surveys under this Act.

(2) The terms of service of an authorised officer shall be determined by the Board and an authorised officer shall carry out such services in relation to information technology, as the Board may determine.

PART V—INFORMATION TECHNOLOGY SURVEYS AND POWERS OF THE AUTHORITY

**19. Information technology surveys.**

(1) The Minister may, on the recommendation of the Board, direct, by statutory order that an information technology survey be taken by the Authority in both public and private sectors.

(2) An order made under subsection (1) shall specify—

(a) the sector in respect of which the survey is to be carried out;

(b) the purpose of the survey;

(c) the date on which the survey is to be undertaken; and

(d) the information to be obtained in the survey.

(3) In carrying out a survey under this section, the Authority—

(a) shall have power to collect information and data regarding information technology for the sector specified in the order;

(b) may use summons and search warrants to facilitate the enforcement of paragraph (a).

**20. Authority to obtain particulars.**

(1) Where data or information on information technology is being collected in accordance with section 19, the Executive Director, an officer of the Authority or an authorised officer, may require any person to supply him or her with any particulars as may be prescribed, or any particulars as the Executive Director may consider necessary or desirable in relation to the collection of the information.

(2) A person who is required to give information under subsection (1), shall, to the best of his or her knowledge and belief provide all the necessary information, in the manner and within the time specified by the Executive Director.

**21. Power of entry and inspection.**

(1) The staff of the Authority or an authorised officer may at all reasonable times enter and inspect any building or place and make such inquiries as may be necessary for the collection of information and data for a survey being carried out under section 19.

(2) Notwithstanding subsection (1), the staff of the Authority or an authorised officer is not entitled to enter a dwelling house except for the purposes of collecting information relating to information technology matters and for the exercise of functions under this Act.

**22. Confidentiality.**

(1) Except for the purpose of a prosecution, public interest, court order or state of emergency—

(a) an individual return or part of the return made for the purpose of this Act;

(b) an answer given to any question put for the purposes of this Act;

(c) a report, abstract or document, containing particulars contained in any return or answer which is arranged as to render possible identification of those particulars with any person, business or undertaking; and

(d) data set or part of data stored in a computer or any other electronic media,

shall not be published, admitted in evidence, or shown to any person who is not employed in the execution of a duty under this Act except with the written consent of the person who made the return or gave the answer, or, in the case of a business or undertaking, from the person having the control, management or superintendence of the business or undertaking.

(2) Subsection (1) does not apply where the person, business or undertaking has published the return, answer, report, abstract or document and opened up a computerised data set for general access.

(3) Nothing in this section shall prevent or restrict the publication of any report, abstract or document without the consent referred to in subsection (1) where the particulars contained in the report, abstract or document render identification possible merely by reason of the fact that they relate to an undertaking or business which is the only undertaking or business within its particular sphere of activities, if the particulars do not render possible identification of the costs of production of, or the capital employed or profits arising in the undertaking or business.

(4) Notwithstanding the restrictions under subsection (1), the Authority may release unit records on computer media, with identifiers removed, where the Authority—

(a) is satisfied that the unit records are to be used for genuine research purposes;

(b) obtains from the recipient of the records a written undertaking that the records will not be released to any other person without the written consent of the Authority;

(c) obtains from the recipient a written undertaking to make available a copy of the research findings to the Authority;

(d) is satisfied that the unit records cannot be identified as relating to any particular person or business enterprise.

**23. Dissemination of information and data on information technology.**

The Authority may release for general dissemination any information or data collected from a survey, after appropriate processing and ascertaining its quality for accuracy, and after ensuring confidentiality with respect to any individual who provided information.

PART VI—FINANCES OF THE AUTHORITY.

**24. Funds of the Authority.**

(1) The funds of the Authority shall consist of—

(a) money appropriated by Parliament for the purposes of the Authority;

(b) loans and grants received by the Authority for its activities; and

(c) revenues collected from services rendered by the Authority.

(2) The Authority shall open and maintain bank accounts in banks approved by the Board.

**25. Estimates.**

(1) The Executive Director shall, within three months before the end of each financial year, cause to be prepared and submitted to the Board for its approval, estimates of the income and expenditure of the Authority for the following financial year.

(2) The Board shall, within two months after receipt of the estimates referred to in subsection (1), cause to be submitted to the Minister for his or her approval, the estimates of income and expenditure for the following financial year as approved by the Board.

(3) Expenditure shall not be made out of the funds of the Authority unless that expenditure is part of the expenditure approved by the Board under the estimates for the financial year in which the expenditure is incurred.

**26. Annual management plan.**

The Executive Director shall, not later than three months before the end of each financial year, prepare and submit to the Board, for approval, an annual management plan for the next financial year.

**27. Accounts.**

(1) The Authority shall keep proper books of accounts of all its income and expenditure and proper records in relation to them.

(2) Subject to any direction given by the Minister, the Board shall cause to be prepared in respect of each financial year, and not later than three months after the close of the financial year, a statement of accounts which shall include a report on the performance of the Authority during that financial year.

(3) The statement of accounts shall comprise—

(a) a balance sheet and a statement of income and expenditure of the Authority in respect of that financial year; and

(b) any other information in respect of the financial affairs of the Authority as the Minister may in writing require.

**28. Audits.**

(1) The accounts of the Authority shall, in respect of each financial year, be audited by the Auditor General or by an auditor appointed by the Auditor General.

(2) The Board shall ensure that within four months after the close of each financial year, the statement of account described in section 27 is submitted for auditing under this section.

(3) The Auditor General and any auditor appointed by the Auditor General shall have access to all books of account, vouchers and other financial records of the Authority and is entitled to have any information and explanations required by him or her in relation to them, as he thinks fit.

(4) The Auditor General shall within two months after receipt of the statement of account under subsection (2), audit the accounts and deliver to the Board a copy of the audited accounts together with his or her report on them stating any matter which in his or her opinion should be brought to the attention of the Minister.

(5) The Board shall as soon as possible upon receiving it, deliver to the Minister a copy of the audited accounts together with the report of the auditor submitted under subsection (4).

**29. Borrowing powers.**

(1) The Authority may, with the prior approval of the Minister, obtain loans and other credit facilities required for meeting its obligations and for carrying out its objects and functions under this Act.

(2) Subject to Article 159 of the Constitution, a loan or credit facility obtained by the Authority under this section may, with the prior approval of the Minister, be guaranteed by the Government and when so guaranteed, the principal sum and interest of the loan shall be charged on the Consolidated Fund.

**30. Financial year of the Authority.**

The financial year of the Authority shall be the same as the financial year of Government.

**31. Compliance with Public Finance and Accountability Act, 2003.**

The Authority shall at all times comply with the Public Finance and Accountability Act, 2003.

PART VII—MISCELLANEOUS

**32. Relationship with other organisations.**

(1) The Authority shall in performing its functions, consult and cooperate with organisations with functions related to, or having aims or objectives related to those of the Authority.

(2) The Authority may, on such terms and conditions considered necessary, delegate any of its functions under this Act to any organisation.

(3) It shall be the duty of any organisation to which subsection (1) relates to cooperate with the Authority in the carrying out of its functions under this Act.

**33. Seal.**

(1) The application of the seal of the Authority on any document shall be authenticated by the signatures of the Chairperson and the Executive Director, and in the absence of the Chairperson, by any one member of the Board, as shall be decided by the Board, and the Executive Director.

(2) Every document purporting to be an instrument issued by the Authority, sealed with the seal of the Authority and authenticated in accordance with subsection (1), shall be taken to be an instrument of the Authority and shall be received in evidence without further proof.

**34. Minister's powers to give directions.**

(1) The Minister may, after consultation with the Executive Director and the Board, give to the Authority directions of a general nature in writing, relating to policy matters in the exercise of the functions of the Authority; and the Authority shall comply with any direction given by the Minister.

(2) The particulars of any directions given by the Minister under subsection (1) shall be included in the annual report of the Authority, together with the extent to which the directions were complied with.

**35. Protection from liability.**

(1) A member of the Board shall not be personally liable in respect of any act or omission done in good faith in the performance of his or her functions under this Act.

(2) An employee or other person acting on behalf of the Authority shall not be personally liable in respect of any act or omission done in good faith in the performance of his or her functions under this Act.

**36. Annual report.**

The Board shall cause to be prepared and shall submit to the Minister within three months after the end of each financial year, an annual report on the activities and operations of the Authority for that financial year.

**37. Minister to report to Parliament.**

The Minister shall in each financial year, submit to Parliament as soon as possible after receiving them, the Auditor General's report and the annual report of the Authority.

**38. Offences.**

(1) A person who is employed in the execution of any duty under this Act who—

(a) by virtue of the employment or duty comes into possession of information which may influence or affect the market value of any share or other security, interest or article and who before the information is made public, directly or indirectly uses it for personal gain;

(b) without lawful authority, publishes or communicates to any person other than in the ordinary course of his or her employment any information acquired by him or her in the course of the employment or duty; or

(c) knowingly compiles for issue, any data or information relating to information technology which he or she becomes possessed of by virtue of his or her employment,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction, to a fine not exceeding six hundred currency points or imprisonment not exceeding five years, or both.

(3) A person in possession of any information which to his or her knowledge is disclosed in contravention of this Act, who publishes or communicates that information to any other person, commits an offence and is liable, on conviction, to a fine not exceeding twenty four currency points or imprisonment not exceeding one year, or both.

(4) A person commits an offence who—

(a) hinders or obstructs the Executive Director, an officer of the Authority or an authorised officer, in the lawful performance of any duties or in lawful exercise of any power imposed or conferred on him or her under this Act;

(b) refuses or neglects—

(i) to complete and supply, within the time specified for the purpose, the particulars required by the Authority in any return, form or other document;

(ii) to answer any question or inquiries put to or made of him or her, under this Act; or

(c) knowingly or negligently makes in a return, form or other document completed by him or her under this Act or in any answer to any question or enquiry put to or made of him or her under this Act, a statement which is untrue in any material particular.

(5) A person who commits an offence under subsection (4) is liable, on conviction, to a fine not exceeding twelve currency points or imprisonment not exceeding six months, or both.

**39. Regulations.**

(1) The Minister may, in consultation with the Board, by statutory instrument, make regulations generally for giving effect to the provisions of this Act.

(2) Regulations made under this section may prescribe in connection with the contravention of the regulations—

(a) a penalty of a fine not exceeding forty eight currency points or imprisonment not exceeding two years imprisonment or both;

(b) in the case of a second or subsequent offence, a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both;

(c) in the case of a continuing offence an additional fine not exceeding ten currency points for each day on which the offence continues;

(d) a requirement that the court convicting the accused may order the forfeiture of anything used in connection with the commission of the offence.

**40. Amendment of Schedules.**

(1) The Minister may, with the approval of Cabinet, by statutory instrument, amend Schedule 1 to this Act.

(2) The Minister may, on the advice of the Board, by statutory instrument, amend Schedule 2 to this Act.

(3) The Minister may, on the advice of the Board, by statutory instrument, amend Schedule 3 to this Act.

**SCHEDULES**

SCHEDULE 1

*Sections 2and 40*

CURRENCY POINT

A currency point is equivalent to twenty thousand shillings.

SCHEDULE 2 *Sections 12 and 40*

MEETINGS OF THE BOARD AND RELATED MATTERS

**1. Meetings of the Board.**

(1) The Board shall meet at least every two months at such places and at such times as may be decided upon by the Board.

(2) The Chairperson shall preside at every meeting of the Board and in his or her absence, the Executive Director shall call the meetings and the members present shall elect from among their number, an acting chairperson.

**2. Quorum.**

The quorum for a meeting of the Board shall be four members; but where a member declares an interest in an agenda item or in the matter before the Board, the member shall not be counted for purposes of forming a quorum in relation to the item or matter in question.

**3. Decisions of the Board.**

(1) Decisions at a meeting of the Board shall be by a majority of the votes of the members present and where there is an equality of votes, the person presiding at the meeting shall have a casting vote in addition to his or her deliberative vote.

(2) A decision may be made by the Board without a meeting, by the circulation of information electronically or using hard copies, among members of the Board and by the expression of the views of the majority of the members in writing, but any member shall be entitled to require that the decision be deferred and the matter on which a decision is sought be considered at a meeting of the Board.

(3) The validity of any proceedings of the Board shall not be affected by any vacancy amongst the members or any defect in the appointment of a member.

(4) The decision reached by the Board thereafter shall be binding on all members.

**4. Disclosure of interest.**

(1) A member of the Board who has a direct or indirect personal interest in a matter being considered or which is about to be considered by the Board shall, as soon as possible after the relevant facts have come to his or her knowledge, disclose the nature of his or her interest to the Board.

(2) A disclosure of interest under subparagraph (1) shall be recorded in the minutes of the meeting of the Board and the member who makes the disclosure shall not, unless the Board otherwise determines in respect of that matter—

(a) be present during any deliberation on the matter by the Board;

(b) take part in the decisions of the Board.

(3) For the purpose of making a decision by the Board under subparagraph (2), in relation to a member who makes a disclosure under subparagraph (1), the member who makes the disclosure shall not—

(a) be present during the deliberations of the Board for making the determination;

(b) influence any other member or participate in the making by the Board of the determination.

(4) Where there is no quorum for the continuation of a meeting only because of the exclusion of a member from the deliberations on a matter in which he or she disclosed a personal interest, the other members present may—

(a) postpone the consideration of that matter until a quorum, without that member is realised; or

(b) proceed to consider and decide the matter as if there is a quorum.

**5. Minutes of proceedings.**

(1) The Board shall cause the minutes of all proceedings of its meetings to be recorded and kept, and the minutes of each meeting shall be confirmed by the Board at the next meeting and signed by the Chairperson of that meeting.

(2) The Chairperson shall submit to the Minister a copy of the minutes of each meeting of the Board as soon as the minutes are confirmed.

**6. Residual power of Board to regulate its proceedings.**

Subject to this Schedule, the Board shall regulate its proceedings.

SCHEDULE 3

Sections 16 (7), 17 and 40

OATH OF OFFICE AND SECRECY

I …… swear that I will faithfully and honestly fulfill my duties as …… in conformity with the requirements of the National Information Technology Authority, Uganda Act, and that I will not directly or indirectly communicate or reveal any matter to any person which shall be brought under my consideration or shall come to my knowledge in the discharge of my official duties except as may be required for the discharge of my official duties or as may be authorised by law. (So help me God.)

**Cross References.**

Public Finance and Accountability Act, 2003, Act No, 6 of 2003.
Public Procurement and Disposal of Public Assets Act, 2003, Act No. 1 of 2003

# APPENDIX 6

## THE ANTI PONOGRAPHY ACT 2014


**THE ANTI-PORNOGRAPHY ACT, 2014.**

THE REPUBLIC OF UGANDA

I SIGNIFY my assent to the bill.

*President*

*Date of assent:* 6/2/2014.

# THE ANTI-PORNOGRAPHY ACT, 2014

## ARRANGEMENT OF SECTIONS

*Section*

*Section*

THE REPUBLIC OF UGANDA

## THE ANTI-PORNOGRAPHY ACT, 2014

**An Act to define and create the offence of pornography; to provide for the prohibition of pornography; to establish the Pornography Control Committee and prescribe its functions; and for other related matters.**

DATE OF ASSENT:

*Date of Commencement:* See section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY

**1. Commencement.**
This Act shall come into force on a date appointed by the Minister by statutory instrument.

**2. Interpretation.**
In this Act, unless the context otherwise requires—

"authorised person" means a member of the Pornography Control Committee or a police officer;

"broadcast" means to put out information or make information available to the public or a person through any electronic medium;

"child" means a person below the age of eighteen years;

"Committee" means the Pornography Control Committee established by section 3;

"currency point" has the value assigned to it in Schedule 1;

"internet-content-developer" means a person, individual or corporate, who produces and uploads or causes to be uploaded on the internet, any matter;

"Internet Service Provider (ISP)" means a person with primary access to the internet, who extends internet access to other secondary users;

"Minister" means the Minister responsible for ethics;

"pornography" means any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or stimulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual excitement;

"procure" means to purchase or obtain or import or being found in possession or custody of, or being found viewing in a premise, any matter prohibited by this Act, except when authorised in writing by the Committee for appropriate anti-pornography purposes such as education and sensitisation by personnel approved by the Committee;

"publish" means to put out written information or make available written information to the public or any person through any print medium;

"traffic" means to deal in or cause or permit or aid the provision or circulation of pornographic matter by way of trade or publishing or entertainment or programming or unrestricted internet access or any other means or purpose.

PART II—PORNOGRAPHY CONTROL COMMITTEE

**3. Pornography Control Committee.**

(1) There is established a Committee to be known as the Pornography Control Committee.

(2) The Committee shall consist of nine members as follows—

(a) a chairperson;

(b) a distinguished practicing advocate, nominated by the Uganda Law Society;

(c) five representatives of whom—

(i) one shall represent media houses;
(ii) one shall represent publishing houses;
(iii) one shall represent the arts and entertainment industry;
(iv) one shall represent the education professionals; and
(v) one shall represent the health professionals.

(d) two other members of whom—
(i) one shall represent cultural leaders; and

(ii) one shall represent religious leaders.

(3) The members of the Committee shall be appointed by the Minister with the approval of Cabinet.

**4. Qualifications of Committee members.**

A member of the Committee shall be a person—

(a) of sound mind;

(b) with high moral character and proven integrity; and

(c) with qualifications or minimum of not less than ten years' experience in law, theology, information communication and technology, journalism, psychiatry or counseling.

**5. Tenure of office of members of Committee.**
A member of the Committee shall hold office for five years and is eligible for reappointment for one more term.

**6. Disqualification and removal of a member of Committee.**
(1) A member of the Committee may be removed from office by the Minister on any of the following grounds—

(a) inability to perform the functions of his or her office arising out of physical or mental incapacity;

(b) misconduct or misbehaviour;

(c) incompetence; or

(d) if convicted of an offence involving moral turpitude.

(2) A member of the Committee may resign his or her office by notice in writing addressed to the Minister, and the resignation shall take effect from the date on which the Minister receives the notice.

**7. Functions of Committee.**
(1) The functions of the Committee are—

(a) to take all necessary measures to ensure the early detection and prohibition of pornography;

(b) to ensure that the perpetrators of pornography are apprehended and prosecuted;

(c) to collect and destroy pornographic objects or materials with the assistance of the police;

(d) to educate and sensitise the public about pornography;

(e) to promote the rehabilitation of individuals, groups, families or communities affected by pornography;

(f) to expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography;

(d) performing any other function that may be assigned to him or her by the Committee.

PART III—PROHIBITION OF PORNOGRAPHY

**13. Prohibition of pornography.**

(1) A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography.

(2) A person who produces or participates in the production of, or traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography contrary to subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding ten years or both.

**14. Child pornography.**

(1) A person who produces, participates in the production of, traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography depicting images of children, commits an offence and is liable on conviction to a fine not exceeding seven hundred and fifty currency points or imprisonment not exceeding fifteen years or both.

(2) For the avoidance of doubt, the definition of pornography in section 2 applies in determining the commission of the offence of child pornography.

**15. Court to issue warrant.**

(1) Where information is brought to the attention of the court that there exists in premises, an object or material containing pornography or an act or event of a pornographic nature, the court shall issue a warrant for the seizure of the object or material and for the arrest of the person promoting the material or object.

(2) An authorised person in possession of a search warrant issued by the court may enter any premises and inspect any object or material including any computer, and seize the object, material or gadget for the purpose of giving effect to this Act.

(3) A person who obstructs an authorised person in the carrying out of any function under this section commits an offence and is liable, on conviction, to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding five years or both.

**16. Authorities to issue directives to offenders.**

(1) The Committee, the court or a police officer not below the rank of superintendent of police, may, in writing, direct any newspaper, publisher, broadcaster, proprietor of any business dealing in computers, telephones or other medium for transmitting electronic information or the proprietor of any place or business dealing in leisure or entertainment, bookshop owner, dealer in photography, newsprint or magazine dealer or vendor, importer or exporter or other person, to desist from dealing in pornography.

(2) A person who fails to comply with a directive issued under subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding five years or both.

**17. Internet Service Providers (ISP).**

(1) An Internet Service Provider (ISP) who, by not using or enforcing the means or procedure recommended by the Committee to control pornography, permits to be uploaded or downloaded through its service, any content of a pornographic nature, commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding five years or both.

(2) Where a publisher or broadcaster or internet-content-developer or dealer in telephone-related business or Internet Service Provider (ISP) commits an offence under subsection (1), the court convicting that person may, for a subsequent offence, by order, suspend the business.

(3) A person who fails to comply with an order given under subsection (2) commits an offence and is liable on conviction to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding five years or both.

**18. Leisure or entertainment.**

(1) Where a proprietor of a place of leisure or entertainment or of a business dealing in leisure or entertainment commits a second or subsequent offence under this Act, the court convicting the offender for the second or subsequent offence may issue an order suspending or prohibiting the offender from dealing in leisure or entertainment.

(2) A person who fails to comply with an order issued under subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding five years or both.

**19. Offences by body corporate.**

Where an offence under this Act is committed by a body corporate—

(a) that body corporate, is liable to a fine not exceeding double the fine prescribed in relation to the offence for an individual who commits the offence; and

(b) a director or secretary of the body corporate or a partner in the firm who is proved to have contributed to the commission of the offence shall be taken also to have committed the offence and is liable to the penalty prescribed for an individual who commits the offence.

**20. Forfeiture and destruction of pornography.**

Where a person is convicted of an offence under this Act, the court shall order the forfeiture to the state and the destruction of all materials and objects used in the commission of the offence.

PART IV—FINANCES

**21. Funds of Committee.**

(1) The funds of the Committee shall consist of monies approved by Parliament and other monies donated for the performance of the functions of the Committee.

(2) The finances of the Committee shall be budgeted for under the budget estimates of the Ministry responsible for ethics.

**22. Annual Report.**

The Committee shall make an annual report to the Minister on the performance of its functions within six months after the end of each financial year.

**23. Minister to lay Annual Report before Parliament.**

The Minister shall as soon as possible lay before Parliament the annual report of the Committee on its functions submitted to him or her under section 22 with any comments on it as he or she may consider necessary.

PART V—MISCELLANEOUS

**24. Register of Pornography Offenders.**

(1) The Committee shall maintain a Register of Pornography Offenders containing the name of every person convicted of an offence under this Act in the form set out in Schedule 3.

(2) The register shall include storage of files with supporting records and documents used in the prosecution that secured the conviction of the offender.

**25. Archives.**

The Committee shall maintain an archive of all relevant administrative records and other documents associated with the carrying out of its functions.

**26. Power of Minister to amend Schedules.**
The Minister may, by statutory instrument, with the approval of the Cabinet amend Schedules 1 and 2.

**27. Regulations.**
(1) The Minister may, by statutory instrument, make regulations—

(a) relating to the establishment of programmes aimed at educating and sensitising the public about pornography and its consequences;

(b) to provide for the rehabilitation of persons affected by pornography;

(c) to provide for the eradication of pornography;

(d) to provide for a multi-sectoral approach against pornography involving Government departments, agencies, institutions and civil society organisations to develop anti-pornographic strategies; and

(e) to provide for the better carrying into effect, the purposes of this Act.

(2) Regulations made under this section may provide—

(a) in respect of a contravention of the regulations, a penalty not exceeding two thousand currency points or imprisonment not exceeding five years or both; and

(b) that the court convicting a person under the regulations may order the forfeiture or destruction of any object or material used in the commission of the offence or connected with the offence.

**28. Repeal of section 166 of the Penal Code Act, Cap. 120.**
Section 166 of the Penal Code Act, Cap.120, relating to traffic in obscene publications is repealed.

**SCHEDULES**

SCHEDULE 1

*Sections 2, 26*

CURRENCY POINT

A currency point is equivalent to twenty thousand shillings.

SCHEDULE 2

*Section 8 and 26*

MEETINGS OF THE COMMITTEE AND OTHER MATTERS

**1. Meetings of the Committee.**

(1) The Committee shall meet for the discharge of business at least four times in each year or upon a request in writing to the Chairperson by at least three members of the Committee.

(2) The Committee shall meet at such time and place as the Chairperson may appoint.

(3) The Chairperson may also call a special meeting of the Committee.

(4) The Chairperson of the Committee may convene an emergency meeting whenever he or she considers it necessary.

(5) A meeting of the Committee shall be convened by a two weeks notice in writing except that a shorter notice may be given for a special meeting.

(6) The Chairperson shall preside at all meetings of the Committee and in his or her absence, a member elected by the members present shall preside.

**2. Quorum.**

The quorum at a meeting of the Committee shall be one-third of the voting members of the Committee for the transaction of ordinary business and all members for the review of a previous decision of Committee.

**3. Minutes of meetings of the Committee.**

(1) The Secretary shall cause to be recorded and kept, minutes of all meetings of the Committee in a form approved by the Committee.

(2) The minutes recorded under paragraph (1) shall be submitted to the Committee for confirmation at its next meeting and when confirmed, shall be signed by the Chairperson and the Secretary in the presence of the members present at the latter meeting.

**4. Decision of the Committee.**

(1) The decisions of the Committee shall be by consensus.

(2) A decision of the Committee shall be agreed upon at the meeting of the Committee.

(3) A member of the council shall have one vote; and where there is an equality of votes, the chairperson or person presiding at the meeting shall have a casting vote.

**5. Validity of meetings not affected by vacancy.**

The validity of any proceedings of the Committee shall not be affected by any vacancy among its members or by any defect in the appointment of any of them.

**6. Disclosure.**

(1) Where a person is present at a meeting of the Committee at which a matter is the subject of consideration in which that person or his or her spouse or nominee is interested in a private capacity, he or she shall, as soon as practicable after the commencement of the meeting, disclose that interest and shall not, unless the Committee directs otherwise, take part in any consideration or discussion or vote on any question relating to the matter.

(2) A disclosure of interest made under this paragraph shall be recorded in the minutes of the meeting at which it is made.

**7. Service of documents and other notices.**

A notice or other document may be served on the Committee by delivery to the office of the Executive Secretary.

**9. Committee may regulate procedure.**

Except as otherwise provided under this Act, the Committee may regulate its own procedure.

*Section 24*

**SCHEDULE 3**

**REGISTER OF PORNOGRAPHY OFFENDERS**

*(To be filled after the case, including all appeals concluded in court.)*

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Serial No. | Case Number | Name of convict (Individual or Organization) | Age of convict | Gender of convict | Convict's physical address (Street, village, town, parish, sub-county, district) | Convict's postal address and telephone number | Particulars of the charge which the offender was convicted of (as appear on the charge sheet) | Full name of the court that convicted the offender | Particulars of the sentence | Date of conviction | Date of entry in Register |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

**Act** *Anti-Pornography Act* **2014**

**Cross References**
Penal Code Act, Cap.120.