CYBER LAWS OF UGANDA

How Laws and Regulations affect Online Activities in Uganda

JANUARY 2019

barefootlaw

CYBER LAWS OF UGANDA

How Laws and Regulations Affect Online Activities in Uganda

January 2019

barefootlaw

In partnership with

digital HUMAN RIGHTS lab

future challenges

betterplace LAB

With support from

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

1 'Author' Tjabbe Bos holds master's degrees in Information Management (MSc) and in Public International Law (LLM). Previously he worked with the Ministry of the Interior of the Netherlands on national policies and regulation on e-government (2007-2011) and on digital identities and data protection in the public sector (2011-2013) and with the European Commission on European Union policies and regulation on cloud computing and data flows (2013-2015) and the fight against cybercrime (from 2015). This article was written in his personal capacity while he was on long-term leave from his position at the European Commission from October 2017 to March 2018).

2 BarefootLaw is a not-for-profit organisation with the aim to improve access to justice in Uganda by providing free access to legal information by using innovative technology. BarefootLaw is based in Kampala, Uganda and has the aim to reach 50 million people across Africa by 2030. In 2017, BarefootLaw won the prestigious King Baudouin African Development Prize for their contribution to development in Africa.

3 The information in this report presents the situation by March 2018.

Acknowledgment

BarefootLaw would like to appreciate those who worked all so tirelessly in the preparation of the Cyber Laws in Uganda Report. Special thanks to our partners the Digital Human Rights Lab, betterplace Lab, Future Challenges and The Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ) for supporting the launch of this report.

Thank you to these entities for making time to share information with us through interviews; the Ministry of ICT and National Guidance, the secretariat of the Justice, Law and Order Sector, the National Information Authority Uganda (NITA-U) the United Nations Capital Development Fund (UNCDF) and Masikini. Our appreciation to Kampala International University (KIU), Makerere University Business School (MUBS) and Kafeero Foundation for accepting to take part of our surveys.

We are indebted to the individuals who voluntarily worked towards compiling this report. Tjabbe Bos for heading and compiling this research process; Hillary Rubangapewany; Robert Okello and Winnie Acio for assisting in the research; Mr. Kenneth Muhangi for peer reviewing the paper. The staff of BarefootLaw for their continuous support.

Foreword

> The world today is firmly within the epoch of the information and communications technology age. For the last 30 years, information technology has been at the centre of the world and human experience. It has facilitated how we interact with each other, how we thrive and how we experience life. In particular, information technology has facilitated a digital economy that is now central to the world economy.

The ubiquity of the digital information age has necessitated governance mechanisms for the control, protection and sharing of cyberspace. Across the world different standards and conventions support regions, countries and sections of the digital economy. Some parts of the world are ahead of the curve in experiencing the information age and, as a result, have more evolved supporting frameworks, whereas some have evolved faster digital economies than the supporting frameworks can handle.

In Uganda's case, the information technology space has grown rapidly, be it the digital economy and its facilitating tools, such as mobile money, or the information and communication space, where people freely interact and share experiences, such as through social media. For a fast-growing cyberspace, the supporting legal framework needs to be dynamic enough to foster the growth while robust enough to protect all parties involved in it. As an innovator within Uganda's digital space, we are acquainted with the extent of legal framework and how it impacts our work.

This project reportably describes the structure in which the legal framework supporting the cyberspace for Uganda exists, highlighting the areas governed by cyber laws, where their strengths are, as well as the gaps that ought to be thinned or closed out completely.

Based on his experience with policy and legislation for the digital economy, Tjabbe Bos presents a compelling view of the current legal framework supporting Uganda's cyberspace and makes carefully thought-out arguments on what the next steps ought to be to make the information technology ecosystem stronger yet fairer and more supportive of all stakeholders in it. Tjabbe has vast experience at a policy development and review level at the European Union, having worked there in various capacities over the last five years. With this wealth of knowledge and experience and its immersion directly in Uganda through his project in partnership with BarefootLaw, this project report, I feel, provides a practical and grounded view of the cyber laws of Uganda.

This project report is important reading for everyone involved at a policy level and in the governance of the information technology space, as well as operators, practitioners and innovators seeking to utilise cyberspace for their own and their communities' advancement.

Gerald Abila
Executive Director, BarefootLaw

Table of Contents

Abbreviations and Acronyms 5

1. Introduction 6

2. The Functioning of the Framework of Cyber Laws 7

3. Methodology of the Cyber Laws Project 8

3.1. Selection of scenarios 8

3.2. Mapping of the regulatory framework 8

3.3. Consultative activities 9

4. Results of the Cyber Law Scenarios 10

4.1. Mobile money systems 10

4.2. Electronic commerce transactions 13

4.3. Cybercrime 18

4.4. Access to government information 22

4.5. Electronic government services 25

5. Relevant Findings 29

5.1. Ease of doing business online 29

5.2. Citizen's rights and consumer protection 29

5.3. Conducive to new technology 29

5.4. International aspects 30

5.5. Enforcement actions 30

5.6. Awareness and access to information 30

5.7. An original approach that meets the needs of Uganda 30

5.8. Legislative technique 31

6. Recommendations 32

7. Annexes – The Framework of Cyber Laws 34

7.1. The legal framework for mobile money schemes in Uganda 34

7.2. The legal framework for e-commerce transactions in Uganda 40

7.3. The legal framework for the fight against cybercrime in Uganda 53

7.4. The legal framework for access to government information in Uganda 64

7.5. The legal framework for electronic government services in Uganda 69

Abbreviations and Acronyms

AYK	Ask Your Government (a Uganda Government website created to facilitate questions from citizens about the government).
E-COMMERCE	Electronic Commerce
E-GOVERNMENT	Electronic Government
ICCPR	International Covenant on Civil and Political Rights
IT	Information Technology
ITU	International Telecommunications Union
NITA-U	National Information Technology Authority, Uganda
UGX	Uganda Shillings (Uganda's national currency)
UNCITRAL	United Nations Commission on International Trade Law
US	United States

1. Introduction

> Since 2016, the number of internet users in Uganda has grown continuously to more than **15 million**

Ugandans are increasingly benefitting from the use of information and communications technology (ICT) in society. Over the past decade, the use of mobile phones has become widespread, with more than 22 million subscriptions in 2016, and the number of internet users in Uganda has grown continuously to more than 15 million in 2016.[4]

The digital economy is also on the rise as small and medium enterprises (SMEs) in Uganda are creating innovative digital solutions that meet increasing demand in society. Government organisations are also using ICT more often[5], which allows citizens and businesses to benefit from improved delivery of government services.

Continued economic growth is projected for Uganda for the coming years[6], which is supported by Uganda's young and expanding population.[7] Further and sustainable growth could be supported by the further use of ICT[8], but Uganda would have to face a number of challenges, including the need for a functioning technical infrastructure and the availability of a workforce with the right digital skills. In addition, an appropriate legal framework that is conducive to these developments will also be an important requirement for continuous growth.

Over the recent years, the Government of Uganda has adopted a framework of laws and regulations that governs online activities of online consumers, businesses and government organisations. The framework covers, amongst other things, electronic commerce transactions, mobile money transactions and malicious activities like cybercrime.[9]

4 According to the Uganda Communications Commission (UCC), in 2016 there were 22 million mobile phone subscriptions. The UCC also reported that in 2016 there were 15,5 million internet users in Uganda. See yearly reporting of the UCC on www.ucc.co.ug

5 United Nations E-Government Survey 2016, which ranked Uganda in position 128 in the e-government development index (EGDI), available at https://publicadministration.un.org

6 World Bank Uganda Economic Update Fact Sheet of 8 February 2017, available at www.worldbank.org

7 According to the 2017 World Population Prospects report of the United Nations, the total population of Uganda was about 41 million in 2016, growing by about 1 million per year. In 2015, about 48 per cent of the population consisted of children below the age of 15, available at www.esa.un.org

8 See brief summary E. Kvochko, "Five ways technology can help the economy", April 2013 and available at www.weforum.org or, more comprehensively: Central Bureau of Statistics of The Netherlands, "ICT and Economic Growth", 2015, available at www.cbs.nl

9 Including, for example, the 2011 Electronic Transactions Act and the 2011 Computer Misuse Act

2. The Functioning of the Framework of Cyber Laws

> Only recently the government has started the collection and publication of information about the use of ICT in Uganda

With the adoption of cyber laws and regulations, the Government of Uganda aimed, amongst other things, to facilitate online activities, provide protection for citizens and consumers and offer legal certainty for businesses. Subsequent policies have also been adopted by the government to complement the regulatory framework, e.g. with a national strategy on information security.[10]

Notwithstanding these efforts, it is currently unclear how the framework of cyber laws functions in practice. Only recently the government has started the collection and publication of information about the use of ICT in Uganda.[11] Although the recent activities provide for making useful information available, e.g. about the extent of e-commerce transactions or cybercrime, the functioning of the legal framework is only touched upon briefly. Amongst other things, in response to a nationwide survey carried out in 2016 and 2017, it turned out that only 18.5 per cent of respondents indicated awareness of the existence of cyber laws in Uganda and 73.5 per cent were not able to refer to any specific cyber law correctly.[12] Notwithstanding the outreach activities of the government to sensitise the public to their rights and obligations when operating online, people are not familiar with the framework of cyber laws and do not appear to rely on these rules when operating online.

In that context, the author of this paper developed a project to gain a better understanding of the functioning of the framework of cyber laws in Uganda. In collaboration with BarefootLaw, a project was developed with the aim to support the functioning of the framework of cyber laws in Uganda by gaining a better understanding of how the framework affects citizens and businesses when they conduct activities online. The project was carried out between October 2017 and March 2018. This document is used to report on the results of the project. The results of the report include recommendations to the government and tips and guidance for businesses and citizens.

10 For instance, the February 2014 "National Information Security Policy", available at www.nita.go.ug

11 NITA, "National Information Technology Survey 2017/18 Report", March 2018, available at www.nita.co.ug

12 ibid.

3. Methodology of the Cyber Laws Project

> The cyber laws project was carried out on the basis of a case study methodology that involved a number of activities to obtain information. The activities were undertaken in two phases: first, the project involved the mapping of relevant laws and regulations for a number of common online scenarios; second, following the mapping of the legal framework, consultative activities were carried out to obtain feedback from consumers, businesses and other stakeholders in Uganda.

3.1 Selection of scenarios

As a preliminary step, scenarios about common online activities of citizens, consumers and businesses were selected. It should be noted that the selection of scenarios also determined the scope of the project. In view of the limited availability of time and resources, only five scenarios were selected. The selection took place on the basis of a *prima facie* understanding of the relevance of these scenarios for people and businesses in Uganda and the availability of a certain regulatory framework in those areas. The following scenarios were selected:

1. Mobile money systems – the rights and obligations of entities that are involved in systems that are used for transactions of mobile money in Uganda;
2. Electronic commerce – the rights and obligations of businesses and consumers in Uganda when they are engaging in transactions on the internet;
3. Access to government information – the rights and obligations of citizens and government organisations in Uganda when a request for access to government information is made;
4. Electronic government services – the rights and obligations of citizens and government organisations in Uganda when they want to engage in the delivery or use of electronic government services.
5. Cybercrime – the offences considered as cybercrimes in Uganda, as well as procedural measures that law enforcement authorities in Uganda can use in the fight against cybercrime.

3.2 Mapping of the regulatory framework

Following the selection of the scenarios, relevant legislative acts and regulations were identified by means of desk research. As Uganda has a common law system, judicial decisions were also considered. However, owing to the recent nature of online developments in Uganda, only a limited number of relevant decisions were found. The analysis of laws, regulations and judicial decisions resulted in an overview of rights and obligations of consumers, businesses and government organisations.

These rights and obligations were also compared with international laws and documents, or the regulatory framework in a specific country. The selection of international documents or the regulatory frameworks of other countries was made on a case-by-case basis. The comparative analysis was carried out on the basis of desk research, with the aim being to gain a better understanding of the nature of the framework of cyber laws in Uganda, as it is often based on international best-practices.

3.3 Consultative activities

The second phase of the project involved activities with the aim being to have a better understanding of the actual application and use of the framework of cyber laws. For that purpose, short articles were published on BarefootLaw's Facebook page. In addition, more targeted consultative activities were carried out. These included interviews with relevant stakeholders, a small-scale survey on cybercrime[13], as well as a presentation and a workshop.

Interviews took place with representatives of government organisations, which included the Ministry of ICT and National Guidance, the secretariat of the Justice, Law and Order Sector, the National Information Technology Authority Uganda (NITA-U) and the United Nations Capital Development Fund (UNCDF). In addition, representatives from Masikini – a major e-commerce provider in Uganda and smaller businesses operating or planning to operate online – were interviewed.

Surveys were conducted amongst students of Kampala International University (KIU) and Makerere University Business School (MUBS) and smaller businesses that are operating online. A workshop with start-up businesses that are operating or are planning to operate online was organised in collaboration with Kafeero Foundation.[14] A presentation was organised as part of the 2018 NSSF Career Expo at Makerere University Business School.[15]

13 Joel Rubangapewany, Tjabbe Bos, Robert Okello, Opiyo Denis Olweny, "A survey on cybercrime in Uganda", July 2018, available on www.bareftoolaw.org.

14 See the website at http://www.kafeero.org/

15 See the website at http://www.mubs.ac.ug/

4. Results of the Cyber Law Scenarios

> The day-to-day mobile money transactions in Uganda involve contact between a mobile money user and a mobile money service provider through its agent.

4.1 Mobile money systems

Every day millions of people in Africa, especially in East Africa, use mobile money systems for their financial transactions. In Uganda, the first scheme for mobile money transactions was introduced in 2009 and currently seven schemes are active. In 2015 more than 21 million registered users made 693 million transactions with a value of more than UGX 32 billion .[16]

The introduction of mobile money schemes has greatly supported financial inclusion in countries like Uganda.[17] More and more financial services are offered through mobile money systems, ranging from mere transactions between accounts or cash-in and cash-out transactions, to loans. More significantly, mobile money schemes also allow their users to conduct electronic transactions.

The day-to-day mobile money transactions in Uganda involve contact between a mobile money user and a mobile money service provider through its agent. However, other entities such as the supervisory authority – the Bank of Uganda – and financial institutions licensed by the Bank of Uganda (e.g. Stanbic Bank or Centenary Bank) have important roles to play in the mobile money system.

4.1.1 The development of the mobile money scenario

As part of the first phase of the cyber laws project, the legal framework for mobile money systems was mapped based on desk research.

In the second phase of the project, an article on the summary of rights and obligations in relation to mobile money systems was published online. The article was published in three parts in January 2018, on BarefootLaw's Facebook page.[18] In addition, mobile money transactions were discussed as part of other consultative activities, which included interviews and workshops.

4.1.2 Summary of legal framework

Mobile money schemes in Uganda are currently not governed by any formal legal framework.

16 Presentation on Mobile Money in Uganda by Mr James Ssettimba of the Bank of Uganda of 14-16 March 2016, available online at: https://www.theigc.org/

17 See, for example: George Wilson Ssonko, "The role of mobile money services in enhancing financial inclusion in Uganda", available at https://www.bou.or.ug

18 https://www.facebook.com/Barefootlaw/

Nevertheless, Uganda has a legal framework that governs the financial system and regulates financial services. The current legal framework in Uganda established, amongst other things, the Bank of Uganda as financial regulator (the 1993 Bank of Uganda Act). In addition, the 2004 Financial Institutions Act governs certain aspects in relation to financial institutions, including their licensing and supervision. Recently, the 2004 Financial Institutions Act was amended to provide for agency banking, which allows banks to offer financial services through agents.

Beyond the formal legal system, other regulatory interventions have also taken place. Amongst other things, the Central Bank of Uganda has published guidelines. Although their legal nature is not clearly specified, they are probably to be considered as a measure of soft law. Amongst other things, the Central Bank of Uganda published Guidelines on consumer protection regarding financial services in 2011 and guidelines for mobile money schemes in 2013. In the 2013 Guidelines, it is recognised that they are an interim measure to enable the operation of mobile money services.

The soft-law approach taken in Uganda is not unlike approaches taken in other African countries, although some countries, including Kenya, have since then enacted formal legislation.[19] No relevant legal documents on mobile money systems at international level were consulted.

4.1.2.1 Roles and responsibilities of mobile money entities

The 2013 Mobile Money Guidelines assign roles and responsibilities to the different entities involved in mobile money schemes. Under the Guidelines, the financial services provided through mobile systems are deemed to be provided by financial institutions licensed by the Bank of Uganda, in partnership with mobile money service providers. Accordingly, the licensed financial institutions, rather than the providers of mobile money services, are considered responsible for the mobile money services from a financial perspective.

According to the Guidelines, mobile money service providers are chiefly considered responsible for operating mobile money platforms that are used for carrying out mobile money transactions.

The Guidelines determine that a mobile network operator is responsible for the mobile money platform, which is operated based on an infrastructure which includes the existence of a mobile network. Although defined as different entities in the Guidelines, mobile money service providers and mobile network operators in Uganda are in many cases the same organisation (e.g. Airtel, Africell, MTN).

The Guidelines also determine that mobile money service providers are responsible for putting in place agreements with licensed financial institutions, mobile money agents and customers respectively. These agreements, although of a private contractual nature, are also governed by the Guidelines.

Regarding agents, the Guidelines indicate, amongst other things, that they can only deliver a certain number of services, which are limited to opening accounts for new customers, receiving or paying cash and attending to customer queries and complaints. The Guidelines determine that agents cannot perform any other mobile money functions and are not allowed to charge any fees directly to customers.

The Guidelines provide that customers are responsible for their transactions in that they need to preserve the confidentiality of their Personal Identification Numbers (PIN).

4.1.2.2 Competition and consumer rights

To foster competition amongst mobile money schemes, the Mobile Money Guidelines indicate that agreements between a mobile money service provider, a licensed institution and a mobile money agent cannot be exclusive. The Guidelines also indicate that mobile money platforms should be capable of becoming technologically interoperable with other mobile money schemes, to allow for mobile money transactions between schemes and between countries.

The Guidelines provide for strict rules to protect consumers when they are using mobile money schemes. They also provide for rules themselves, but

19 See the 2011 Payment Service Act and the 2014 National Payment System Regulations of Kenya

also determine that the 2011 Bank of Uganda Financial Consumer Protection Guidelines apply to mobile money transactions. Amongst other things, the Guidelines determine that mobile money service providers are obliged to provide secure transactions, transparent terms of service to protect their customers' privacy and to provide for appropriate and effective procedures to handle complaints.

4.1.3 Observations

While the adoption of the 2013 Mobile Money Guidelines by the Bank of Uganda has been an important step for the functioning of mobile money schemes and the uptake of mobile money services by the public in Uganda, the results of the cyber laws project have nonetheless allowed for the identification of several issues from a legal perspective. While assessing the regulatory framework for mobile money schemes, it should especially be acknowledged that the use of mobile money in Uganda has grown significantly over the past few years. Whereas the mobile money system may have been considered as developing in 2013, there can be no doubt that the system has grown more mature over the past few years. Every day significant amounts of transactions for significant amounts of money are made, which challenges the way financial transaction systems are currently regulated.

First, the soft-law approach of the 2013 Mobile Money Guidelines may increasingly pose a number of challenges to the mobile money system in Uganda. Considering the nature of soft law, the Bank of Uganda may find it increasingly difficult to operate as financial regulator of mobile money systems. As a result, mobile money players may be inclined to take more risks in view of the lack of oversight. This may especially present problems in view of the 2016 amendment of the Financial Institutions Act, which provides for agency banking. As a result of these amendments, it can be expected that new players will enter the mobile money market and that market innovation will take place. This may be increasingly difficult to control from a regulator's perspective.

Second, the development of the mobile money market in Uganda has allowed for a small number of mobile money service providers to take a significant market share. Although the Guidelines determine that agreements with other mobile money entities (e.g. agents and financial service providers) cannot be exclusive and that providers should make provision for interoperable services, a small number of service providers appear to have taken a dominant position. Their combined role as service provider and network operator appears to have exacerbated this development. Although the introduction of agency banking with the 2016 amendment of the Financial Institutions Act may enable entirely new players to enter the market for mobile money services, it also appears that small and innovative businesses will find it increasingly difficult to operate in this market.

Thirdly, the elements highlighted above affect how businesses and customers perceive mobile money systems in Uganda. Consumers and businesses usually equate mobile money service providers with mobile network operators – which are perceived as large corporations that can act as they wish. As mobile money merchants (businesses that accept mobile money payments from their customers) are not recognised as mobile money players in the Guidelines, they do not receive any protection against dominant mobile money service providers. Mobile money agents and customers are usually unaware of their rights and obligations under the Guidelines. Where they are disadvantaged by the practices of mobile money service providers, such as a decrease in rates for mobile money agents or an increase in rates for mobile money customers, they are left feeling helpless and unable to pursue or resolve these issues.

4.1.4 Recommendations for the government

On the basis of these observations, the following recommendations are addressed to the Government of Uganda:

First, the time appears ripe for the introduction of a formal legal framework to govern mobile money systems. A particular challenge for regulatory changes will be to provide for strict conditions for established players, while the framework should allow for new mobile money service providers to enter the market.

In addition, it should determine the rights and obligations of relevant mobile money entities and provide for clear and realistic measures for their enforcement.

The framework should also be used to address the role of mobile money merchants (businesses that allow for consumers to make transactions with mobile money) and establish oversight regarding mobile money services and reduce transaction costs for mobile money users. The reduction in costs would allow for the growth of mobile money systems across the country, which would likely benefit economic growth in general and the growth of digital economy more specifically.

Second, the government should provide for the rights and obligations of the mobile money merchants in the current and any future regulatory framework. Interventions of the competent regulator(s) should take place in a transparent way, allowing the public to take note of the position and actions of the regulator.

Finally, the government should raise awareness with mobile money players, particularly with consumers and businesses, about their rights and obligations under the regulatory framework.

4.1.5 Guidance for businesses and consumers

Businesses that are making use of mobile money systems in their role as mobile money merchants are advised to take note of their obligations under the regulatory framework. Although mobile money agents are currently not governed by the 2013 Guidelines, they often have obligations under the terms and conditions provided by the mobile money service providers that they are working with. Businesses are advised to consider these terms and conditions and compare them with the terms and conditions of other mobile money service providers. Where relevant, they may also consider making use of mobile money intermediates to allow for mobile money payment services.

Particular attention should be taken by businesses that are operating as mobile money agents. Notable obligations for mobile money agents are the limited number of services they can provide, as well as rates that are set by mobile money service providers. Although mobile money agents are indispensable players in the system, they are also vulnerable players in comparison with the few dominant mobile money service providers in the Ugandan market. Mobile money agents should consider forming an association to ensure better consideration of their interests.

Consumers are also advised to take note of their rights as provided for under the regulatory framework. The 2011 and 2013 Guidelines provide for a high level of protection, which they should not hesitate to invoke in relation to mobile money services. Where relevant, consumers should not hesitate to complain about the performance of mobile money service providers to the Bank of Uganda in its role as financial regulator.

4.2 Electronic commerce transactions

The growth of internet usage has widely opened up new opportunities to conduct electronic transactions. The sale and purchase of goods and services by and to consumers over computer networks, also known as electronic commerce or e-commerce, generally reduces trade costs for businesses and consumers. It also opens up new markets (across borders) and offers more choice for lower prices.

Worldwide, the e-commerce market is dominated by major service providers like Amazon.com, eBay or Alibaba, but e-commerce also presents opportunities for businesses operating at regional or national level. The total value of e-commerce transactions worldwide is estimated to have risen from US $1.3 trillion in 2014 to US $4.5 trillion in 2021.[20] The size of the e-commerce market in Africa was estimated at US $8 billion in 2013[21], but had been projected to grow to US$50 billion by 2018.[22]

Although in 2016 only 1.7 per cent of people in Uganda indicated that they had bought any products

20 Figures are available at www.statista.com

21 ibid.

22 ibid.

or services on the internet[23], Uganda was ranked 86th in the 2017 UNCTAD study on e-commerce readiness[24], one of the highest positions for African countries, just behind Kenya and just above Mexico. Popular e-commerce providers in Uganda are *UGunlocked, US2UG, Jumia* and *Masikini*, which often operate as intermediaries between e-commerce providers in the United States, China or the European Union, on the one hand, and consumers in Uganda, on the other.

4.2.1. The development of the e-commerce scenario

As part of the first phase of the cyber laws project, the legal framework for e-commerce transactions was mapped by desk research.

In the second phase of the project, a summary of rights and obligations in relation to e-commerce transactions was published in an article on the internet. An article was published in two parts on BarefootLaw's Facebook page in January 2018.[25] In addition, the legal implications of e-commerce transactions were discussed as part of other consultative activities, including interviews and workshops.

4.2.2. The legal framework for e-commerce transactions

The sale and purchase of goods and services in Uganda are governed by the laws of contracts, including the 2006 Contracts Act. According to these rules, contracts may be defined as agreements with legal effect where there has been an offer and acceptance of that offer. Contracts create obligations and, where these are not respected, consequences may arise, and thses are not limited to compensation to the innocent party. Contracts can be oral or in written form. The Act recognises that electronic data messages may also be considered as contracts in written form.

Apart from being in electronic form, contracts may also be concluded electronically as e-transactions, e.g. with electronic devices. In order to facilitate these kinds of electronic transactions, the Parliament of Uganda in 2011 enacted the Electronic Transactions Act, which recognises that contracts may be in electronic form and provides rules for their formation. Additional rules were provided in the 2013 Electronic Transactions Regulations and the 2016 Certification of Providers of Information Technology Products and Services Regulations.

At international level, no formal treaties that govern electronic transactions per se exist. Nevertheless, most countries around the world have adopted laws and regulations to govern these matters over the past decades. Some countries have relied on model laws developed at international level, including those provided by the United Nations Commission on International Trade Law (UNCITRAL), which adopted model laws on e-commerce in 1996[26] and on the use of electronic signatures in 2001.[27] At regional level, the European Union also adopted rules that provide certain obligations for businesses operating online, as well as rights for consumers when they engage in e-commerce transactions.[28]

4.2.2.1. The formation of electronic contracts

As buyers and sellers may be in different locations and may send or receive electronic messages through different computer systems with a delay, electronic contracts may easily raise questions on the time and place of their formation. Therefore, the Electronic Transactions Act determines where and when an electronic contract is deemed to be formed: at the time and place where the person who made the offer received the acceptance of the offer.

The Electronic Transactions Act also provides for the formation of automated contracts, where one or both of the parties rely on 'electronic agents' and do not intervene in the formation of the contract in

23 NITA, "National Information Technology Survey 2017/18 Report", March 2018, available at www.nita.co.ug

24 United Nations Conference on Trade and Development, UNCTAD B2C e-Commerce Index 2017, available at www.unctad.org.

25 https://www.facebook.com/Barefootlaw/

26 UNCITRAL Model Law on Electronic Commerce of 1996 and UNICTRAL Model Law on Electronic Signatures of 2001, available at www.uncitral.org

27 ibid.

28 See, for instance, European Union Directive 2011/83/EU on consumer rights, available at www.eurlex.eu

person. Notwithstanding that these contracts may be formed without human intervention, parties are in principle bound by the contract.

Regarding the formation of electronic contracts, and especially where electronic agents are involved in the formation of the contract, it may be difficult to determine the person with whom a contract has been concluded. Therefore, the Electronic Transactions Act also explains basis on which an offer or acceptance may be attributed to a person. The Act indicates a preference for the use of electronic signatures based on the 2011 Electronic Signatures Act, as they provide for reliable ways to identify persons.

4.2.2.2 Obligations for businesses

In view of the specific nature of electronic commerce transactions, a number of specific obligations for businesses that want to operate in the e-commerce market were introduced. When offering goods or services online, the Electronic Transactions Regulations obliges sellers to provide detailed information regarding their identity, location, as well as contact details. Failing to provide this information is considered a criminal offence.

In addition, businesses that want to provide information technology products or services are required to obtain certification from the competent regulator, the National Information Technology Authority Uganda (NITA-U). Detailed procedures for obtaining certification, including considerable fees for applying for certification, are provided by the 2016 Certification of Providers of Information Technology Products and Services Regulations. Providing information technology products or services without certification is considered a criminal offence.

4.2.2.3 Consumer protection

As buyers and sellers may not be in the same location when conducting an electronic transaction, consumers may be left in a vulnerable position, e.g. as it may be difficult for a consumer to assess the quality of a product or to obtain after-sales services. Therefore, the Electronic Transactions Act provides for additional protection for consumers. The provisions on consumer protection are mandatory and any agreement that aims to limit them should be considered as void.

When offering goods or services online to consumers, sellers are required to provide detailed information regarding the product or service and their identity and contact details. Sellers are also required to allow consumers to check and correct their order and withdraw from the transaction before placing the order. Where these requirements are not respected, consumers can cancel the transaction within 14 days. Following a cancellation, a consumer is obliged to return the goods or to stop using the service, and a seller is obliged to reimburse the consumer. Consumers may also complain with the competent regulator, NITA-U, where a service provider does not comply with these obligations.

A consumer is also entitled to cancel a transaction after the receipt of the goods or the services within seven days, without the need to state any reason. In case of a cancellation, a consumer can only be charged for the direct costs of the return of the goods. The seller is held to reimburse the consumer within 30 days when a payment has already been made.

Finally, sellers are required to deliver goods within 30 days following an order. Where a delivery cannot be made within 30 days, a consumer is entitled to cancel the transaction.

4.2.2.4 Territorial application

The Electronic Transactions Act indicates that it applies to any person, irrespective of the person's nationality or citizenship, or whether the person is inside or outside Uganda.

4.2.3 Observations

Although the legal framework that governs e-commerce transactions in Uganda can be regarded as quite advanced in terms of the rights and obligations it provides for businesses and consumers, the results of the cyber laws project have also allowed for the identification of a number of issues from a legal perspective in this area.

First, it may be questioned whether the legal framework for e-commerce transactions appropriately takes into account the particular circumstances of the Ugandan e-commerce market. It appears the legislative framework was mostly developed with international model laws in mind, including those provided by UNCITRAL, without appropriate considerations for the particular challenges of the Ugandan e-commerce market. Indeed, at the time of enactment of the 2011 Electronic Transactions Act, not even 4 per cent of internet users had ever bought a product or service online.

This apparent disconnect between the legal framework and the actual e-commerce market can, for instance, be seen in relation to the obligations it places on businesses that want to operate online. Although the publication of information for the benefit of clients and consumers appears reasonable, the requirement of certification for providers appears disproportionate in a country where a majority of businesses are not even formally registered as such. Even though these obligations are currently not enforced, their mere existence already creates a chilling effect on the e-commerce market. It does not seem likely that many businesses would be able to live up to these obligations, including the rather high fees that are required for certification. The obligation to certify is also likely to favour large foreign companies to enter and gain a significant share of the market in Uganda, rather than providing new opportunities for small and innovative local start-ups. Overall, these obligations can be expected to hold back the development of the e-commerce market in Uganda.

In the same vein, consumer protection rules also appear rather disproportionate. Although the protection of consumers of online transactions can be deemed important in building trust, which leads to the development of the e-commerce market, it also places obligations on providers of e-commerce services. On the one hand, the question can be raised as to whether consumers in Uganda really expect a level of protection as high as is currently provided – also in view of the protection they have when engaged in normal (offline) transactions. On the other hand, businesses will also find it difficult to provide the level of protection when it is invoked by the consumer. Indeed, where most products bought online in Uganda have their origin in other continents, notably in the United States, the European Union or China, and where reliable mail services are largely absent, obligations to deliver within 30 days or to provide for a cancellation of a transaction within seven or 14 days are difficult to implement for a business.

In addition, the legal framework for e-commerce transactions in Uganda does not seem to fully acknowledge the cross-border aspect of e-commerce transactions. Although the Electronic Transactions Act includes a jurisdictional provision that defines a rather wide scope, it is unclear to what extent it also applies to foreign service providers that are delivering products or services in Uganda, or Ugandan providers that want to deliver products or services in another country. Although the latter category of providers is in its infancy, many service providers that are currently active in Uganda actually appear to follow foreign rules based on the country from which they import their products, e.g. the United States. The lack of clarity may lead to conflicts of law and subsequent legal disputes, with detrimental effects on consumer trust and market development.

Finally, it also appears that only few businesses and consumers are currently aware of their rights and obligations when providing or when buying products or services online. In a market where even established players are not aware of their obligations, it cannot be expected that consumers are aware of the protection they are granted under the law, or that they are able to effectively invoke those rights. Notwithstanding the availability of a market regulator, NITA-U, and the possibility to file complaints about the conduct of service providers, it is unlikely that consumers will be able to pursue their interests.

4.2.4 Recommendations for the government

On the basis of these observations, the following recommendations are addressed to the Government of Uganda.

First, the Government of Uganda may consider revising the legal framework to better take into account the specific circumstances of the e-commerce market in Uganda. This would require better understanding of the e-commerce market in Uganda, for which close cooperation between the competent regulator, NITA-U, e-commerce providers and consumers would be indispensable. Better interactions on the basis of open consultations should take place.

Notably, when considering revising the legal framework, the Government of Uganda could consider changing obligations for providers of information technology products or services to certify. An alternative mechanisms that could be considered is the introduction of a threshold in terms of size or time of incorporation, to avoid disproportionate obligations on small businesses and innovative start-ups in the e-commerce market. In view of the nascent development of the e-commerce market in Uganda, the flexibility for businesses to enter and operate in the market currently appears more important than maintaining strong controls. Although consumer protection rules provide for trust in the e-commerce market, existing provisions should also be evaluated on the basis of the particular characteristics of the e-commerce market in Uganda.

In addition, the government could consider facilitating cross-border transactions better. In view of the general movement towards more economic integration with East African countries in the East African Community, the Government of Uganda may want to consider pursuing this in particular for e-commerce transactions. A compatible framework with other East African countries could support economic growth in general and e-commerce transactions in particular. On a related note, the competent regulator, NITA-U, could provide more clarity as regards applicable law when businesses and consumers are engaged in cross-border transactions. Guidelines in this area would provide legal certainty and could result in further development of the e-commerce market.

A more active role of the regulator, in relation to the enforcement of rights and obligations on the basis of the current regulatory framework, could also provide for more trust between and awareness of businesses and consumers. More awareness-raising activities in general would also provide businesses and consumers with more information about their rights and obligations and could provide for more trust in the e-commerce market.

4.2.5 Guidance for businesses and consumers

Businesses that want to provide products and services online are advised to be aware of their obligations under the current legal framework. Notably, the requirements to provide sufficient information as well as to be certified are relevant in this regard, as their circumvention could result in regulatory action and even criminal prosecution. Businesses are advised to consider the relevant requirements for certification and, in view of possible certification, to ensure having in place a transparent business model that is supported by documentation. Where necessary, businesses should consider seeking advice on their legal obligations to ensure compliance.

Similarly, it is also recommended that consumers inform themselves about their rights when conducting transactions online. Consumers should compare their consumer rights with the terms and conditions as offered by e-commerce providers and be aware of any discrepancies. In particular, the terms and conditions of providers that are offering products or services on the basis of cross-border transactions, e.g. products bought in the United States and delivered in Uganda, should be scrutinised. Where relevant, consumers should not hesitate to approach the competent regulator, NITA-U, to resolve any issues on the basis of the legal framework in Uganda. Nevertheless, before invoking their rights, consumers should also be mindful of and realistic about the characteristics that the e-commerce market in Uganda has, e.g. in terms of the time it may take to import and deliver products from another country.

4.3. Cybercrime

With the increased use of computers, new types of crimes have also evolved that target the use of computers or involve the use of computers to commit other crimes. Cybercrimes can have a direct impact on people's lives where data is lost, money is stolen, or a person's privacy is infringed upon. The impact of cybercrime can also be seen on a wider scale, for instance where viruses are used to infect computer systems of businesses and critical government systems. In May 2017, more than 230, 000 computers in 150 countries were affected by the Wannacry ransomware attack, including critical government systems, with an economic impact estimated at hundreds of millions of US dollars.[29]

With more and more people using mobile phones, computers and the internet, cybercrime is also posing a growing risk to Ugandans. Although official figures on the extent of cybercrime in Uganda are not available, individual cases where fraud was committed with mobile money are already reported on.[30] As part of a small-scale survey, a majority of university students in Kampala reported having been victims of at least one type of cybercrime.[31] In a limited number of cases, criminals have also been convicted before Ugandan courts for committing more elaborate cybercrimes, as part of which unlawful access to government systems was gained.[32]

29 See the reports on the Wannacry cyberattack of the European Union Network and Information Security Agency (ENISA) on https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

30 See media reports on http://www.monitor.co.ug/Business/Technology/Uganda-at-risk-of-cyber-crime--experts-warn/688612-3348368-if44eq/index.html

31 Joel Rubangapewany, Tjabbe Bos, Robert Okello, Opiyo Denis Olweny, "A survey on cybercrime in Uganda", July 2018, available on www.bareftoolaw.org.

32 See Uganda v Ssentongo & 4 Ors (Criminal Session Case 123 of 2012) [2017] UGHCACD 1 (14 February 2017), available at www.ulii.org

As the reach of the internet extends beyond borders, Ugandans may also fall victim to international groups of cybercriminals. In view of its international nature, and the advanced expertise cybercriminals often have, cybercrime is difficult to fight for law enforcement authorities. Competent authorities need to keep up with technological developments and increasingly need to collaborate with authorities in other counties. Recently, Uganda has expressed an intent to work more closely together with other countries under the 2001 Council of Europe Convention on Cybercrime, which currently has more than 50 signatory States.[33]

4.3.1 The cybercrime scenario

As part of the first phase of the cyber laws project, the legal framework for the fight against cybercrime was mapped on the basis of desk research.

In the second phase of the project, a summary of the legal framework, describing a number of offences and penalties, was published in an article on the internet. The article was published in January 2018, on BarefootLaw's Facebook page and its website.[34] In addition, cybercrimes were discussed as part of other consultative activities, including interviews and workshops.

4.3.1 Summary of the legal framework

In Uganda, the 1950 Penal Code Act, the 1950 Criminal Procedural Act and the 1996 Police Act provide general rules on substantive and procedural criminal law, as well as general powers and duties of police officers, which may be relied upon to fight cybercrime. More specific statutory law on cybercrime was introduced with the 2006 Copyright and Neighbouring Rights Act, the 2010 Regulation of Interception of Communication Act and the 2011 Computer Misuse Act.

With the 2006 Copyright and Neighbouring Rights Act, Parliament provided for the protection

33 See https://www.coe.int/en/web/cybercrime/-/glacy-uganda-kick-started-the-process-to-accede-to-the-budapest-convention and media reports on https://pctechmag.com/2018/01/ministry-of-ict-national-guidance-hosts-the-council-of-europe-on-the-budapest-convention-on-cyber-crime/

34 https://www.facebook.com/Barefootlaw/

of literary, scientific and artistic intellectual works, including on the internet. The aim of the 2010 Regulation of Interception of Communication Act was to provide for the lawful interception and monitoring of certain communications. The 2011 Computer Misuse Act was enacted by Parliament with the aim to, amongst others, prevent unlawful access to, abuse or misuse of computers. It provides for definitions of cybercrimes, related penalties and some procedural measures that law enforcement authorities can use in their fight against cybercrimes.

Although Uganda has already expressed a preliminary interest to work more closely with other countries in the fight against cybercrime, Uganda has not yet ratified the main multilateral treaty in the area, the 2001 Council of Europe Budapest Convention on Cybercrime.[35] Regional initiatives that provide rules for the fight against cybercrime also exist, including a Convention of the African Union[36], although the latter has not yet entered into force owing to the limited number of ratifications by African States.[37] While drafting its legislation, Uganda appears to have relied on international model laws, including model laws provided in the framework of the International Telecommunications Union (ITU) and the Commonwealth[38], which provide for a certain level of compatibility with the legal framework of other countries.

4.3.2.1. Types of cybercrime

The 2011 Computer Misuse Act defines a number of cybercrimes, which could be grouped into four different categories. In all cases, computers are defined broadly, which may therefore involve individual computers or devices (e.g. mobile phones) or computer networks.

First, crimes that target computer systems could be distinguished, including obtaining unauthorised access to a computer, unauthorised interference with computer data, the production or use of a device or program to overcome security measures or to commit any other cybercrime, interception of computer services or the unauthorised disclosure of access codes or other information.

Second, electronic fraud is defined as a criminal offence, i.e. where money was stolen and where part of the process involved communication through a computer network.

Third, computers can also be used to produce or distribute child pornography, regarding which the 2011 Computer Misuse Act defines a number of offences.

Fourth, the 2011 Computer Misuse Act defines the offences of cyber harassment, cyber stalking and offensive communication.

The 2011 Computer Misuse Act introduces penalties for these offences, ranging from a fine of (maximum) UGX 480,000 and a maximum imprisonment of 1 year for the use of offensive communication to a fine of (maximum) UGX 4.8 million and 10 years of imprisonment for some of the other offences. In a number of cases, for instance where protected computers were involved in the commission of the cybercrime (i.e. a computer relating to the defence of Uganda or a computer system of the police), cybercriminals may be punished with a maximum imprisonment for life.

With the 2006 Copyright and Neighbouring Rights Act, certain infringements of copyright of computer works are defined as a criminal offence, as well as the infringement of copyright by means publication or distribution on the internet. A person who commits an offence in relation to copyright protected works is punishable on conviction by a maximum fine of UGX 2 million and/or a maximum imprisonment of 4 years.

4.3.2.2. Procedural measures to fight cybercrime

In view of the specific nature of cybercrimes, the 2010 Regulation of Interception of Communications Act

35 See https://www.coe.int/en/web/cybercrime/-/glacy-uganda-kick-started-the-process-to-accede-to-the-budapest-convention and media reports on https://pctechmag.com/2018/01/ministry-of-ict-national-guidance-hosts-the-council-of-europe-on-the-budapest-convention-on-cyber-crime/

36 2014 African Union Convention on Cyber Security and Personal Data Protection

37 By February 2018, only Senegal had ratified the Convention.

38 See for an overview of cybercrime model laws the discussion paper of the Council of Europe on "Cybercrime model laws" of 9 December 2014, available at https://rm.coe.int/

and the 2011 Computer Misuse Act were also used to introduce a number of procedural measures to allow authorities to better fight cybercrime. On the basis of these laws, law enforcement authorities may intercept communications on a telecommunications network on the basis of a warrant. Similarly, law enforcement authorities may in certain circumstances oblige a person to decrypt information.

Police officers may also order the preservation of computer data where they expect that the data is relevant to an investigation but may be vulnerable to loss or deletion. Following a court order, officers may also order the disclosure of that preserved computer data or the production of computer data, for instance from a provider of computer services. Law enforcement officers are also entitled to search and seize computers and computer data.

4.3.2.3. Territorial scope of the Act

The 2011 Computer Misuse Act has a broad territorial scope as it allows for offences to be prosecuted where they are related to Uganda in a number of different ways. According to the Act, criminals can be prosecuted for cybercrimes committed when they were in Uganda or where the device used for or affected by the crime was in Uganda. Offences under the Act can be prosecuted irrespective of the nationality of the perpetrator or whether the person is inside or outside Uganda.

4.3.3. Observations

Although the legal framework in Uganda for the fight against cybercrime appears to provide an adequate basis for law enforcement and judicial authorities to investigate and prosecute cybercrimes, the results of the cyber laws project have also allowed for the identification of a number of issues from a legal perspective in this area.

First, it may be questioned whether the legal framework in Uganda is sufficiently consistent to provide for the right mechanisms for the fight against cybercrime. Although the use of international model laws can usually be considered as beneficial, including for better international collaboration, it appears this may have had some detrimental effects on the consistency of the legal framework in Uganda. For example, some of the substantive provisions that define offences appear to be overlapping and some definitions appear superfluous or to be missing instead. In addition, the use of international model laws also may have resulted in certain needs not being addressed sufficiently, including, for example, electronic fraud conducted with mobile money. This may be especially problematic in the area of criminal law, where clarity and specificity of provisions is particularly important.

Second, it appears that the legal framework currently does not provide for legal means to cooperate internationally. As cybercrime is increasingly a cross-border phenomenon, with cybercriminals targeting people or devices in other parts of the world, international cooperation between law enforcement and judicial cooperation becomes increasingly important. Although cooperation can perhaps take place on an ad hoc basis, proper collaboration that would provide credible evidence that can be used in criminal proceedings should be based on a firm legal framework. As of now, such a framework is not available in Uganda, which may hamper investigations by competent authorities in Uganda, as well as in other countries.

Third, proper conditions and safeguards to take account of the rights of suspects, accused persons or other persons do not appear to be present in all cases. In order to be able to guarantee rights and freedoms attributed under international law or the 1995 Constitution as part of cybercrime investigations, the legal framework should provide for appropriate conditions and safeguards. In certain cases, for instance where authorities are attributed the right to order service providers to produce subscriber information, or to provide encryption keys, these safeguards are not always apparent.

Fourth, it appears that competent authorities for the fight against cybercrime do not always have the right resources and tools to properly investigate and prosecute cybercrimes on the basis of the measures that are provided by the legal framework. Whereas authorities may not have sufficient access to technical means, this also relates to a lack of awareness of and a sense of urgency in relation

to cybercrime. As a result, the confidence of the general public in the protection they are afforded under the legal framework is rather low, although this may also be attributed to the lack of awareness among the general public of the existence of the legal framework.

Finally, it has become clear that people in Uganda are usually not aware of the existence of the legal framework regarding cybercrime. On the one hand, the general public is not aware of the risks of cybercrime, the actions that can be considered as cybercrimes and the protection that the legal framework affords them. On the other hand, it also seems that authorities are not always aware of the threat cybercrime poses to security, or of the measures the legal framework offers them to fight cybercrime.

4.3.4. Recommendations for the government

On the basis of these observations, the following recommendations are addressed to the government of Uganda.

First, the government may consider revising existing legislation to allow for competent authorities to better fight current and future cybercrime threats. Although it does not appear that the existing legislation has any significant lacunae, the government could consider clarifying and providing consistent definitions of offences, as well as better alignment with main multilateral frameworks for the fight against cybercrime. In particular, the absence of a legal framework for international cooperation and appropriate conditions and safeguards to protect fundamental rights should be considered as a priority in case the government decides to revise its legal framework.

Second, the government could consider strengthening the capacity of competent authorities to fight cybercrime. Whereas the existing legal framework provides for the use of certain measures as part of investigations, competent authorities should also have access to the right technical means and expertise to allow them to rely on these measures in practice. This would require investment in equipment as well as appropriate training for law enforcement officers. The better use of appropriate tools, such as production orders addressed to providers, could also obviate the need to use less proportionate measures such as the interception of communications or arrests.

Third, the government could seek international counterparts in order to ensure that appropriate protection can be provided against international cybercrime threats. Although cooperation with regional counterparts could already be contributing to better protection, e.g. in the framework of the East African Community, cooperation at multilateral level also appears warranted. The government could consider concluding regional agreements with neighbouring countries or accession to the Council of Europe Budapest Convention on Cybercrime.

Fourth, the government could consider raising awareness about cybercrime. On the one hand, the government could ensure that competent authorities have got stronger awareness of the threat of cybercrime. Competent authorities could be convinced of the need to treat cybercrimes as a priority and could be informed about how they can use the regulatory framework to conduct investigations and prosecute criminals. On the other hand, the government could consider raising awareness of the risks of cybercrime among the general public, as well as about the need to report cybercrimes to allow competent authorities to investigate and prosecute cybercriminals.

4.3.5. Guidance for businesses and citizens

Businesses that use ICT and that are operating online are advised to inform themselves about the risks of cybercrime. In particular where electronic transactions are conducted, businesses should be aware of the risks, e.g. of online fraud with stolen credit card information. Although businesses may accept a certain level of risk, efforts should be made to mitigate or avoid risks where necessary, e.g. through the use of appropriate cybersecurity measures.

Where businesses become the victim of cybercrimes, e.g. of online fraud with stolen credit card information, they should report it to ensure follow-up actions by competent authorities. Only where cybercrimes are reported and where competent authorities are

made aware of the need to investigate and prosecute cybercrimes can a safer online environment develop.

Citizens, in particular in their role as consumers of e-commerce services, should also inform themselves of the risks of cybercrimes. Equally, they should protect themselves with appropriate cybersecurity measures and report cybercrime to the police.

4.4 Access to government information

With the growing use of information and communication technology, the value of information in our society has increased significantly. Information is now an important driver of economic development and access to information has become essential for citizens, businesses and government to play a meaningful role in society.

Information of interest to citizens and businesses is often collected and held by government agencies. A public body may hold information that directly affects a person, e.g. a decision that affects someone's ability to operate a business. Moreover, access to information held by public bodies is often regarded as important for the functioning of a democratic society as it allows for government accountability. Certain information may also represent a business opportunity, for instance where a company could develop innovative services on the basis of government-held information.

It is increasingly recognised that information held by government agencies is public information that should be accessible to the public. Citizens, businesses and civil society organisations (CSOs) are pressuring government agencies to provide better access to information and many countries have enacted legislation that provides for a right of access to information that obliges government to make public key information and to respond to people's requests for information.[39]

In 2014 the Government of Uganda also published the Ask Your Government (AYK) website to facilitate requests for government information and to help citizens to get the information they want from public authorities.[40] Citizens can use the website to make requests and previous requests are stored on the website for further reference. From 2014 up to December 2018, about 2,688 requests were made on the portal.

4.4.1. The access to government information scenario

As part of the first phase of the cyber laws project, the legal framework for access to government information was mapped on the basis of desk research.

In the second phase of the project, a summary of the legal framework for access to government information was published in an article on the internet. The article was published in January 2018, on BarefootLaw's Facebook page and its website.[41] In addition, the right to government information was discussed as part of other consultative activities, including interviews and workshops.

4.4.2. The legal framework

The right for citizens to access public information held by the government is provided under the 1995 Constitution,[42] although information that would affect the security or sovereignty of the State or interfere with the right to the privacy of any other person is exempted.

Subsequent court decisions have provided for limitations regarding the scope of these exceptions that can be invoked by the government to limit the right of access to information.[43] The right of access to information, as confirmed by another

39 See, for instance, the Open Government Partnership (OGP) based on the 2011 Open Government Declaration, in which more than 70 countries around the world are participating (not including Uganda). More information is available at www.ogi.org

40 See http://askyourgov.ug/

41 https://www.facebook.com/Barefootlaw/

42 Article 41, The Constitution of the Republic of Uganda, 1995 (as Amended)

43 Major General David Tinyefuza v. Attorney General (Ruling) (Constitutional Petition No.1 of 1996)) [1997] UGCC 2 (5 March 1997), available at www.ulii.org

court decision, may in certain cases also be invoked by private sector organisations.[44]

In 2015, Parliament also adopted the Access to Information Act with further rules for the implementation of the right for citizens to access information held by the government. The Act provides for certain conditions and procedures that should be followed. Although certain types of information are exempted under the Act, the right of access to information is defined broadly and the reason for which a request is made should not be considered by a government agency when assessing such a request. Further rules in the form of the 2011 Access to Information Regulations were adopted to clarify procedures and provide for access to information in electronic form.

Under international law the right to seek, receive and impart information, which also applies to government-held information, is recognised as a human right in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

At regional level, the African Charter on Human and Peoples' Rights (ACHPR), which has also been ratified by Uganda, acknowledges that every individual shall have the right to receive information. Other regions and countries have also adopted rules that provide for a right of access to information, including at European level.[45] For instance, in the Netherlands, legislation has been adopted that provides detailed rules for the right of access to government information, and also provides for penalties for cases where a government organisation does not respect mandatory deadlines.[46]

4.4.2.1. Types of information

In principle, the right of access to information in Uganda covers all information held by government bodies and agencies. Nevertheless, certain types of information or information held by certain government bodies are exempted where access to that information could infringe on other important interests. For example, records held by Cabinet, information related to someone's health or that could infringe on a person's right to privacy, that could endanger the national security of Uganda or commercial information provided by a third party, are exempted from the right of access to information.

4.4.2.2. Procedures for making a request

When making a request for access to information, certain procedures have to be followed. A person who is making the request has to comply with certain conditions, including that certain forms have to be used. A public body also has obligations and has to put in place procedures to facilitate handling requests. Any person that wants to make a request is entitled to receive support to facilitate the request, and in principle a request has to be processed within a period of 21 days.

Every public body is obliged to have an information officer that is responsible for following these procedures. The information officer has to make available information on these procedures. The officer is also responsible for making available information on what information can be accessed by the public without the need to make a request.

4.4.2.3. Forms of requests and format of the information

A government body may provide electronic forms that can be used for making requests. In addition, persons have a right to make requests in electronic form, e.g. by e-mail.

A person making a request for information may specify the format in which they would prefer the information to be made available. The person may also ask for the information to be made available in electronic format, and even in a format that is machine-readable. Where the information is not available in the requested format, a public body has to consider the possible conversion of the information to the format requested.

44 Greenwatch (U) Ltd. v. Attorney General HCCS 139/2001, available at www.ulii.org

45 See, for instance, the 2009 Council of Europe Convention on Access to Official Documents or the 2003/98/EC European Union Directive on the re-use of Public Sector Information

46 See the 1991 Public Administration Act of the Netherlands

4.4.3. Observations

Notwithstanding the right of access to government information that is attributed to the people of Uganda under the 1995 Constitution and the existence of further detailed rules and a website to implement the right, the results of the cyber laws project have also allowed for the identification of a number of issues from a legal perspective in this area.

First, it appears that many citizens are not aware of their right of access to information. People are unaware that they can request the government to disclose information, which also appears to apply to businesses that may be able to rely on government information to develop and offer additional services. Notwithstanding the existence of a legal framework since 2005 and a dedicated government website, it appears that in most instances requests for government information are phrased as a request for a favour, rather than a request that is based on a formal right.

Second, on a related note, it can be observed that the right of access to information is subject to a rather large number of exceptions. Although subsequent court decisions have clarified that government organisations do not have full discretion when it comes to the decision to not disclose information on the basis of an exception, it is clear that the exceptions limit the effectiveness of the right of access to information in practice. Citizens and businesses can be expected to be discouraged by the existence of so many possible exceptions, which they will expect to be invoked at the will of the government officials in charge.

Third, limitations to the enforcement of the right of access to information may be problematic and may limit the opportunity for citizens to obtain access to justice. Although a refusal by a government agency to disclose information can be challenged before a Chief Magistrate Court, it is not likely that many people in Uganda are able and confident enough to pursue their right in that way. Pursuing a procedure before a Chief Magistrate Court or High Court may be difficult and costly, in particular as the high number of possible exceptions that can be invoked by a government organisation does not make it likely for a complaint before a court to be granted.

Finally, the current legal framework for access to information held by government agencies does not provide for an obligation for government agencies to proactively publish information. The current legal framework only provides for an obligation to provide information on the basis of a request for information, and an obligation to create an overview of the information that is already available without the need to make a request. In addition, government organisations could also be obliged to proactively publish information that could be considered as useful for businesses and citizens.

4.4.4. Recommendations for the government

On the basis of these observations, the following recommendations are addressed to the Government of Uganda. First, the government could consider raising awareness regarding the right of access to government information among government agencies, businesses and citizens. Government agencies should be made aware of the right of citizens and their related obligations. In general, the government should consider measures that would support the development of a culture of openness and transparency, which might enable government agencies to grant more requests and disclose more information. Businesses and citizens could also be targeted by activities to make them aware of their right of access to information and to create more awareness of what citizens and businesses could use that right for in practice, e.g. to develop innovative services that provide additional added value on the basis of raw data collected by government agencies.

Second, these activities could be supported by the development of recommendations or guidelines that would clarify the scope of the right of access to government information, notably in relation to the exceptions that are provided for under the current legal framework. The government could develop a policy framework that guides government organisations to assess requests more favourably and to give confidence to businesses and citizens that their request will be dealt with in a positive way.

Highlighting best practices, e.g. about government agencies that provide access to information on a regular basis, could also be used for that purpose.

Third, the government could consider introducing an obligation for government agencies to proactively make available certain types of government information. Whereas the government could consider revising the existing legal framework to introduce such an obligation, this may also be achieved by developing an appropriate national policy to that end.

Finally, the Government of Uganda could consider joining international initiatives regarding the right of access to information, including the Open Government Initiative. Joining international initiatives could support the development of a culture of transparency and openness amongst government organisations in Uganda and could provide access to international best practices that could be used to improve the functioning of the legal framework in Uganda.

4.4.5. Guidance for businesses and consumers

Businesses are advised to inform themselves of their right of access to information and consider possible business opportunities that could be developed on the basis of government information. Businesses could also consider approaching government agencies with general expectations and specific requests, or even with advice, which could convince government agencies to provide information proactively, consider requests more favourably or comply with requests in electronic form that would allow for easier processing of the disclosed information.

It is recommended that citizens inform themselves of their right of access to information and use their right to request information where possible. Where relevant, citizens should not hesitate to contact information officers in governmental agencies or to involve non-governmental organisations (NGOs) in supporting their requests. Making requests and filing complaints in case those requests are refused by a government agency are likely to provide for clearer rules and procedures and support a culture of openness and transparency in the long run.

4.5 Electronic government services

The increasing use of the internet presents new business opportunities, and also allows for the delivery of electronic services by government organisations (also known as e-government services). In many countries across the world, government organisations are now offering electronic services to their citizens and businesses, which saves them significant amounts of time and money.[47] E-government services can be used to provide information to citizens and businesses, but also to allow for more sophisticated interaction to support democratic processes or to allow for electronic transactions to take place.

In addition, the use of ICT by government organisations also allows a more efficient functioning of government organisations, with subsequent benefits for businesses and citizens.

The delivery of e-government services is also taking off in Uganda, and recently the government launched an eCitizen Portal that provides an overview of government services that can be delivered on the internet.[48]

4.5.1 The e-government services scenario

As part of the first phase of the cyber laws project, the legal framework for e-government services was mapped on the basis of desk research.

In the second phase of the project, a summary of the legal framework for e-government services was published in an article on the internet. The article was published in January 2018, on BarefootLaw's Facebook page and its website.[49] In addition, e-government services were discussed as part of

47 See the United Nations E-Government Survey 2016, which ranks countries according to the availability of e-government services, available at https://publicadministration.un.org

48 See the portal at www.ecitizens.go.ug

49 https://www.facebook.com/Barefootlaw/

other consultative activities, including interviews and workshops.

4.5.2 Summary of the legal framework

Where government organisations have a responsibility for a public matter, this may include the need to deliver services to citizens or businesses, e.g. to issue driver's licences. The process and conditions for the delivery of these services will usually be regulated, including on whether requests can be made in electronic form.

The 2011 Electronic Transactions Act provides for general rules for the delivery of e-government services in Uganda. More detailed rules are provided with the 2013 Electronic Transactions Regulations and the 2015 E-Government Regulations.

At policy level, a national framework also provides for certain guidelines for government organisations to develop their capabilities to use ICT for their internal organisation and service delivery.[50]

No legal framework for the delivery of e-government services at international level has been assessed as part of the cyber laws project. However, several countries around the world have adopted laws that support the delivery of e-government services to their citizens and businesses. For instance, Denmark, which is considered as one of the most advanced countries in the world in terms of the delivery of e-government services, has adopted a legal framework that makes it mandatory for certain government services to be delivered electronically.[51]

4.5.2.1. Government websites, but no mandatory e-government services

In Uganda, the 2011 Electronic Transactions Act only provides for a general legal framework for when government organisations choose to deliver services electronically. Under the Act, government agencies are free to decide whether they want to deliver services in electronic form.

Although it does not introduce an obligation for government organisation to deliver services electronically, the 2015 E-Government Regulations make it mandatory for government organisations to establish and maintain websites. The Regulations provide for detailed rules for government websites, including that they have to be updated regularly and need to provide information about the organisation's mission, its services, relevant laws and policies, as well as contact details.

4.5.2.2. Rules for three types of e-government services

Under the 2011 Electronic Transactions Act, three types of e-government services are specifically recognised. First, the Act specifies that where a document needs to be filed or retained for the provision of a government service, that document may be filed or retained in electronic form. Second, where a permit, licence or approval needs to be provided, that may be provided in electronic form. Third, the Act determines that where a payment is required, the transaction may be processed electronically.

4.5.2.3. Conditions when using e-government services

Where a government agency chooses to deliver government services electronically, the 2011 Electronic Transactions Act provides that the organisation may set certain conditions. Government agencies may, for instance, specify the manner and format in which electronic messages should be sent, or in which form electronic licences or permits are issued.

The 2013 Electronic Transactions Regulations determine that these specifications have to be assessed and confirmed by the Minister for ICT, after which they may be notified in the Uganda Gazette. Thus far, however, it is unclear if any specifications have ever been notified in the Gazette.

4.5.2.4. Roles and responsibilities amongst public bodies

The Act that establishes NITA-U also attributes to it a role to promote and provide technical guidance for the establishment of e-government services. The 2015 E-Government Regulations also oblige NITA-U to provide for an electronic government infrastructure and a government web portal that

50 See the 2010 National Electronic Government (e-Government) Framework of Uganda of the Ministry of ICT, available at www.nita.go.ug

51 Including..... based on the Danish 2012 Digital Post Act

needs to include services for citizens, businesses and the government.

4.5.2.5. Personal data protection in government

Finally, the 2015 Regulations also provide for rules to ensure the security of information and protection of personal data for e-government services. Although government agencies are allowed to share personal data with other public and private organisations, they are not allowed to disclose the information without a person's consent.

If a government agency nevertheless shares personal data without a person's consent, the responsible organisation and the responsible officer can be convicted of a maximum fine of UGX 1.4 million and a maximum prison sentence of three years.

4.5.3. Observations

Notwithstanding the existence of a legal framework regarding the delivery of e-government services, the results of the cyber laws project have also allowed for the identification of a number of issues from a legal perspective in this area.

First, the existing legal framework does not provide for an obligation for government organisations to deliver government services electronically and leaves it to each individual organisation to decide whether or not to deliver services electronically. As a minimum, the current legal framework only provides for rules for government agencies to establish a website that should be used to present certain information. Other obligations that would further the delivery of e-government services at national or regional level are currently not provided for. As a result, it appears that not many government agencies are providing e-government services that allow for electronic transactions. Only a limited number of government agencies appear to have decided to offer e-government services that can be used to conduct electronic transactions. One example is the Ministry of Internal Affairs that provides an electronic platform that can be used by foreign citizens to request a visa that would allow them to travel to Uganda.[52]

Second, notwithstanding the existence of a government portal that brings together information about e-government services, there does not appear to be a clear overview of e-government services that are currently available that would provide for or enable electronic transactions. The existing eCitizens Portal mainly appears to provide an overview of websites and government information, rather than a one-stop shop that can be used by citizens or businesses to arrange for administrative matters in an electronic way. Similarly, notwithstanding an obligation for government agencies to report relevant conditions or requirements, there does not appear to be a comprehensive overview of legal conditions and requirements that are relevant for the delivery of e-government services.

Third, citizens and businesses do not appear to be aware of the existence of e-government services and the legislative framework that facilitates their delivery. Citizens and businesses do not appear to know which government agencies provide e-government services, neither do they appear to be confident regarding the capabilities of government agencies to deliver services electronically. As a result, the overall demand for e-government services appears to be low.

4.5.4. Recommendations for the government

On the basis of these observations, the following recommendations are addressed to the Government of Uganda.

First, the government could consider ensuring the existence of a stronger and more harmonised approach regarding the delivery of e-government services that is based on legislation. Although NITA-U already has a coordinating role regarding the delivery of e-government services, a stronger authority could facilitate the delivery of electronic services by government organisations in Uganda. Whereas a strong policy framework could be relied upon to reinforce the delivery of e-government services in Uganda, the government could also consider a legislative approach, e.g. to identify a number of organisations or services that are required to provide e-government services by a certain date.

52 See the portal at http://visas.immigration.go.ug

Second, the government could create a better overview of e-government services that are currently available to conduct electronic transactions, as well as of relevant conditions and requirements for the delivery of those services. Based on existing obligations, the government should already have an overview of relevant conditions and requirements used by individual government agencies, which could be relied upon to provide a repository of available e-government services and relevant conditions and requirements. On that basis, citizens and businesses could gain a better understanding of the availability and possible use of e-government services, which could instil in them trust in such services and facilitate their use of them.

Finally, the government could raise awareness among businesses and citizens about the availability of e-government services and the existence of a regulatory framework on which they can rely. On that basis, citizens and businesses could also gain a better understanding of the availability and use of e-government services, which inspire in them trust in such services and facilitate their use of them.

4.5.5. Guidance for businesses and consumers

Businesses and citizens are advised to inform themselves of the availability of e-government services that they may be able to rely on, as the better use of those services may present significant benefits to them in terms of time and money saved. While making use of e-government services, businesses and citizens should inform themselves about the obligations of government agencies, e.g. to present certain information on their website. Where it is relevant, businesses and citizens may consider reminding government agencies of their obligations, in order to facilitate the faster adoption of ICT by government organisations.

Nevertheless, businesses and citizens should also be aware of their obligations while making use of e-government services, e.g. to present information in a particular form, in order to ensure the validity of their electronic requests.

Businesses and citizens could also consider approaching government agencies with general expectations and specific requests for e-government services, or even with advice, which could convince government agencies to make better use of ICT and provide more and better e-government services.

5. Relevant Findings

> Although the scenarios that were developed as part of the cyber laws project relate to different online activities that are based on different laws and regulations, they allow for drawing a number of general conclusions on the framework of cyber laws in Uganda.

5.1 Ease of doing business online

A first conclusion relates to the ease of doing business online in Uganda. Across the different case studies explored, it was found that significant obligations are introduced for businesses that want to operate online, either directly or through rights that are assigned to consumers or citizens. In certain cases, these obligations also appear to favour large established players and make it more difficult for small local players to enter the market and develop.

Although certain obligations for businesses operating online are inevitable to ensure public safety, they should be carefully designed to ensure proportionality in view of the development of online markets and internet use in Uganda.

5.2 Citizens' rights and consumer protection

A second conclusion pertains to the rights attributed by the framework of cyber laws, either to people in their capacity as citizens or consumers. In a number of scenarios, these rights have been explored and, in comparison with what is provided at international level or in third-party countries, found to be of quite an ambitious level. A considerable level of consumer protection is, of course, laudable and could inculcate the trust needed to convince people to go online and lead to market development. However, it should also be established whether these rights can really be implemented in view of the development of the market or government agencies in Uganda. Indeed, rights that cannot be invoked or enforced in practice are not meaningful.

5.3 Supporting development and use of new technology

A third conclusion relates to innovation and the development of new technology. In order to allow for the development of technology and its use by society, legislation should be sufficiently flexible. Although current cyber laws in Uganda are still not outdated almost a decade after their development, the extent to which current and potential

future laws are restrictive to the development of technologies merits careful consideration.

It was already concluded hereinabove that strict rules for businesses to operate in the e-commerce market may not have been conducive to economic developments in that area, and future developments such as artificial intelligence. A soft-law approach, rather than formal legislation, may be useful in a certain state of market development, although such approaches may have to be revised at a moment where a market becomes mature and a limited number of players obtain a dominant position in the market (including as observed in relation to mobile money systems).

5.4 International aspects

A fourth conclusion focuses on international aspects of the framework of cyber laws. In view of the borderless nature of the internet, cross-border transactions or cooperation between competent authorities becomes increasingly important. To provide for legal certainty, the legal framework should also provide for and facilitate those interactions.

Although a number of cyber laws include jurisdictional provisions, they do not appear to be based on a realistic perspective on the digital economy where most major providers of services or products are actually based abroad. As a result, these provisions mostly raise questions rather instead of providing answers and, thus, lead to legal uncertainty.

5.5 Enforcement actions

A fifth conclusion could be drawn in relation to the enforcement of rights and obligations under the framework of cyber laws. On the basis of the different scenarios explored, it appears there is an absence of enforcement action by competent authorities, ranging from the criminal justice area to finances, telecommunications and the IT sector.

Whereas the lack of enforcement action may result from the unavailability of resources, it may also relate to the many grey areas under the framework of cyber laws, e.g. the soft-law approach with mobile money. Even where competent authorities or regulators use their powers to intervene, this largely goes unnoticed by the general public, with a negative influence on trust as a result.

5.6 Awareness and access to information

A sixth conclusion regards awareness of and access to information about cyber laws. While mapping relevant cyber laws, but in particular during the consultative activities, it became clear that the public, businesses and government organisations in Uganda are largely unaware and are not well informed about the framework of cyber laws. Whereas a basic, rather superficial knowledge of the existence of cyber laws could usually be observed, the overall majority of stakeholders involved in the project were not aware of specific rights or obligations as part of the framework of cyber laws.

5.7 An original approach that meets the needs of Uganda

A seventh conclusion touches upon the need to consider the distinctiveness of the development and use of ICT in Africa, and more specifically in Uganda. Although developments in ICT take place at the global level, it should be acknowledged that Africa and Uganda specifically have their own dynamic, e.g. the development of mobile money. This dynamic should also be considered when legislation is being drafted. Although the use of international model laws, an as example, has advantages, it should not be relied upon as the only source for the development of legislation. Instead, laws should be prepared on the basis of the views of all stakeholders, for which appropriate consultative activities are essential.

5.8 Legislative technique

An eighth conclusion can be drawn as regards the legally technical aspects of the framework of cyber laws in Uganda. When observed in relation to each other, it becomes clear that the drafting of the different Acts and regulations may have been coordinated better. Although many of the Acts and regulations relate to the same concepts, sometimes different or overlapping definitions are used, such as in relation to what constitutes a computer, an information system or a data message. In other cases, essential definitions appear to have been omitted.

Whereas some of these deficiencies could result from the use and combination of different international model laws, others could perhaps also have been avoided through better coordination amongst government institutions during the process of legislative drafting.

6. Recommendations

On the basis of the aforementioned conclusions, a number of recommendations can be formulated.

First, in order to assess and improve the framework of cyber laws, the government should obtain a good understanding of how these laws operate and function in practice. In this regard, the government initiative to conduct a national IT survey, the first results of which were presented in March 2018[53], should be welcomed. In addition to that, the government should better engage with relevant stakeholders, including international partners, businesses, NGOs and citizens. The role of the competent authorities and regulators cannot be underestimated here.

Second, on the basis of a better understanding of the framework of cyber laws, the government should revise or complement it. Revision of the framework that governs e-commerce, cybercrime and mobile money appear important candidates for legislative work. A soft-law approach may appear useful in the short term, but a more formal approach should be considered to meet the needs in the longer term. Government policies should be updated and developed to complement the legal framework, e.g. to provide more details or legal certainty. Due account will have to be taken of international aspects, in relation to the development of the East African Community (EAC) or other international treaties. Proper consultations and coordination amongst institutions and branches of government should lead to a coordinated effort to ensure quality outcomes.

Third, on a related note, government organisations should step up efforts to enforce rights and obligations under current and future legal instruments. Regulators should be transparent about their interventions and should demonstrate their added value to the public. Enforcement actions should, of course, be meaningful and be taken where they are essential for the functioning or development of a sector, rather than to focus on emerging sectors or small businesses.

Finally, all stakeholders involved should undertake efforts to create greater awareness of the rights, obligations and prohibitions provided by the framework of cyber laws. Businesses should inform themselves about business

53 NITA, "National Information Technology Survey 2017/18 Report", March 2018, available at www.nita.co.ug

requirements and seek legal advice where necessary. Citizens should also seek information and inform themselves about their rights whenever they go online. A special role can be discerned for the government to actively reach out to businesses and citizens about their rights and obligations in order to ensure access to justice in relation to these matters. In that context, the existing activities of government agencies to sensitise the public regarding cyber laws can be welcomed and should be extended, where possible. Civil society also has a role in this regard to convince the government of the need to ensure access to justice in these areas. Where possible, civil society should also take on an independent role to inform businesses and citizens, e.g. by providing general guidance or specific tips that would allow them to better engage in online activities.

7. Annexes -The Framework of Cyber Laws

7.1 The legal framework for mobile money schemes in Uganda

i. The 1995 Constitution

The 1995 Constitution of The Republic of Uganda establishes the Bank of Uganda as the Central Bank of Uganda (Article 161(1)). The Constitution defines the functions of the Bank of Uganda (Article 162(1)), amongst other things, as to (…) (b) regulate the currency system in the interest of the economic progress of Uganda, (c) encourage and promote economic development and the efficient utilisation of the resources of Uganda through effective and efficient operation of a banking and credit system and (d) do all such other things not inconsistent (…) as may be prescribed by law.

ii. The 1993 Bank of Uganda Act Cap 51

On the basis of the Constitution, the 1993 Bank of Uganda Act (Chapter 51 of the Laws of Uganda, 2000) was enacted by Parliament to provide rules for the functioning of the Bank of Uganda, which is referred to as the Central Bank of Uganda in the Act. In terms of its powers, the Act attributes the Central Bank with legal personality and it may do all things necessary to better carry out its functions (Section 5).

The functions of the Central Bank are, amongst other things, to supervise, regulate control and discipline all financial institutions (Section 4(j)). The Act defines a financial institution as a bank, credit institution, building society and any institution classified as a financial institution by the Central Bank (Section 1).

Under Part VII, the Act regulates the relationship between the Central Bank and financial institutions. Pursuant to Section 36, the Central Bank may provide facilities for clearing financial instruments generally on terms determined by the Central Bank.

Following Section 37, the Central Bank shall cooperate with financial institutions to – inter alia – promote adequate and reasonable banking services for the public, to ensure high standards of conduct and management throughout the banking system and to provide facilities for clearing financial instruments.

On the basis of Section 52, the Minister can make regulations for better carrying into effect the provisions of the Act.

iii. The 2004 Financial Institutions Act

In 2004, the Parliament of Uganda enacted the Financial Institution Act to, amongst other things, provide for the regulation, control and discipline of financial institutions by the Central Bank.

According to Section 2 of the Act, it only applies to financial institutions that are defined as companies "licensed to carry on or conduct financial institutions business in Uganda include[ing] a commercial bank, merchant bank, mortgage bank, post office savings bank, credit institution, a building society, an acceptance house, a discount house, a finance house or any institution which by regulations is classified as a financial institution by the Central Bank (Section 3)".

A financial institution's business is defined (Section 3) as the business of, amongst other things, (a) acceptance of deposits, (b) issue of deposit substitutes, (c) lending or extending credit), (e) issuing and administering means of payment, (f) providing money transmission services, and (n) creating and administration of electronic units of payment in computer networks.

The Act also provides rules for, amongst other things, the licensing of these financial institutions, restrictions and prohibitions, supervision by the Central Bank and possible corrective actions. Amongst other things, the Act sets out capital requirements for financial institutions (Part IV) and rules for handling unclaimed balances (Section 119).

Following Section 131 of the Act, the Central Bank may, in consultation with the Minister, make regulations to, amongst other things, (b) provide for the licensing of financial institutions, (h) classify institutions as financial institutions for the purposes of the definition of a financial institution in Section 3 of the Act and (k) provide for anything required or authorised by this Act to be provided for by regulations or by notice.

iv. The 2016 Financial Institutions (Amendment) Act

With the enactment of the 2016 Financial Institutions (Amendment) Act, Parliament introduced several updates in the 2004 Financial Institutions Act, including on agent banking. The Amendment Act provides for the possibility for financial institutions to contract a person to provide a financial institution business on behalf of the financial institution (Section 1(a)).

Based on Section 2(a) of the Amendment Act, the Central Bank shall provide further rules in respect of agents and agent banking.

v. The 2003 Micro Finance Deposit-Taking Act

The 2003 Micro Finance Deposit-Taking Act was enacted by Parliament to provide for the licensing, regulation and supervision of microfinance businesses in Uganda.

Following Section 2 of the Act, a microfinance deposit-taking institution is defined as a company licensed to carry on, conduct, engage in or transact in microfinance business in Uganda.

Microfinance business is defined as the business carried on as the a) acceptance of deposits, b) employing such deposits wholly or partly by lending or extending credit for the account and at the risk of the person accepting those deposits, including the provision of short-term loans to small or micro enterprises and low-income households, usually characterised by the use of collateral substitutes, such as group guarantees or compulsory savings or c) transacting such other activities as may be prescribed by the Central Bank (Section 2).

The Act sets out requirements and procedures for these entities to request and obtain a licence from the Central Bank. Although certain financial services cannot be provided by microfinance businesses (Section 19), they are nevertheless considered as licensed financial institutions once they have obtained a licence under the Act.

vi. The 2011 Bank of Uganda Financial Consumer Protection Guidelines

In 2011 the Central Bank of Uganda adopted guidelines to (a) promote fair and equitable financial services practices by setting minimum standards for financial services providers in dealing with consumers, (b) increase transparency in order to inform and empower consumers of financial services, (c) foster confidence in the financial services sector and (d) provide efficient and effective mechanisms for handling consumer complaints relating to the provision of financial products and services (Paragraph 4).

In accordance with Paragraph 2 of the Guidelines, its scope of application is defined as including all providers of financial services regulated by the Central Bank in respect of services they transact in Uganda (a) and their agents (b). Paragraph 3 of the Guidelines defines financial institutions as a bank, a credit institution, a microfinance deposit-taking institution, a forex bureau or a money remittance company which is regulated by the Central Bank.

Following the guidelines, financial services providers have obligations towards customers in terms of fairness, reliability and transparency (Paragraph 5).

i. Fairness of financial services

Fairness entails that customers should be provided with clear (Paragraph 6(2)) and suitable (Paragraph 6(3)) information before the purchase of a service. A so-called cooling-off period of 10 days should also be provided, within which a customer may revoke or terminate a contract entered with a financial service provider (Paragraph 6(6)).

Changes in the terms of services must be reported to customers (Paragraph 6(8)) and financial institutions are limited in the way they can recover debts when a consumer is unable to repay a loan (Article 6(9)) or when closing customers' accounts (Paragraph 6(10)).

ii. Reliability of financial services

In terms of reliability, financial service providers are obliged to ensure that their ATMs and self-serving banking channels are available day and night, except for emergencies or scheduled maintenance (Paragraph 7(2)). Customer information must be protected and cannot be disclosed to third parties, except where they are obliged to do so by law or with the consent of the customer (Paragraph 7(3)). To protect a consumer's account, a financial service provider is obliged to advise its customers, including on handling a Personal Identification Number (PIN) (paragraph 7(4)).

iii. Transparency of financial services

Regarding transparency, financial service providers must provide fair, clear and transparent information to their customers (Paragraph 8(1)). Summaries of key documents, including contracts, should be provided (Paragraph 8(2)) and terms and conditions should clearly spell out fees, charges, penalties, other rates and liabilities or obligations (Paragraph 8(3)).

iv. Customer complaints

Finally, financial service providers are obliged to put in place and operate appropriate and effective procedures to handle customer complaints (Paragraph 9(2)).

Financial service providers should inform their customers of these procedures (Paragraph 9(3)) and have an obligation to investigate complaints, assess the complaints fairly and offer redress or remedial action that is appropriate (Paragraph 9(4)(a)-(e)).

Customers should be kept informed of the progress of the investigation and should be sent a final response within two weeks after the complaint was received by the provider (Paragraph 9(6)). Financial service providers have the obligation to monitor complaints to identify recurring or systemic issues (Paragraph 9(7)) and must present periodical reports to the Central Bank (Paragraph 9(8)).

v. The 2000 Uganda Communications Act

In 2000, Parliament enacted the Uganda Communications Act with the objective to develop a modern communications sector and infrastructure, amongst other things by liberalising and introducing competition in the sector (Section 2).

The Act establishes the Uganda Communications Commission (Section 3) with the functions to, amongst other things, monitor, inspect, license and regulate communications services (Section 4).

Following Section 1 of the Act, a communications service is a service performed consisting of the dissemination or interchange of sound, video or data content using postal, radio or telecommunications media, excluding broadcasting.

vi. The 2013 Bank of Uganda Mobile Money Guidelines

In 2013, the Central Bank adopted the Bank of Uganda Mobile Money Guidelines. According to Paragraph 14 of the Guidelines, they are an interim measure while the regulatory framework is being revised by the Central Bank and other stakeholders.

i. Objectives of the Guidelines

The objectives of the Guidelines are defined as to a) provide clarity on mobile money services to customers, mobile money service providers, licensed institutions, mobile money agents and other parties involved in the provision of mobile money services in Uganda, b) outline the approval procedure for parties seeking to engage in the provision of mobile money services, c) stipulate the roles and responsibilities of parties engaged in the provision and usage of mobile money services, d) foster consumer protection for mobile money customers, including a mechanism for handling complaints relating to the provision of mobile money services and further the interests of customers in mobile money services, e) enhance competition in the provision of mobile money services and related markets and f) promote financial inclusion (Paragraph 3).

ii. Personal scope and definitions

The scope of application of the Guidelines is defined as all mobile money service providers, all institutions licensed by the Central Bank and partnering with mobile money service providers, all mobile money agents and mobile money customers (Paragraph 4).

In Paragraph 5, the Guidelines provide for several relevant definitions. A mobile money service provider is defined as a person offering mobile money services. A mobile money agent refers to a third party acting on behalf of a mobile money service provider to deal directly with customers. A licensed institution is defined as a financial institution licensed under the 2004 Financial Institutions Act or a microfinance deposit-taking institution licensed under the 2003 Micro Finance Deposit-Taking Act. A mobile network operator (MNO) is defined as a person licensed to provide communications services via mobile networks.

iii. Persons that can offer mobile money services

The Guidelines limit the categories of persons that can offer mobile money services to those that are i) registered companies and that are ii) institutions licensed by the Central Bank or persons partnering with those institutions (Paragraph 6(a)).

Where a person is partnering with an institution licensed by the Central Bank, the Central Bank sets several conditions that must be met before approval is granted. Where approval is granted by the Central Bank, the mobile money service is approved as a product of the licensed institution (Paragraph 6(b)).

iv. Roles and responsibilities of mobile money actors

a) The Central Bank

The Guidelines indicate that the Central Bank is responsible for the approval and supervision of mobile money services (Paragraph 7(1)). The Central Bank can also supervise mobile money services (Paragraph 13) and inspect the technology systems of service providers (Paragraph 9).

b) The Uganda Communications Commission

The Uganda Communications Commission (UCC) is responsible for the licensing and supervision of mobile network operators (MNOs) that provide the infrastructure for mobile money schemes (Paragraph 7(2)).

c) Mobile Money Service Providers

A mobile money service provider is responsible for managing and operating a mobile money platform, as well as for the reconciliation and for attending customer

complaints. Mobile money service providers are responsible for putting in place appropriate and thoroughly tested technology systems (Paragraph 6(b)(iv)). About mobile money agents, service providers should provide for agreements and are responsible for several other conditions, including appropriate training (Paragraph 7(3)).

d) Licensed financial institutions

Institutions licensed by the Central Bank that service providers are partnering with are responsible for monitoring the service providers (Paragraph 7(4)).

The licensed institution and the service provider should enter into an agreement that establishes an escrow account that provides for funds that could be used to reconcile the balance of all mobile money accounts daily (Paragraph 6(b)(iii). Licensed institutions should also be provided with the authority and relevant customer identification documentation to reconcile the balance in case of insolvency or bankruptcy of the mobile money service provider (Paragraph 6(b)(i) and (ii)).

e) Mobile money agents

Persons can only become a mobile money agent when they are i) registered businesses with a physical address and ii) have a bank account with a licensed institution. Agents can open new accounts for customers, receive and pay cash and attend to customer queries and complaints. Agents are prohibited from carrying out transactions when a mobile money platform is not operating properly, from carrying out transactions on behalf of customers and to directly charge customers any fees (Paragraph 7(5)).

f) Customers

Customers are mandated to exercise due care when performing transactions and to follow instructions properly. Customers are also responsible for their PIN, which they should keep secret and not disclose to anyone (Paragraph 7(6)).

v. Interoperability and competition

With a view to making mobile money schemes interoperable, within Uganda and beyond the country, the Guidelines determine that providers of mobile money schemes shall use systems that are capable of becoming technically interoperable with other mobile money schemes.

In Paragraph 10 of the Guidelines, mobile money service providers and any other persons are prohibited from engaging in any practices, contracts, arrangements or understandings that would be likely to substantially inhibit competition in the market. More specifically, under Paragraph 6(b)(i), it is determined that agreements between service providers and licensed institutions cannot be exclusive. In addition, under Paragraph 7(3), it is determined that agreements between service providers and agents cannot be exclusive.

vi. Consumer protection

The Guidelines also provide protection for consumers by clarifying that the 2011 Uganda Financial Consumer Protection Guidelines apply to mobile money schemes (Paragraph12).

In addition, specific rules are provided to ensure that transactions made by consumers are sufficiently assured and secure (Paragraph 12(a)), that consumers are provided with sufficient information on the terms of service by the service provider and agent (paragraph 12(b)) that their privacy and the confidentiality of their customer information and data is sufficiently protected (Paragraph 12(c)) and that appropriate and effective procedures to handle customer complaints are put in place by mobile money service providers (Paragraph 12(d)).

vii. The 2011 Electronic Transactions Act and the 2011 Electronic Signatures Act

With the adoption of the Electronic Transactions Act and the Electronic Signatures Act, the Parliament provided for a regulatory framework for the use, security, facilitation and regulation of electronic communication and transactions and the use of electronic signatures.

In Section 2 of the Electronic Transactions Act, an electronic transaction is defined as the exchange of information or data, the sale or purchase of goods or services, between businesses, households,

individuals, governments, and other public or private organisations, conducted over computer-mediated networks.

In Section 2 of the Electronic Signatures Act, an electronic signature is defined as 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. A wide interpretation of what a computer constitutes in provided in Article 2, also including electronic devices or communications facility related to such a device or group of devices.

The Electronic Transactions Act provides that information shall not be denied legal effect, validity or enforcement solely claiming it is wholly or partly in the form of a data message (Section 5(1)) and where an act, document or information is required to be in writing, produced, recorded or retained, it may be written, produced or retained in electronic form (Section 5(3)). In addition, a contract shall not be denied legal effect merely because it is concluded partly or wholly by means of a data message (Section 14(1)).

The Electronic Signatures Act provides that where a law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature issued which is as reliable as was appropriate for the purpose for which the data message was generated or communication considering all the circumstances, including any relevant agreement (Section 4(1)).

viii. Relevant case law

In **Katuntu vs. MTN Uganda LTD & Anor (HCCS no 248 of 2012),** the parties sought for the High Court of Uganda to consider the application of legislation regulating the financial sector on providers of mobile money services.

Amongst other things, the plaintiffs asked Court for a declaration that providers of mobile money services, including MTN, Airtel, Uganda Telecom and Orange Uganda, are providers of financial services and should be considered as banks or financial institutions under applicable law.

As part of a comprehensive assessment of the locus standi of the plaintiffs (the interest of the plaintiffs in the issues brought before court), the Court also considered relevant definitions in the 2004 Financial Institutions Act. The Court considered that the definition of a 'financial institution' in the Act is clear and does not leave doubt that these providers "are not financial institutions or banks under the Financial Institution Act" (page 44 of the decision).

The Court, however, did not consider whether these companies should be regarded as financial institutions, e.g. by the Central Bank of Uganda. Here, the Court considered that companies that want to conduct financial institutions business should apply for a licence with the Central Bank, but cannot be compelled to do so. Where they are nevertheless conducting financial institutions business without having been granted a licence to do so, the Court found that it would be a matter for the Public Prosecutor's office to be considered under criminal law (page 53).

Taking into account these considerations, the Court concluded that the plaintiffs did not have locus standi and, therefore, dismissed the case.

ix. Examples from other countries

Kenya

In Kenya, mobile money schemes were introduced in 2007. One of Kenya's mobile network operators, Safaricom, introduced the M-Pesa system to facilitate money transfers. In 2015, mobile money transactions accounted for about 25 per cent of Kenya's gross domestic product.

With a view to supporting the development of mobile money schemes, the Central Bank of Kenya issued guidelines in 2010. In 2011, the Parliament of Kenya adopted the Payment Service Act to make provision for the regulation and supervision of payment systems and payment service providers. On that basis, the National Payment System Regulations were adopted in 2014, with a view to,

amongst others, providing for the authorisation and oversight of payment service providers, designation of payment systems and designation of payment instruments (…).

The Regulations set out a regulatory framework for mobile payment service providers. Following Section 2, the Regulations define a mobile payments service provider as means a telecommunications service provider licensed under the Kenya Information and Communications Act and authorised by Central Bank of Kenya to offer payment services. Detailed provisions regarding the licensing of mobile payment service providers as well as roles and responsibilities of other relevant entities are set out.

7.2 The legal framework for e-commerce transactions in Uganda

I. 2010 Contracts Act

With the 2010 Contracts Act, Parliament aimed to codify the law relating to contracts and other related matters. First, the Act provides for definitions and some of the basic elements of the formation of contracts

In Section 2, the Act defines an offer as the willingness to do or to abstain from doing anything signified by a person to another, with a view to obtaining the assent of that other person to the act or abstinence.

An acceptance is defined as an assent to an offer made by a person to whom the offer is made. In addition, a promiser is defined as a person who makes an offer. A promisee is a person who accepts an offer. An offer that is accepted is regarded as a promise. An agreement is a promise or a set of promises. A contract is an agreement enforceable by law.

i. The establishment of a contract

Where the communication of an offer and an acceptance of the offer between a promiser and promisee (Section 3(1)) are completed successfully (Section 4), an agreement is established between that promiser and promisee. An agreement amounts to a contract where it was made with the free consent of parties with the capacity to contract, for a lawful consideration and with a lawful object, with the intention to be legally bound (Section 10).

ii. The form of a contract

A contract may be oral or in written form (Section 3(2)). A contract is deemed to be in written form where, amongst other things, it is in the form of a data message (Section3(3)(a)).

What constitutes a data message is not defined in the Contracts Act, but could be considered as "data generated, sent, received or stored by computer means", as defined by the 2011 Electronic Transactions Act.

iii. Obligations, non-performance and breach of contract

In principle, parties to a contract are obliged to perform or offer to perform their promises (Section 33(1)), unless dispensed with or excused under the Act. Unless a contrary intention appears in the contract, all the persons who make a joint promise as part of a contract shall be bound to fulfil the promise (Section 38).

Unless a contract states otherwise or there is a request of the promisee that states otherwise, the engagement under a contract shall be performed by the promisor within reasonable time (Section 42(1)). The contract or the part of the contract that has not been performed at or before the specified time becomes voidable if parties determined that time was of the essence (Section 47(1)). If time is not of the essence, the promisee is entitled to compensation (Section 47(2)).

Where there is a breach of contract, the party who suffers the breach is entitled to receive compensation for any loss or damage caused (Section 61(1)).

II. 2011 Electronic Transactions Act

With the 2011 Electronic Transactions Act, Parliament provided for, amongst other things, the use, security, facilitation and regulation of electronic communications and transactions.

In Section 4 of the Act, its objectives are defines as, amongst other things, to:

a) enable and facilitate electronic (…) transactions,

b) remove and eliminate the legal and operational barriers to electronic transactions, (…)

d) provide legal certainty and public confidence in the use of electronic (…) transactions, (…)

h) develop 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 to

j) foster economic and social prosperity.

In Section 2 of the Act, an electronic transaction is defined as the exchange of information or data, the sale or purchase of goods or services, between businesses, households, individuals, governments, and other public or private organisations, conducted over computer-mediated networks.

A data message is defined as 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.

A computer is defined as 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 a group of such interconnected or related devices.

An automated transaction is defined as 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 are not reviewed by a natural person in the ordinary course of the natural person's business or employment.

A service provider is defined as (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.

An information systems service is defined as including 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.

A consumer is defined as 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.

An 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.

A person includes any company or association or body of persons corporate or unincorporated.

i. The legal effect of an electronic transaction

In Section 5(1) of the Act, as a main principle it is determined that information shall not be denied legal effect, validity or enforcement solely on the grounds that it is wholly or partly in the form of a data message.

In addition, it is determined that information that is part of a contract that is not in the public domain is regarded as incorporated in a data message where it 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 where it is 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 (Section 5(2)).

For contracts, this is further clarified in Section 14(1), where it is provided that a contract shall not be denied legal effect merely because it is concluded partly or wholly by means of a data message.

In Section 14(2) it is determined that a contract concluded 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. Amongst other things, these rules are important in case of conditional or limited transactions, e.g. transactions as part of a seasonal sale.

It is also provided that even an automated transaction may result in the formation of a contract through an action performed by an electronic agent or by a party to the transaction using an electronic agent (Section 13(1)). The party using an electronic agent is in principle bound by the contract irrespective of whether the party reviewed the actions of the agent or the terms of the contract (Section 13(2)).

ii. Time of dispatch and receipt of an offer or acceptance

Rules for the determination of the time of dispatch and receipt of a data message are provided in Sections 15 and 16 of the Act, unless these are otherwise agreed by the person sending the message and the persons receiving the message. Amongst other things, these rules are important to determine when an offer or acceptance was sent and agreement was formed.

A message is considered as sent at the time the message enters an information system outside the control of the person sending the message (Section 15(1)). Where multiple information systems are involved in the sending of the message, the message is sent at the time when the message enters the first information system outside the control of the person sending the message (Section 15(2)).

Regarding the receipt of a data message, it is provided that where an addressee has designated an information system for the receipt of a message, a data message is considered as received at the time the message enters that designated information system (Section 16(1)(a)), or where it is received by the addressee in case the message was sent to another information system rather than the one that was designated by the addressee (Section 16(1)(b)). Where the addressee has not designated an information system for the receipt of a data message, a data message is received when the data message enters an information system of the addressee (Section 16(2)).

iii. The place of receipt or dispatch of an offer or acceptance

The location of the dispatch or receipt of a data message is determined in Section 17, unless otherwise agreed by the person sending and the person receiving the message. It is provided that the place of dispatch of a data message is considered to be the place of business of the sender or the message (Section 17(1)(a)). Similarly, the place of receipt of the data message is considered to be the place of business of the person receiving the message (Section 17(1)(b)).

Where a person sending or receiving a data message has more than one place of business (Section 17(2)(a)) and one of those places can be considered as more closely related to the transaction, that place of business is presumed to be the place of business (Section 17(2)(a)(i)). Where none of the places of business can be considered as more closely related to the transaction, the principal place of business is considered as the place of business (Section 17(2)(a)(ii)).

Where a person sending or receiving a data message does not have a place of business (for instance where it is a consumer sending or receiving a data message), the place where the person ordinarily resides is considered as the place of business (Section 17(2)(b)).

It is also determined that the actual physical location of the information system which is used for receiving the message is not relevant and may be different from the location where the message is considered to be received (Section 16(3)).

iv. Attributing an offer or acceptance to a person

As it may be difficult to determine the identity of the person sending an offer or an acceptance by means of a data message, Section 19 of the Act provides for rules to determine to whom a message can be attributed.

First, a data message can be attributed to a person originating a message when it is sent by the person originating the message (Section 19(1)(a)). In

addition, a data message can be attributed to a person originating a message when it is sent by an agent of a person originating a message or by a person who has the authority to act on behalf of the person originating a message (Section 19(1)(b)) or by an information system that was programmed by a person originating a message or on behalf of that person (Section 19(1)(c)).

A person receiving a data message can regard the message as sent by an originator of that message when the receiver applies a previously agreed method to ascertain whether the message came from the originator (Section 19(2)(a)), when the message was sent by another person while using a method provided by a third party that can be used to ascertain that the message came from the originator (Section 19(2)(b)), or when the message was sent by an agent of the originator of the message (Section 19(2)(c)).

Following Section 19(3), a person receiving a data message cannot consider that message as coming from the originator of the message where the originator sent a notice to that effect to the person receiving the message (Section 19(3)), where the person receiving the message should have known that the message was not coming from the originator when that person had taken reasonable care (Section 19(3)(b)) or where it was unreasonable for the person receiving the message to consider that the message came from the originator (Section 19(3)(c)).

According to Section 20(1), an acknowledgment of the receipt of a data message is not necessary to give legal affect to a data message, unless specified otherwise. If specified by the sender of a data message, that message can, however, be made conditional on the receipt of an acknowledgement (Section 20(2)) while considering particular conditions regarding the time and form of the message (Section 20(3) – 20(8)).

v. Consumer protection

In Part IV, the Electronic Transactions Act provides for the protection of consumers, where they enter or intend to enter into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier. In Section 28 of the Act, it is determined that a provision in an agreement that excludes any of the consumer rights provided in the Act shall be considered as void.

vi. Information requirements for suppliers

Following Section 24(1), a person has to provide certain types of information when offering goods or services for sale, hire or exchange through an electronic transaction. The information that has to be provided on the website or electronic communication used for the offering of goods and services should include the following:

a) the full name and legal status of the person,

b) the physical address and telephone number of the person,

c) the website 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.

vii. Additional requirements for suppliers

In addition to the information, a person offering goods or services for sale, hire or exchange through an electronic transaction must also provide a consumer with an opportunity to (Section 24(2)):

a) review the entire electronic transaction,

b) correct any mistakes, and

c) withdraw from the transaction before placing an order.

viii. Cancellation within 14 days

In case a person selling, hiring or exchanging goods or services through an electronic transaction fails to provide the information or opportunities specified under Section 24(1) and 24(2), a consumer may cancel a transaction within 14 days after receiving the goods or services.

If a consumer invokes his right to cancel a transaction pursuant to Section 24(3), the consumer is obliged to return the goods to the person who offered the goods, or to cease using the services the person offered (Section 24(4)(a)).

Following a cancellation of the transaction, the person selling or offering the goods or services is held to refund the consumer for all payments after deducting the direct costs of returning the goods (Section 24(4)(b)). The person selling or offering the goods should refund the customer by making a secure payment system (Section24(5)). Where the person selling or offering the goods does not refund the customer or does not use a secure payment system, that person will be liable for any damage suffered by the customer (Section 24(6)).

However, the right for a consumer to cancel a transaction pursuant to Section 24(3) does not apply to electronic transactions of a particular nature or relating to particular services or goods, including (Section 24(7)):

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 foodstuffs, 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

   a. are made to the specifications of the consumer,

   b. are clearly personalised,

   c. by reason of their nature cannot be returned, or

   d. 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.

ix. Cancellation within seven days

A consumer is also entitled to cancel an electronic transaction after the receipt of the goods or services. Following Section 25(1), a consumer may cancel an electronic transaction within seven days of the receipt of the goods or services (a) or within seven days of the conclusion of the agreement (b). No further qualification for the customer to invoke this right is provided.

Where a consumer invokes the right to cancel an electronic transaction after the receipt of the goods or services, that consumer cannot be charged for any other costs than the direct costs of returning the goods (Section 25(2)).

Where a consumer has already effected the payment for the goods or services before the cancellation of the electronic transaction, the consumer is entitled to a full refund of the money paid within 30 days (Section 25(3)).

x. Performance of electronic transaction

According to Section 27(1) of the Act, unless otherwise agreed between a supplier and a consumer, a supplier should execute an order for goods or services by electronic means within 30 days.

In case a supplier fails to execute an order for goods or services by electronic means within 30 days, a consumer has the right to cancel the order after giving a written notice of seven days to the supplier (Section 27(2)).

In case a supplier is unable to supply the goods or services because they are not available, the supplier should notify the consumer before the expiry of the agreed time for the execution of the order. The supplier should subsequently refund the consumer for any payment made in respect of the order for goods or services within 30 days (Section 27(3)).

xi. Territorial application

Following Section 33(1), the Act has effect to any person, irrespective of the person's nationality, citizenship or whether the person is inside or outside Uganda.

xii. Implementing regulations

In Section 35 of the Act, the Minister is attributed the powers to make regulations for (a) any matters that are required to be prescribed, (b) administrative or procedural matters that are necessary to give effect to the Act or (c) matters which are necessary and expedient to give effect to the Act.

iii. The 2013 Electronic Transactions Regulations

With the 2013 Electronic Transactions Regulations, the Minister responsible for ICT provided rules to further implement the 2011 Electronic Transactions Act.

In sub-regulation 2 of the Regulations, NITA-U, as established under the 2009 National Information Technology Authority Uganda Act, is attributed the role of the Authority for the purpose of the Regulations.

i. General information to be provided by service providers

According to Regulation 9(1) of the Regulations, providers of information systems services are obliged to make available the following information to the recipient of a service and relevant enforcement authorities. It is also specified that the information needs to be provided in a form and manner that is easily, directly and permanently accessible:

a) the name of the service provider,

b) the physical address at which the service provider is established,

c) the details of the service provider, including his electronic mail address, which make it possible to contact the service provider rapidly and communicate with him or her in a direct and effective manner,

d) where the service provider is registered in a trade or where a similar register available to the public, the details of the register in which the service provider is entered and his or her registration,

e) where a service provider exercises a regulated profession:

   i. the details of any professional body or similar institution with which the service provider is registered,

   ii. the professional title of the service provider, and

   iii. a reference to the professional rules applicable to the service provider and the means to access them.

Following Regulations 9(2), where a service provider refers to prices, these must be indicated clearly and unambiguously and shall indicate whether they are inclusive of tax.

ii. Information to be provided when concluding a contract electronically

In Regulation 12(1) of the Regulations, service providers are obliged to provide to a recipient of a service the following information. The information should be provided before the contract is concluded and in a clear, comprehensible and unambiguous manner.

a) The technical steps necessary to conclude the contract,

b) Whether the contract will be filed by the service provider and whether it will be accessible,

c) The technical means for identifying and correcting input errors prior to placing the order,

d) The languages offered for the conclusions of the contract.

Following Regulation 12(2), where a service provider subscribes to a code of conduct, the service provider should indicate which code of conduct and provide information on where the code of conduct can be accessed electronically.

According to Regulation 12(4), the information mentioned in Regulations 12(1) and 12(2) does not have to be provided in situations where a contract is concluded exclusively by exchange of electronic mail or by equivalent individual communication (Regulation 12(4)).

In case a service provider provides a recipient of a service with terms and conditions applicable to the contract, Regulation 12(3) determines that the terms and conditions should be provided in a way that allows the recipient to store and reproduce them.

iii. Complaints and offences

Based on Regulation 18(1) of the Regulations, a person may report to the Authority a service provider that has not provided the information as required under Part IV of the 2011 Electronic Transactions Act. As indicated hereinabove, Part IV of the 2011 Electronic Transactions Act includes provisions on the protection of consumers, including on information to be provided by suppliers or sellers to consumers (Section 24 of the Act).

In addition, the failure to provide information as required under Section 24 of the 2011 Electronic Transactions Regulations is defined as an offence in Regulation 20 of the Regulations. A supplier or seller who fails to supply the information may be convicted for a maximum fine of UGX 120.000 .

iv. The 2009 National Information Technology Authority Act

With the 2009 National Information Technology Authority Act, Parliament provided for the establishment of the National Information Technology Authority Uganda (NITA-U), as well as for its objectives, functions, composition, management and finances and certain other related matters. In Section 3(1) of the Act, NITA-U is established as an autonomous body. NITA-U is established as an agency of government under the

general supervision of the responsible Minister (Section 3(3)).

In Section 4, the objectives of the Authority are defined as, amongst other things, to (b) promote standardisation in the planning, acquisition, implementation, delivery, support and maintenance of information technology equipment and services, and to ensure uniformity in quality, adequacy and reliability of information technology usage throughout Uganda.

Accordingly, in Section 5 of the Act, the functions of the Authority are defined as, amongst other things, to (c) co-ordinate, supervise and monitor the utilisation of information technology in the public and private sectors, (d) regulate and enforce standards for information technology hardware and software equipment procurement in all Government ministries, departments, agencies and parastatals, (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, to (h) regulate the electronic signature infrastructure and other related matters as used in electronic transactions in Uganda and to (q) protect and promote the interests of consumers or users of information technology services or solutions. Moreover, in Section 6(e) of the Act, the Authority is attributed the powers to charge fees for the services provided.

Section 39(1) of the Act authorises the Minister to make regulations to give effect to the provisions of the Act. According to Section 39(2), these Regulations may also provide for penalties for cases where the provisions as part of these Regulations are contravened.

v. The 2016 Certification of Providers of Information Technology Products and Services Regulations

With the 2016 Certification of Providers of Information Technology Products and Services Regulations, the Minister of Information and Communications Technology and National Guidance provided further rules for the implementation of the 2009 National Information Technology Authority Act.

i. Definitions in relation to certification

In Regulation 2 of the Regulations, NITA-U is defined as the Authority.

Regulation 2 defines certification as a formal procedure by which the Authority assesses, verifies and attests that a person providing information technology products or services meets the requirements and standards prescribed under the Regulations.

In Regulation 2, an information technology service is defined as a service that provides value to a customer provided by a supplier, application solution provider, consultant, and service delivery, including an internet café. In relation to an information technology service, 'providing' is defined as offering those services for sale to the general public.

ii. Obligation of certification for service providers

In Regulation 3(1) of the Regulations, it is determined that persons cannot deliver information technology products or services unless the person is certified in accordance with the Regulations.

Regulation 4(1) of the Regulations provides that the Authority is responsible for the certification of providers of information technology products or services under the Regulations. Nevertheless, in Regulation 4(2) it is determined that the Authority may use the services of a recognised certification body to certify providers of information technology products or services.

iii. Applications for certification

According to Regulation 5(1) of the Regulations, a registrar is established for the purpose of the certification procedure under the Regulations. The chief executive of the Authority is established as the registrar. In Regulation 5(2), it is determined that the registrar is responsible for (i) receiving and processing applications for certification, (ii) registering certified providers and (iii) implementing any decisions of the Authority regarding the certification. For that purpose, following Regulation 5(3), the registrar

is to establish and maintain a register of certified providers.

Before providing information technology products or services, a person must apply for the registration with the registrar (Regulation 6(1)). For the purpose of the request for certification, a person has to use a pre-determined form (Schedule 1 to the Regulations) and pay a fee (Schedule 3 to the Regulations). The request must be accompanied by a description of the nature of the products or services for which the request for certification is made (Regulation 6(3)).

According to Schedule 3 to the Regulations, fees for an application range from UGX 72, 450 to be paid to the Authority to UGX 166, 530 to be paid to the certification body (for providers of services with an annual gross revenue that exceeds UGX 3 billion and five hundred) to UGX 14,490 to be paid to the Authority and UGX 55, 510 to be paid to the certification body (for providers of services with an annual gross revenue that does not exceed UGX 1 billion). Natural persons that would like to apply for a certification for the delivery of information technology products or services will be charged a fee of UGX 28,980 to be paid to the Authority and UGX 111, 020 to be paid to the certification body.

iv. The certification process

According Regulation 8(1), the Authority has to assess every application for certification to ensure that the applicant complies with all requirements for the delivery of information technology products or services. Where the Authority uses the services of a recognised certification body in accordance with Regulation 4(2), the recognised certification body will assess the application and will provide a recommendation to the Authority (Regulation 8(2)). The Authority may request more information from the applicant to enable the Authority to make a decision (Regulation 8(3)).

Following a request for certification, Regulation 8(4) determines that the Authority should assess the application to ascertain that the application (a) complies with the administrative, legal and technical requirements issued by the Authority, (b) demonstrates experience of the applicant in the provision of information technology products or services and (c) complies with applicable standards relating to the provision of information technology products or services.

On the basis of an application, the Authority should assess the person who made the application on the basis of the requirements included in Section 2 of the Regulations (Regulation 7(1)). Section 2 of the Regulations sets out requirements for providers of information technology products and services, including that the provider should:

a) be a legally registered business in Uganda or outside Uganda,

b) have sound organisational, financial and planning systems to ensure stability in the provision of information technology products or services ,

c) have facilities and equipment to ensure the provision of information technology products or services,

d) have a satisfactory past work performance, track record of credibility, and experience in a given industrial activity for which the certification is sought,

e) have experienced information technology professionals required for the provision of information technology products or services for which the certification is sought,

f) identify the site to be covered under the scope of proposed certification which shall generally be a location at which the person carries out operations,

g) clearly specify the scope of information technology products or services to be included under the certification sought, and that the provider

h) complies with applicable standards relating to the provision of information technology products or services.

In addition, Regulation 7(2) determines that a person who intends to deliver information technology products or services should:

a) be registered in accordance with the law, where it concerns a legal person,

b) abide by the standards for the provision of information technology products or services,

c) demonstrate financial viability, where necessary,

d) put in place and maintain a sound quality management system,

e) have in place policies and procedures to govern the provision of information technology products or services,

f) where applicable, employ competent and qualified staff to provide information technology products or services, and

g) provide the appropriate infrastructure and equipment required to provide information technology products or services.

v. Grant and refusal of certification

On the basis of the assessment of the requirements as set out hereinabove, the Authority should either grant or refuse the certification. The Authority has 45 days after the receipt of the application to take this decision (Regulation 9(1)).

Where the Authority decides to certify a provider, the Authority should provide that provider with a certificate of that decision upon the payment of a certification fee by that provider (Regulation 9(2)). The certificate will be valid for a period of three years or any other period that the Authority may prescribe following the Regulations (Regulation 9(3)). The certificate must be displayed by the certified provider in a clearly visible place on the premises of the provider (Regulation 10)).

Certification fees are prescribed in Schedule 3 to the Regulations and range from UGX 2,070,000 to be paid to the Authority to UGX 7,930,000 to be paid to the certification body (for providers of services with an annual gross revenue that exceeds UGX 3 billion and five hundred) to UGX 414,000 to be paid to the Authority and UGX 1,586,000 to be paid to the certification body (for providers of services with an annual gross revenue that does not exceed UGX 1 billion). Natural persons that would like to apply for certification for the delivery of information technology products or services will be charged a fee of UGX 207, 000 to be paid to the Authority and UGX 793, 000 to be paid to the certification body.

Where the Authority decides to reject or refuse an application, the Authority should provide reasons for that decision. The registrar is obliged to inform the applicant of the decision to reject or refuse the application within 30 days of the decision (Regulation 9(4)).

vi. Suspension or revocation of the certification

Certification may be suspended or revoked by the Authority where (a) the provider is operating in contravention of the 2009 National Information Technology Authority Act or the Regulations or (b) where the capacity of the provider to provide information technology products or services has diminished in a manner that affects the certification (Regulation 11(1)).

The Authority should give notice to the provider in writing before the suspension or revocation. Following the notice, the provider can indicate, within 30 days, why the certification should not be suspended or revoked (Regulation 11(2)). Where the certification is nevertheless suspended or revoked, the Authority should provide reasons for the suspension or revocation (Regulation 11(3)).

Following revocation of the certification, the registrar should remove the provider from the register of certified providers (Regulation 11(4)(a)). Following a suspension, the registrar should make an entry to that effect in the register (Regulation 11(4)(b)).

Following Regulation 12(1), the Authority may decide to reinstate a certification after it was suspended. The Authority may reinstate the certification where it is satisfied that the provider has addressed the matters that were the reason for the suspension of the certification and where the provider has completed the payment of the fee prescribed in Schedule 3 to the Regulations.

Following Regulation 12(2), a provider may make a new application for certification after it was revoked.

The application shall be assessed on the basis of Regulation 8.

vii. Surrender of certification

A certified provider may also surrender a certificate to the Authority (Regulation 13(1)). Following the surrender of a certificate, the provider is no longer allowed to provide information technology products or services, subject to the directions of the Authority (Regulation 13(2)).

viii. Renewal of the certification

In Regulation 14(1), it is determined that a provider should apply for the renewal of a certification six months before its expiry. The Authority can renew certification where it is satisfied that the provider meets the requirements for the certification (Regulation 14(2)). A provider will have to accompany an application for the renewal of a certification with the fee prescribed in Schedule 3 to the Regulations.

ix. Inspections and reviews

In order to ensure compliance with the 2009 National Information Technology Authority Act and the Regulations, the Authority is attributed the powers to inspect and monitor certified providers (Regulation 15(1)). Every certified provider is obliged to pay an annual inspection fee as prescribed in Schedule 3 to the Regulations.

The Authority is obliged to carry out a preliminary inspection within six months after the grant of the certification (Regulation 15(2)) and a full inspection within a year after the grant of the certification, and every year after that (Regulation 15(3)). In addition, the Authority may also conduct ad hoc inspections (Regulation 15(4)). The Authority has to prepare a report of every inspection (Regulation 15(5)).

vi. 2011 Electronic Signatures Act

With the adoption of the 2011 Electronic Signatures Act, Parliament provided a regulatory framework for the use of electronic signatures.

The Act provides that where a 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 communication in the light of all the circumstances, including any relevant agreement (Section 4(1)).

Accordingly, electronic signatures can be used for the attribution of an offer or acceptance to a person in relation to an electronic transaction pursuant to Section 19 of the Electronic Transactions Act.

vii. Relevant case law on e-commerce

In Cargo World Logistics Ltd v. Royale Group Africa Ltd (CIVIL SUIT NO. 157 OF 2013) [2014] UGCOMMC 181 (15 December 2014), the High Court clarified that a contract can be agreed on the basis of an exchange of e-mail messages.

viii. Examples in other countries

i. The United Nations Commission on International Trade Law

The UN Commission on International Trade Law (UNCITRAL) developed model laws to facilitate the development of electronic commerce.

ii. 1996 UNCITRAL model law on electronic contracts

In 1996, UNCITRAL developed a model law on electronic contracts (MLEC) with the aim of removing obstacles and improving predictability in relation to electronic contracts. The MLEC defines a data message as any information in electronic form. It provides that information cannot be withheld from having legal effect solely on the grounds that it is in the form of a data message (article 5). Similar to the 2011 Electronic Transactions Act, it provides that where information is required in writing, it can be in form of data message (article 6). It also provides that for the formation of contracts, an offer and acceptance may be in form of data message (article 11). It also provides rules for the use of signatures in relation to data messages (article 7).

iii. 2001 UNCITRAL model law on electronic signatures

In 2001 UNCITRAL developed a model law on electronic signatures (MLES) with the aim to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and handwritten

signatures. The MLES defines an electronic signature as data in electronic form that can be used to identify a signatory of a data message and its approval of the message. Similar to the 2011 Electronic Signature Act, an electronic signature is considered as appropriate where it is as reliable and as appropriate for the purpose of the data message (article 6). Which technical solution is considered as appropriate can be determined in line with international standards (article 7), with due care being taken by each signatory (article 8).

iv. The European Union

In the European Union, a legal framework has been developed with the aim to facilitate the functioning of the internal market and to provide consumers with an appropriate level of protection.

a) 2001 European Union Directive on electronic commerce

The 2001 European Union Directive on electronic commerce ensures that contracts can be concluded by electronic means and that legal requirements applicable to the contractual process do not create obstacles for the use of electronic contracts or result in such contracts being deprived of legal effectiveness and validity (Article 9(1)). In addition, the Directive determines that for information society services (services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services) a provider has to provide certain information about, amongst other things, the different technical steps to follow to conclude the contract, and the technical means for identifying and correcting input errors prior to the placing of the order (Article 10(1)). When an order is placed through technological means, the service provider is also obliged to acknowledge the receipt of the recipient's order without undue delay and by electronic means. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them (Article 11(1)).

b) 2011 European Union Directive on consumer rights

The 2011 European Union Directive on consumer rights provides a high level of protection for consumers as part of distance contracts (contracts concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded). The rights provided by the Directive cannot be waived by consumers and any agreement that restricts the rights shall not be binding (Article 25).

The 2011 Directive determines that certain information has to be provided to a consumer before that consumer is bound by a contract, including information about (Article 6(1)):

(a) the main characteristics of the goods or services,

(b) the identity of the trader, such as his trading name,

(c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address,

(d) (…),

(e) the total price of the goods or services inclusive of taxes,

(f) (…),

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right (…),

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods, (….)

The Directive also provides for certain formal requirements, including that the information provided in Article 6(1) shall be made available to

the consumer, that the trader shall ensure that the consumer explicitly acknowledges that the order implies an obligation to pay and that the trader shall provide the consumer with confirmation of the contract concluded (Article 8).

The Directive introduces a right for consumers to withdraw from a distance contract within 14 days, without the need to give any reason and without incurring any costs. The trader has to inform the consumer of the right of withdrawal (Article 6(1)(h)) before the contract is agreed, or that the trader's prerogative to exercise the right is extended to 12 months from the initial withdrawal period (Article 10(1)). The consumer has to inform the trader of a decision to withdraw (Article 11(1)), as a result of which the obligations of the parties to perform the contract will be terminated (Article 12). The trader shall reimburse the payments made by the consumer within 14 days (Article 13(1)) and the consumer shall return the goods to the trader within 14 days and will only bear the direct costs of returning the goods (Article 14(1)). The right of withdrawal does not apply to the following contracts (Article 16):

a) service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader,

b) the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period,

c) the supply of goods made to the consumer's specifications or clearly personalised,

d) the supply of goods which are liable to deteriorate or expire rapidly,

e) the supply of sealed goods which are not suitable for return due to health protection or hygiene reasons and were unsealed after delivery,

f) the supply of goods which are, after delivery, according to their nature, inseparably mixed with other items,

g) the supply of alcoholic beverages, the price of which has been agreed upon at the time of the conclusion of the sales contract, the delivery of which can only take place after 30 days and the actual value of which is dependent on fluctuations in the market which cannot be controlled by the trader,

h) contracts where the consumer has specifically requested a visit from the trader for the purpose of carrying out urgent repairs or maintenance. If, on the occasion of such visit, the trader provides services in addition to those specifically requested by the consumer or goods other than replacement parts necessarily used in carrying out the maintenance or in making the repairs, the right of withdrawal shall apply to those additional services or goods,

i) the supply of sealed audio or sealed video recordings or sealed computer software which were unsealed after delivery,

j) the supply of a newspaper, periodical or magazine with the exception of subscription contracts for the supply of such publications,

k) contracts concluded at a public auction,

l) the provision of accommodation other than for residential purposes, transport of goods, car rental services, catering or services related to leisure activities if the contract provides for a specific date or period of performance,

m) the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal.

Unless otherwise agreed, the trader is obliged to deliver goods without undue delay and not later than 30 days from the conclusion of the contract (Article 18(1)). Where a trader has failed to deliver the goods within the agreed time or time limit of 30 days, the consumer shall call on the trader to deliver within an additional period of time. Where the trader fails to deliver the goods within the additional period of time, the consumer is entitled to terminate the contract (Article 18(2)). In that case, the trader is obliged to reimburse all sums paid under the

contract (Article 18(3)).

c) *2015 proposals for a European Union Directive on aspects concerning contracts for the online and other distance sales of goods and for a Directive on certain aspects concerning contract for the supply of digital content*

Currently, the European Union is considering proposals for a Directive on aspects concerning contracts for the online and other distance sales of goods and for another one on certain aspects concerning contracts for the supply of digital content. These directives have the aim to facilitate the functioning of the internal market of the Union and to provide consumers with an appropriate level of protection while taking into account the further development of technology and electronic commerce. Once adopted, these Directives will provide for the harmonisation of rules regarding the conformity of goods and digital content bought online, available remedies in case of a lack of conformity and the possible termination and consequences of the termination of these contracts.

7.3 The legal framework for the fight against cybercrime in Uganda

i. General provisions of criminal law

Some of the relevant provisions on criminal law can be found in the 1950 Penal Code Act, the 1950 Criminal Procedure Code Act and the 1996 Police Act.

With the 1950 Penal Code Act, Parliament provided for general rules of criminal responsibility and definitions of criminal offences and maximum penalties. With the 1950 Criminal Procedure Code Act, general procedures to be followed in criminal cases are provided. With the 1996 Police Act, the general structure, organisation and functions of the police force are provided.

The 1996 Police Act provides, amongst other things, for general powers and duties of police officers to prevent the commission of offences or to detect and bring offenders to justice (Section 21), including for searches (Section 27), for the seizure and retention of property (Section 29) and for the power to instigate criminal proceedings (e.g. to apply for search warrants (Section 31)).

ii. 2010 Regulation of Interception of Communication Act

i. Aims and definitions

With the 2010 Regulation of Interception of Communication Act, Parliament provided for the lawful interception and monitoring of communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda.

In Section 1 of the Act, interception by means of a telecommunication system or radio communication system is defined as listening to, recording, reading or copying the contents of a communication, whether in whole or in part

Section 1 also defines a service provider as the provider of a postal service or telecommunication service. Telecommunication services are defined as services consisting of transmission of data, voice, 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.

In Section 1, protected information is defined as information that is encrypted by means of a key.

ii. Prohibition of interception

Section 2(1)(a) of the Act provides for a general prohibition of the interception of communication over a telecommunication system. As an exception, however, it is provided that the interception of communication is allowed where a person is (i) party to the communication, (ii) has the consent of the person by or to whom the communication is sent, or (iii) is authorised by a warrant.

In addition, Section 2(2) provides that the bona fide interception of a communication for or in connection with the provision, installation, maintenance or repair

of a telecommunication service is also not covered by the general prohibition.

The intentional interception, or intent to intercept, is defined as an offence for which a person can be convicted with a maximum fine of UGX 2.4 million and/or imprisonment of a maximum of five years (Section 2(3) of the Act).

iii. Procedures to obtain a warrant

Section 4 to 6 of the Act provide for procedural rules for law enforcement authorities to obtain a warrant for the interception of communications, including the persons authorised to apply for a warrant, the issuance of the warrant by a designated judge and the scope of a warrant.

iv. The role of telecommunications providers

In Section 8(1) of the Act, providers of telecommunications services are obliged to provide assistance for the lawful interception of communications, including (b) installing hardware and software facilities and devices to enable interception of communication at all times.

The failure to provide assistance is defined as an offence, for which a provider may be convicted with a penalty of a maximum fine of UGX 2.4 million or a maximum imprisonment of five years (Section 8(2)(a)). In addition, a provider's telecommunications licence also be cancelled (Section 8(2)(b)).

Telecommunications service providers are obliged to obtain certain information from any person to whom they are providing services, including the person's full name, residential address, business address, postal address and the person's identity number contained in the person's identity document (Section 9(1)(a)). For that purpose, service providers are obliged to ensure that their existing customers register their SIM cards (Section 9(2)).

In addition, Section 11(1) of the Act obliges providers or telecommunications services to (a) provide a telecommunications service which has the capability to be intercepted and (b) store call-related information. The responsible Minister is to provide directives to providers with further specifications for these obligations (Section 11(2) and (3)).

v. Obligations regarding encrypted information

On the basis of Section 10(1) of the Act, persons who are believed to have possession of a key in respect to encrypted information may be imposed to disclose that information by a person who is authorised to do so (as specified in Section 4(1)).

A disclosure requirement may be imposed where the authorised person believes that (a) a key to the protected information is in the possession of a person and where (b) the information is necessary (i) in the interest of national security, (ii) for the purpose of preventing or detecting an offence that may result to loss of life or threat to life, (iii) for the purpose of preventing or detecting an offence of drug trafficking or human trafficking or (iv) in the interest of the economic well-being of Uganda.

A disclosure requirement should be given by notice, for which certain conditions regarding its manner, form and scope are provided (Section 10(2) and (3)).

Following a notice, a person who is in possession of both the encrypted information and the encryption key should (a) use any key in the person's possession to provide access to the information and (b) disclose the information in an intelligible form (Section 10(4)). A person who had possession of an encryption key, but no longer possesses the key, may be obliged to disclose information that will facilitate the obtaining or discovering the key (Section 10(5)).

The failure to disclose information following a notice is defined as an offence, for which a person may be convicted of a penalty of a maximum fine of UGX 2.4 million or awarded a maximum imprisonment of five years (Section 10(6)).

Providers or telecommunications providers and holders of encryption keys may be entitled to compensation for, respectively, their assistance in the interception of communication or the disclosure of an encryption key, or for rendering the encrypted information intelligible (Section 12).

iii. The 2011 Computer Misuse Act

i. Aims and definitions

The 2011 Computer Misuse Act was adopted with the aim to make provisions:

- 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.

In Section 2 of the Act, a computer is defined as 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, including 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.

Information is defined as including data, text, images, sounds, codes, computer programs, software and databases. Data is defined as electronic representations of information in any form. Data messages are defined as data generated, sent, received or stored by computer means, including a) voice, where the voice is used in an automated transaction and b) a stored record.

A program or computer program is defined as data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

An information system is defined as a system for generating, sending, receiving, storing, displaying or otherwise processing data messages, including the internet or any other information sharing system.

ii. Certain actions and notions relating to cybercrimes

Part II of the Act includes general provisions with certain acts or notions relating to cybercrimes that determine the scope of some of the cybercrimes included in the Act.

Section 3 of the Act defines the act of securing access to a program or data as: a) viewing, altering or erasing a program or data, b) copying or moving 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) using or destroying it, or d) causing it to be output from the computer in which it is held whether by having it displayed or in any other manner.

Section 4 of the Act defines using a program as a) causing a computer to execute a program or b) causing a computer to perform a function of a program.

Section 5 of the Act defines that access to a program or data held in a computer is authorised if a) a person is entitled to control access to the program or data or b) if the person has consent to access to program or data from any person who is charged with giving that consent.

According to Section 6(1) of the Act, a reference to a program or data held in a computer includes a reference to a program or data held in any removable storage medium, and a computer is considered as containing any program or data held in any such storage medium. Following Section 6(2), a reference to part of a program equals a reference to a program.

Section 7 of the Act defines that the modification of content on a computer takes place where the function of a computer or of a connected computer results in: a) the alteration or erasure of a program, data or data message or b) a program, data or data message being added.

Following Section 8 of the Act, modification of content on a computer is unauthorised if a) a person who modifies the content is not entitled to determine whether the modification should be made or if b) the person who modifies the content does not have the consent of a person who is entitled.

iii. Procedural measures to fight cybercrime

In Part III of the Act, certain procedural powers that are relevant to the fight against cybercrime are attributed to relevant investigative officers.

In Section 9(1), it is determined that an investigative

officer may apply for a court order for the expeditious preservation of data. The preservation of data can be ordered where there are reasonable grounds to believe that the data is vulnerable to loss or modification. Following Section 9(2), preservation orders can be made for traffic and subscriber data. As defined in Section 2, traffic data includes data relating to communication by means of a computer system generated by a computer system that formed a part of the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service. Against whom preservation orders may be served is not defined.

Following Section 10, an investigative officer may apply for a court order for the disclosure of the preserved data that is required for a criminal investigation or the prosecution of an offence. This may include all data preserved (Section 10(a)), irrespective of whether one or more service providers were involved, or some of the data that is sufficient to identify a service provider that was used for transmitting the data (Section 10(b)). The order for the disclosure of preserved data may also include an electronic key that enables access to or allows for the interpretation of the data.

An investigative officer may also apply for a court order for the production of data that is required for a criminal investigation or the prosecution of an offence (Section 11(1)). The court order can be used to compel a) a person to submit specified information that the person has possession or control over and which is stored in a computer or b) a service provider to submit subscriber information in relation to the services it is offering where it has possession or control over that information. Following Section 11(2), a production order should be deemed to require a person to produce or give access to information in a form that can be taken away, and which is visible and legible.

In Section 28, specific rules on searches and seizures are provided. On the basis of Section 28(1), a magistrate or judge may issue a warrant authorising a police officer to enter and search premises where there is reasonable ground to believe that any of the offences under the Computer Misuse Act is or are about to be committed on those premises and that evidence of those facts is on those premises.

On the basis of Section 28(2), an authorised officer may seize a computer system or take samples or copies of data where a) they are concerned in or there is reasonable ground to believe that that they are concerned in the commission or the suspected commission of any offence, b) they may afford evidence of the commission or the suspected commission of any offence, or c) it is intended to be used or there is reasonable ground to believe that it is intended to be used in the commission of any offence. Pursuant to Section 28(3), the seizure or samples or copies of applications or data may only be taken on the basis of a search warrant. Where a search warrant is issued on a Sunday, it may be executed between sunrise and sunset, or at any time where the warrant provides for that (Section 28(4)). For the execution of a search warrant, an authorised officer may at any time search any computer system (Section 28(5)(a)), require a person to provide assistance (Section 28(5)(b)) or compel a service provider to collect or record or cooperate and assist in the collection of traffic data in real time where it is transmitted by means of a computer system (Section 28(5)(c)).

Authorised officers have to observe due regard for the rights and interests of persons affected by these powers (Section 28(6)). Obstructing, hindering or threatening an authorised officer in the performance of his duties in relation to searches and seizures is considered as an offence that is liable for a fine and imprisonment of a maximum of 6 months (Section 28(7)). Computer systems or copies or samples of data taken by an authorised officer need to be returned within 72 hours, unless an order for the extension of that the time has been obtained (Section 28(8)).

An authorised officer is a police officer who has obtained an authorising warrant for the search or seizure under Section 28(1)).

In Section 29, special rules are provided on the admissibility and weight of electronic evidence in legal proceedings. No rules on evidence shall be used

to deny the admissibility of electronic evidence merely on the ground that it is in electronic form, if it is the best evidence that can be expected to be presented or merely on the ground that it is not in its original form (Section 29(1)). Additional rules for the presentation and weight of electronic evidence in legal proceedings are provided.

iv. Definitions of cybercrimes

In Part III of the Act, definitions of cybercrimes and related sentences are provided.

a) Cyberattacks: crimes targeting computers

i. *System interference*

The first types of offences are related to crimes that are directed at the particular use of computer systems. Section 12 provides for the offence of unauthorised computer access. In Section 12(1), the unauthorised access to or interception of a program or data is defined as an offence. In Section 12(2), the intentional and unauthorised interference with data that causes a program or data to be modified, damaged, destroyed or rendered ineffective is defined as an offence. In Section 12(3), the unlawful production, sale, offering for sale, procurement for use, design, adaptation for use, distribution or possession of a device, including a program, password, access code or similar data, which is designed primarily to overcome security measures for the protection of data, is defined as an offence. In Section 12(4), the use of such a device is defined as an offence. In Section 12(5), the access of an information system with the aim to execute a denial of service attack or a partial denial of service attack is defined as an offence.

According to Section 12(6), the intent of a person in relation to any of the offences relating to unauthorised computer access does not need to be directed at a particular program or data, a program or data of a particular kind or a program or data held in a particular computer. Unauthorised computer access is punishable by a maximum fine of UGX 4.8 million and/or maximum imprisonment of 10 years (Section 12(7)).

In Section 13(1), it is provided that unauthorised access as defined in Section 12 with the intent to commit or facilitate the commission of any other offence is also considered as an offence. The offence of unauthorised access and the other offence may be committed by the same or by another person (Section 13(2)). The offences may also be committed on different occasions (Section 13(3)). The offence is punishable by a maximum fine of UGX 4.8 million and / or maximum imprisonment of 10 years (Section 13(4)).

ii. *Data interference*

Section 14 provides for unauthorised modification of computer material as an offence. In Section 14(1), the offence of unauthorised modification of computer material is defined as any act that causes an unauthorised modification of the content of a computer with the required intent and knowledge at the time when the act was committed.

The requisite intent should be directed at the modification of the content of a computer and by doing so to: a) impair the operation of the computer, b) prevent or hinder access to a program or data on the computer, or to c) impair the operation of the program or the reliability of the data (Section 14(2)). The intent does not need to be directed at a particular program or data, a program or data of a particular kind or a program or data held in a particular computer (Section 14(3)). The requisite knowledge should be considered as knowledge that the modification is unauthorised (Section 14(4)). It is not relevant whether the unauthorised modification or the intended effect is intended to be permanent or temporary (Section 14(5)). The offence is punishable on conviction by a maximum fine of UGX 7.2 million and /or maximum imprisonment of 15 years.

iii. *Interception*

Section 15 provides for offences relating to the unauthorised use or interception of a computer service. In Section 15(1)(a), securing access to a computer without authority for the purpose of obtaining directly or indirectly any computer service is defined as an offence. In Section 15(1)(b), intercepting or causing to be intercepted without authority, directly or indirectly, any function of

a computer by means of an electro-magnetic, acoustic, mechanical or other device is defined as an offence. In Section 15(1)(c), using or causing to be used, directly or indirectly, a computer or any other device for the purpose of committing an offence as defined in Section 15(1)(a) or Section 15(1)(b) is defined as an offence.

For these offences, it is not relevant whether they were directed at a particular program or data, a program or data of a particular kind or a program or data held in a particular computer (Section 15(3)). The offence is punishable on conviction by a maximum fine of UGX 4.8 million and/or a maximum penalty of 10 years, and in the case of a subsequent conviction to a maximum fine of UGX 7.2 million and/or maximum imprisonment of 15 years (Section 15(1)). Where damage is caused as a result of the offence, a person is punishable in the case of a conviction to a maximum fine of UGX 3.36 million and/or maximum imprisonment of 7seven years (Section 15(2)).

iv. *Obstruction of the use*

Section16 provides for offences relating to the unauthorised obstruction of use of a computer. In Section 16(a), knowingly and without authority or lawful excuse interfering with or interrupting or obstructing the lawful use of a computer is defined as an offence. In addition, Section 16(b) defines that the knowingly and without authority or lawful excuse impeding or preventing access to or impairing the usefulness or effectiveness of a program or data stored in a computer as an offence. The offence is punishable on conviction by a maximum fine of UGX 4.8 million and / or a maximum penalty of 10 years, and in the case of a subsequent conviction to a maximum fine of UGX 7.2 million and / or a maximum imprisonment of 15 years (Section 16(1)).

v. *Disclosure of access codes*

Section 17 provides for the offence of the unauthorised disclosure of an access code. In Section 17(1), knowingly and without authority disclosing a password, access code or any other means of gaining access to any program or data held in a computer, knowing or having reason to believe that it is likely to cause loss, damage or injury to a person or property, is defined as an offence. The offence is punishable on conviction by a maximum fine of UGX 4.8 million and/or a maximum penalty of 10 years, and in the case of a subsequent conviction to a maximum fine of UGX 7.2 million and/or a maximum imprisonment of 15 years (Section 17(2)).

vi. *Disclosure of information*

Section 18 provides for the offence of the unauthorised disclosure of information. In Section 18(1), disclosing or using electronic data, a record, a book, a register, correspondence, information, a document or any other material for any other purpose than for which it was obtained is defined as an offence. The disclosure or use of electronic data, a record, a book, a register, correspondence, information, a document or any other material for the purposes of anything in the Act or for any prosecution for an offence under any written law or in accordance with an order of court are exempted from the definition. The offence is punishable on conviction by a maximum fine of UGX 4.8 million and / or a maximum penalty of 10 years (Section 18(2)).

b) Electronic fraud

Section 19 provides for the offence of electronic fraud. In Section 19(2), deliberately performing deception with the intent 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, is defined as an offence. The offence is punishable on conviction by a maximum fine of UGX 4.8 million and / or a maximum penalty of 10 years (Section 19(1)).

c) Cybercrimes relating to child pornography

Section 23 provides for offences relating to child pornography. Child pornography is defined as pornographic material that depicts a) a child engaged in sexually suggestive or explicit conduct or 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 (Section 23(3)).

In Section 23(1), a number of acts relating to child pornography are defined as an offence. The production of child pornography for the purpose of its distribution through a computer (Section 23(1)(a)), the offering or making available of child pornography through a computer (Section 23(1)(b)), the distribution or transmission of child pornography through a computer (Section 23(1)(c)), the procurement of child pornography through a computer for oneself or for another person (Section 23(1)(d)) or the unlawful possession of child pornography on a computer (Section 23(1)(e)) are defined as an offence. In addition, making available pornographic material to a child is defined as an offence (Section 23(2)). The offence is punishable on conviction by a maximum fine of UGX 4.8 million and/or maximum imprisonment of 10 years (Section 23(4))).

d) Cyber harassment and stalking

Section 24 provides for the offence of cyber harassment. In Section 24(2), several acts relating to cyber harassment are defined as an offence. The use of a computer for the purpose of a) making a request, a suggestion or a proposal which is obscene, lewd, lascivious or indecent, b) threatening to inflict injury or physical harm on the person or property of a person or c) knowingly permitting any electronic communications device to be used for the aforementioned is defined as an offence. The offence is punishable on conviction by a maximum fine of UGX 1.44 million and/or maximum imprisonment of three years (Section 24(1)).

Section 25 provides for the offence of offensive communication. Wilfully and repeatedly using electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of a person with no purpose of legitimate communication is defined as an offence. Whether or not a conversation ensues is not considered relevant. Offensive communication is considered as a misdemeanour that is punishable on conviction by a maximum fine of UGX 480 thousand and/or maximum imprisonment of one year.

Section 26 provides for the offence of cyber stalking. Wilfully, maliciously and repeatedly using electronic communication to harass another person and making 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 is defined as an offence. The offence is punishable on conviction by a maximum fine of UGX 2.4 million and/or maximum imprisonment of five years.

v. Protected computers

A number of other provisions with general application to some or all of the offences are included in the Act. Section 20 provides for enhanced punishment where access to a protected computer was obtained for the commission of the offence of unauthorised access (Section 12), unauthorised modification of computer material (Section 14), unauthorised use or interception of computer service (Section 15) or unauthorised obstruction of use of a computer (Section 16). Where convicted of any of these offences, a person is punishable on conviction by maximum imprisonment for life.

For the purpose of the article, a computer is considered as a protected computer where a person knows or ought to have known that a computer, a program or data is used directly in connection with or is 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 (Section 20(2)). For the purpose of a prosecution under the article, a person is presumed to have the knowledge regarding the status of the protected computer until it is proven otherwise (Section 20(3)).

vi. Aiding, abetting and attempts

Section 21 provides for the criminal liability for the person who abets another person in committing any of the offences under the Act (Section 21(1)), as well

as for an attempt to commit any of the offences under the Act (Section 21(2)). What constitutes an attempt to commit any of the offences under the Act is defined broadly (Section 22) and it is, for instance, irrelevant whether the commission of the offence was completed or prevented, either due to circumstances independent of the person's will or whether on the person's own motion (Section 22(2)(a)) or whether it was impossible to commit by reasons or circumstances not known to the person (Section 22(2)(b)).

vii. Compensation for victims

Section 27 provides for the possibility for the court to determine compensation to be paid by a person convicted under the Act to the aggrieved party for any losses suffered by the aggrieved party.

viii. Judicial competences

Section 31 determines that a chief magistrate or magistrate grade I is in the position to hear and decide regarding any of the offences under the Act and has the power to impose the full penalty or punishment in respect of those offences.

ix. Territorial jurisdiction

Section 30 provides for a wide territorial scope for the Act. In the article, it is determined that the Act can be applied to offences where the perpetrator was in Uganda at the time the offence was committed or where the computer, program or data was in Uganda at the time the offence was committed (Section 30(3)).

It is determined that these offences can be prosecuted under the Act irrespective of the nationality or the citizenship of the perpetrator (Section 30(1)), and irrespective of if the person is inside or outside Uganda (Section 30(2)).

IV. 2006 Copyright and Neighbouring Rights Act

With the 2006 Copyright and Neighbouring Rights Act, Parliament provided for the protection of literary, scientific and artistic intellectual works and their neighbouring rights.

In Section 2 of the Act, a computer program is defined as a set of instructions expressed in any language, code or notation, intended to cause the device having an information processing capacity to indicate, perform or achieve a particular function, task or result.

A publication is defined as the lawful reproduction of a work or of an audio-visual or audio-visual sound recording or fixation, or of sound recording for availability to the public; and includes public performances and making available of a work on the internet.

A reproduction is defined as the making of one or more copies of a work or sound recording in any manner or form, including any permanent or temporary storage of the work or sound recording in electronic form.

i. The right of protection of copyright

In Section 4(1) of the Act, it is determined that authors of any work have a right of protection of the work, provided that the work is original and is reduced to material form in whatever method. The protection is provided irrespective of the quality of the work or the purpose for which it is created.

The protection is in principle afforded without any further formalities (Section 4(2)). A work is considered original if it is the product of the independent efforts of an author (Section 4(3)).

ii. Works eligible for copyright

In Section 5(1) it is provided that literary, scientific and artistic works that are eligible for copyright are, amongst other things:

a) computer programs and electronic data banks and other accompanying materials, (…)

b) any other work in the field of literature, traditional folklore and knowledge, science and art in whatever manner delivered, known or to be known in the future.

iii. Economic rights in relation to copyright protected work

Section 9 of the Act determines that the owner of a protected work has the exclusive right to do or authorise other persons to, amongst other things:

a) publish, produce or reproduce the work,

b) distribute or make available to the public the original or copies of the work through sale or other means of transfer of ownership, (…)

c) communicate the work to the public by wire or wireless means or through any known means or means to be known in the future, including making the work available to the public through the internet or in such a way that members of the public may access the work from a place and at a time individually chosen by them,

d) where the work is a pre-existing work, make a derivative work,

e) commercially rent or sell the original or copies of the work, (…)

iv. Moral rights in relation to copyright protected work

Section 10(1) of the Act determines that the author of a protected work also has the following exclusive rights that cannot be assigned to another person (Section 10(3)):

a) Claim authorship of that work, except where the work is included incidentally or accidentally in reporting current events by means of media or other means;

b) Have the author's name or pseudonym mentioned or acknowledged each time the work is used or whenever any of the acts under Section 9 is done in relation to that work, except where it is not practicable to do so; and

c) Object to, and seek relief in connection with, any distortion, mutilation, alteration or modification of the work.

In addition, the author of a protected work has the right to withdraw the work from circulation if it no longer reflects the author's convictions or intellectual concepts. If the author invokes this right, any authorised user of that work who might, in any material way, be affected by the withdrawal must be indemnified by the author (Section 10(2)).

v. Licences or transfer of economic rights

Following Section 14(1), an owner of a copyright protected work is allowed to, amongst other things:

a) assign the economic rights to another person,

b) license another person to use the economic rights

c) transfer or bequeath the economic rights to another person in whole or in parts (…)

vi. Neighbouring rights

Certain other rights that relate to the copyright protected work, so-called neighbouring rights, are also attributed to persons that have a supporting role in relation to a copyright protected work, including performers and producers of a work (Sections 21 to 34 of the Act).

vii. Infringement of copyright, remedies, offences and penalties

Section 46(1) provides that an infringement of copyright or neighbouring rights in relation to a work occurs where a person does or causes or permits another person to do any of the following without a valid transfer, licence, assignment or other authorisation:

a) Reproduce, fix, duplicate, extract, imitate or import into Uganda a work otherwise than for his or her own private use,

b) Distribute a work in Uganda by way of sale, hire, rental or like manner, or

c) Exhibit a work to the public for commercial purposes by way of broadcast, public performance or otherwise.

Section 45(1) provides for a right for a person whose rights in relation to a copyright protected material are infringed upon are in imminent danger of being infringed to institute civil proceedings in the Commercial Court. The civil proceedings can be instituted for an injunction to prevent the infringement or to prohibit the continuation of the infringement. Amongst other things, a person who incurs damages because of the infringement may claim damages against the person responsible for the infringement, irrespective if that person being successfully prosecuted (Section 45(4)).

Section 47(1) provides for the definition of a number of criminal offences in relation to a copyright protected work, including where a person, without the authorisation of or a licence

from the owner of the work or an agent of the owner of the work:

a) publishes, distributes or reproduces the work,

b) performs the work in public,

c) broadcasts the work,

d) communicates the work to the public, or

e) imports any work and uses it in a manner which, were the work made in Uganda, would constitute an infringement of copyright.

A person who commits the offence is punishable on conviction by a maximum fine of UGX 2 million and/or maximum imprisonment of four years. Similarly, Section 48(1) determines that the infringement of a neighbouring right is liable on conviction to a fine of UGX 2 million and/or a maximum imprisonment of four years.

v. Case law

In Uganda v. Nsubuga & 3 Ors (HCT-00-AC-SC-0084-2012) [2013] UGHCCRD 13 (3 April 2013), the High Court of Uganda examined a case where the computer system of the Uganda Revenue Authority was compromised with alleged losses of more than UGX 3 billion. Several persons were prosecuted and convicted for, amongst other things, the unauthorised use and interception of computer services (Section 15), electronic fraud (Section 19), unauthorised access to data (Section 12(1)) and producing, selling or procuring, designing and being in possession of devices, computers, and computer programs designed to overcome security measures for protection of data (Section 12(3)). The Court considered life imprisonment, but sentenced each of the persons to, cumulatively, 20 years of imprisonment and a fine of USD 4,500 (amounting to around UGX 16 million).

In Uganda v. Ssentongo & 4 Ors (Criminal Session Case 123 of 2012) [2017] UGHCACD 1 (14 February 2017), the High Court of Uganda decided on a case of conspiracy to steal money from the MTN mobile money system with alleged losses of almost UGX 10 billion. Several persons were prosecuted and charged for, amongst other things, electronic fraud (Section 19 of the Act) and the unauthorised disclosure of access codes (Section 17 of the Act). Whereas one of the accused was convicted for electronic fraud as the person created mobile money accounts in the name of other persons, the same person was actually acquitted of the unauthorised disclosure of access codes as no loss or likely loss as a result of it occurred.

In Kalungi vs. Uganda (Corruption Division HCT-00-AC-CN-0041-2015) [2016] UGHCACD 2 (28 April 2016), the High Court of Uganda confirmed that a compact disc can be considered as electronic evidence (Section 29 of the Act) and can be admissible in court proceedings. On the basis of the evidence, the Court affirmed the conviction of the accused persons.

vi. Examples in other countries

i. The 2001 Council of Europe Budapest Convention on Cybercrime

The 2001 Convention on Cybercrime of the Council of Europe, sometimes also referred to as the Budapest Convention, is the main multilateral legal framework for the fight against cybercrime. The Convention was concluded by the Council of Europe with the aim to protect society against cybercrime by adopting appropriate legislation and fostering international cooperation.

Whereas membership of the Council of Europe is limited, the Convention on Cybercrime is open for ratification by other countries upon invitation. The Convention has already been ratified by more than 50 countries, including the United States, Japan, Mauritius and Senegal.

a) Definitions of cybercrimes and penalties

The Convention obliges State Parties to adopt certain measures of substantive and procedural criminal law. Parties to the Convention are required to put in place measures to recognise, at least, the offences of illegal access to computer systems (Article 2), illegal interception of transmissions (Article 3), data interference (Article 4), system interference (Article 5) and misuse of devices (Section 6). Further offences that should at least be covered by the parties'

legal system are computer-related forgery (Article 7), computer-related fraud (Article 8), certain conduct relating to child pornography (Article 9) and infringements of copyright and related rights (Article 10).

Parties to the Convention are required to put in place effective, proportionate and dissuasive sanctions, which include deprivation of liberty (Article 13), but the exact required levels are not defined in detail. A broad jurisdictional basis must be put in place to ensure that these offences can be investigated and prosecuted (Article 11).

b) Procedural measures for the fight against cybercrime

State Parties also have to provide for procedural measures to allow authorities to order the expedited preservation of data (Articles 16 and 17), the production of data by persons or service providers (Article 18) and the search and seizure of data (Article 19). Real-time collection of traffic data (Article 20) and the interception of content data (Article 21) should also be provided for. Parties have to ensure that sufficient conditions and safeguards are put in place, also in relation to the protection of human rights (Article 15).

c) International cooperation in the fight against cybercrime

Finally, several measures to facilitate international cooperation have to be adopted by parties to the Convention, including measures based on mutual legal assistance (Chapter III). State Parties are also obliged to establish a point of contact that is available on a 24-hour, seven-day-a-week basis to facilitate assistance for the purpose of investigations and proceedings in relation to cybercrime (Article 35).

ii. The 2011 European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography

In 2011, the European Union adopted a Directive on combating the sexual abuse and sexual exploitation of children online and on child pornography. On the basis of the Directive, Member States are required to adopt provisions of substantive criminal law, including definitions of offences relating to the creation and distribution of child pornography. Related minimum and maximum penalties and certain administrative measures for the prevention of these offences are also included.

Amongst other things, the production of child pornography should be punishable by a maximum term of imprisonment of at least three years and the distribution, dissemination or transmission of child pornography should be punishable by a maximum term of imprisonment of at least two years.

iii. The 2013 European Union Directive on Attacks against Information Systems

In 2013, the European Union adopted a Directive on attacks against information system. On the basis of the Directive, Member States are required to adopt certain provisions of substantive criminal law, including definitions of offences relating to system and data interference. Related minimum maximum penalties and certain procedural and administrative measures to facilitate investigations of and the prosecution for these offences are also provided for in the Directive.

Amongst other things, the illegal access to information systems should be punishable by a maximum term of imprisonment of at least two years. Illegal interference with a computer system or computer data, where committed intentionally, should be punishable by a maximum term of imprisonment of at least three years.

iv. A proposal for a European Union Directive to combat electronic fraud

In 2017, a proposal for a European Union Directive was drawn up to make law enforcement action against online fraud and counterfeiting of non-cash means of payment more effective. The proposal builds on the 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment and includes provisions of substantive criminal law, related penalties and certain procedural and administrative measures.

Amongst other things, it is proposed that the transfer of money, monetary value or virtual currencies in order to make an unlawful gain for the perpetrator

or a third party by means of computer or data interference be made punishable by a maximum term of imprisonment of at least 3 years.

7.4 The legal framework for access to government information in Uganda

i. Provisions of international law

At international level, the freedom to seek, receive and impart information is recognised as a human right in the Universal Declaration of Human Rights (Article 19) and the International Covenant on Civil and Political Rights (ICCPR) (Article 19(2)), to which Uganda is a signatory State.

At regional level, the African Charter on Human and Peoples' Rights (ACHPR), also ratified by Uganda, acknowledges that every individual shall have the right to receive information (Article 9).

In 2002, the ACHPR adopted a Declaration of Principles on Freedom of Expression in Africa, which recognises that "public bodies hold information not for themselves but as custodians of the public good" and states that "everyone has a right to access this information, subject only to clearly defined rules established by law".

ii. Constitution of the Republic of Uganda 1995 as amended

The 1995 Constitution provides for a right of access to information in the possession of the government. Article 41(1) of the Constitution determines that every citizen has the right of access to information in the possession of the State or any other organ or agency of the State. The article provides for an exception to the right for where the release of information would be likely to affect the security or sovereignty of the State or interfere with the right to the privacy of any other person.

Article 41(2) of the Constitution instructs Parliament to adopt legislation that determines the types of information that are subject to the right of access to information and provides for procedures that should be followed to obtain access to the information.

According to Article 43(1) of the Constitution, the enjoyment of the rights and freedoms included in that chapter, including the right of access to information, shall not prejudice the fundamental or other human rights or freedoms of others or the public interest.

iii. Access to Information Act, 2005

The 2005 Access to Information Act has the objective to i) provide for the right of access to information pursuant to 41 of the Constitution, ii) prescribe the types of information that are referred to under that article and iii) prescribe the procedure for obtaining that information. Under Section 3 of the Act, its purposes are defined as, inter alia, the promotion of an efficient, effective, transparent and accountable government and to empower the public to scrutinise and participate in government decisions that affect them.

Section 5(1) of the Act defines that all citizens of Uganda have a right of access to information and records in the possession of the State or any public body, except where the release of the information is likely to affect the security or sovereignty of the State or the right to privacy of another person.

A public body cannot take into account any beliefs of what the reasons for making a request are when deciding to grant or deny access (Section 6).

i. Types of information that can be requested

The Act has a wide scope of application as Section 2(1) provides that it applies to all information and records of government ministries, departments, local governments, statutory corporations and bodies, commissions and other government bodies or agencies, unless they are specifically exempted by the Act. Throughout the Act, several different types of information are exempted from the right of access to information, including:

- Records of Cabinet and its commissions (Section 2(2)(a)),
- Records of court proceedings before the conclusions of the case (Section 2(2)(b)),
- Health records or other records the disclosure of

which would constitute an invasion of the right to privacy of a person (Section 21 and 26),

- Certain types of commercial information of a third party (Section 27),
- Certain types of confidential information that have been provided to the government body by a third party (Section 28),
- Information the disclosure of which could be expected to endanger the safety of a person or property (Section 29),
- Information the disclosure of which could affect the proceeding of law enforcement or legal proceedings (Section 30),
- Information that has been determined as privileged from production in legal proceedings (Section 31),
- Information the disclosure of which could affect the defence and security of Uganda or international relations (Section 32),
- Information relating to an ongoing government process that could be adversely affected by the information's disclosure (Section 33).

Nevertheless, the Act also provides for several conditions under which these types of information may still be disclosed, including where a person (Section 26(2)) or a third party affected (27(2), 28(2) and 31) has consented to the disclosure of the information or where the information is already publicly available.

In addition, notwithstanding the exemptions to the right of access to information provided for in the Act, information must be disclosed by a government body if it would provide evidence of a serious contravention of the law or an imminent risk to public safety, public health or the environment that would be greater than the harm to the interests protected under the exemptions provided for the in the Act (Section 34).

If a record contains certain information that cannot be provided under the exemptions to the right of access to information, other parts of that record to which access can be provided should still be disclosed (Section 19).

ii. Procedures for making a request for access to information

To facilitate requests for information, the Act assigns to chief executives of public bodies the role of information officers. These information officers have the obligation to ensure that records of the public body are accessible under the Act (Section 10). Information officers are obliged to compile a manual that describes the functions of the public body, its contact details and the procedures put in place to facilitate requests for access to information (Section 7(1)(a) to (j)). The manual has to be published at least once every two years (Section 7(2)). The information officer is also obliged to publish an overview once every two years of information of the public body that is available without the need to make a request for access to information (Section 8).

According to the Act, a request for access to information should be made in writing (Section 11(1), unless a person is not able to do so because of illiteracy (Section 11(3)). The request must include a specific description of the information requested as well as information about the person that makes the request (Section 11(2)).

iii. Procedures for public bodies to process a request for access for information

According to Section 12 of the Act, information officers have a duty to assist persons that want to make a request for access to information. They should also notify and give a person an opportunity to seek assistance and comply with any requirements before an information officer can refuse a request on the ground that it is not eligible.

Where a person has sent a request for access to information to a public body that does not have the information, the information officer is obliged to transfer the request to another public body that has the information (Section 13(1)). The information officer shall forward the request within 21 days of its receipt and shall inform the person that made the request upon the transfer.

Where the information to which access has been requested cannot be found or does not exist, and

where all reasonable steps to find the information have been taken, the information officer must inform the person that made the request (Section 14). The information officer will have to provide an overview of the steps that were taken to find the information.

Where the requested information is already expected to be made public imminently, the information officer may delay the disclosure of the information following the request for access to information (Section 15(1)). The information officer must notify the person, following which the person may indicate that there are reasonable grounds why the information should nevertheless be disclosed following the access to information request (Section 15(2)).

iv. Forms of access to information

Following Section 11(2)(b), a person making a request for access to information can specify which form of access is required. The following forms of access are recognised:

- In case the information is in written form, a copy of the information can be supplied, or arrangements can be made for inspection,
- If the information is not in written form,
    - reproductions of visual images or transcriptions may be supplied, or arrangements can be made for inspection or,
    - reproduction in the form of sound for the hearing of which arrangements can be made or written or printed transcriptions may be made,
- If the information is held on a computer, in electronic or machine-readable form, the information or a selection derived from that information may be provided access to by making use of computer equipment,
- If the information is available or capable of being made available in machine-readable form, by supplying a copy in that form, or
- In any other case by supplying a copy of the record.

v. Granting a request for access to information

The information officer who receives a request for access to information has the obligation to take a decision to grant or deny the access to information within 21 days (Section 16(1)) and to notify the person who made the request accordingly.

The original period of 21 days may be extended by another 21 days in case the request is for many documents, which requires a search for documents in different geographical locations or is consented to by the person who made the request (Section 17).

If the request is granted, the information officer may determine a fee that has to be paid (Section 16(2)) before the access to the information will be given (Section 20(1)) and the form in which the information will be provided.

vi. Refusing a request for access to information

If the request is refused, the information officer must notify the person who made the request of the refusal and of the reasons for the refusal (Section 16(3)(a)). Information must also be provided that the refusal of the request can be appealed before a court (Section 16(3)(c)). Where an information officer does not respond to a request for access to information within 21 days, the request is deemed to be refused (Section 18), which creates an opportunity to make an appeal before a court.

Where a request is refused, a person may lodge a complaint with a Chief Magistrate Court (Section 37). The decision of a Chief Magistrate Court can be appealed to the High Court (Section 38). Proceedings before these courts are civil in nature and the burden of proof lies with the party that is claiming it complies with the rules provided under the Act (Section 41). Where a person files a complaint regarding the decision of a government body to refuse a request, the burden of proof that rules were applied appropriately will thus lie with the government body.

Following a complaint, a Court may confirm, amend or set aside a decision of an information officer and

in that sense may require an information officer to grant or deny access to information (Section 42(b)). Interim measures, declaratory orders or compensation may also be provided for by the Court.

vii. Offences and penalties

Where a person destroys, damages, alters, conceals or falsifies information with the intent to deny right of access to information under the Act, this is considered as a criminal offence (Section 46).

Nevertheless, officers responsible for providing access to information are provided with protection against civil or criminal liability for any act or omission done in good faith in the exercise of the performance of any power or duty under the Act (Section 45).

viii. Powers to establish further rules

Under Section 47, the Minister is attributed the powers to make regulations that provide for further details for the application of the 2005 Access to Information Act. Amongst other things, it is defined that these regulations may be used to establish uniform criteria to be used by information officers, as well as for the developments of forms.

iv. Access to Information Regulations, 2011

The 2011 Access to Information Regulations provide for template forms that persons making a request for access to information should use, as well as templates for notifications that information officers need to provide following requests for access to information.

i. Additional procedures for requests

The Regulations also provide for procedures to be followed for requests for access to information, including where a request is made in electronic form. Following Regulation 3(2), a government body may provide a form in electronic format. Following Regulation 4(1), a requester may send a request for access to information by e-mail or in any other electronic form.

ii. Reasons to be provided by government organisations

Where a person asks for the information to be provided in electronic form and the public body decides it cannot comply, the public body must provide reasons why the information could not be provided in electronic form and has to provide the information in another form that can be used by a requester (Regulation 5).

iii. Criteria to decide on the format of information to be provided

Regulations 6 (a) to (h) of the Regulations provides criteria that public bodies need to consider where a request is made to supply the information in a specific format.

Where information is not available in the requested format, an information officer should consider the conversion of the information in the requested format while taking into account:

- the cost to the public body;
- the potential degradation of the record;
- if the requester is to be given access to only a part of a record;
- the facility with which the record may be provided in the format requested;
- the existence of the record within the public body in another format;
- the format that is useful to the requester;
- the possibility that the record can be converted to another format;
- that it is useful to the requester;
- the impact of the conversion on the operations of the public body;
- the availability of the required personnel and resources; and
- the availability of the necessary technology and equipment.

v. Case law

In Major General David Tinyefuza v. Attorney General ((Ruling) (Constitutional Petition No.1 of 1996)) [1997] UGCC 2 (5 March 1997), the Court determined that unfettered discretion of the State

to determine exceptions to the right of access to information is inconsistent with the rights as provided by Article 41 of the Constitution. A Court can determine whether a matter falls within the exceptions as provided by Article 41 of the Constitution, for which the State must provide evidence.

In Greenwatch (U) Ltd. v. Attorney General HCCS 139/2001, the Court, amongst other things, held that the mere fact that a company is a limited liability company is not sufficient to disqualify the company from the possibility of being a government agency for purposes of Article 41 of the Constitution. What constitutes a government body for the purpose of the application of the right of access to government information is thus to be considered broadly. In addition, the Court held that a corporate body could qualify as a citizen under Section 41 of the Constitution to have access to information in the possession of the State or its organs and agencies. Next to natural persons, legal persons could also thus enjoy the right of access to government information.

vi. Examples in other countries

Currently more than 90 countries worldwide and 11 countries in Africa have enacted legislation that provides for freedom of information and access to government information.

i. 2011 Open Government Declaration

On the basis of the 2011 Open Government Declaration, the Open Government Partnership (OGP) was established as a multilateral initiative to promote, amongst other things, the availability of information about governmental activities. More than 70 countries around the world are participating in the initiative. Although Uganda has demonstrated willingness to be eligible to join the initiative, it has not yet joined.

ii. 2009 Council of Europe Convention on Access to Official Documents

In Europe, the 2009 Council of Europe Convention on Access to Official Documents provides for a right of everyone, without discrimination on any ground, to have access, on request, to official documents held by public authorities (Article 2). Possible limitations should be set down in law, be necessary in a democratic society and be proportionate to the aim of protecting, amongst other things: national security, public safety etc. (Article 3). Public authorities are also obliged to, at their own initiative and where appropriate, to make public official documents (Article 10).

iii. 2003 European Union Directive on the Re-Use of Public Sector Information

In addition, the 2003 European Union Directive on the Re-Use of Public Sector Information focuses on the economic aspects of reuse of information. As a general principle, Member States are obliged to ensure that documents shall be reusable (Article 3). Through electronic means, where relevant and possible, public bodies are obliged to make documents available for reuse (Article 4). Member States are also obliged to make practical arrangements facilitating the search for documents available for reuse, accessible where possible and appropriate online and in machine-readable format (Article 9).

iv. 1991 Public Administration Act of the Netherlands

In the Netherlands, requests for access to government information can be made on the basis of the 1991 Public Administration Act. Anyone is entitled to make a request. Public bodies are held to comply with the request within four weeks, unless the publication of the information would harm national security or infringe on another person's privacy or commercial interest. Where the decision following the request is delayed beyond the deadline, the public body is held to pay damages for each day it is late beyond the deadline. When a request is honoured, the information is deemed to be publicly available. Certain costs can be charged by public bodies responding to a request, although copies of information of less than six pages are provided for free. The national government usually provides any information for free.

v. 2015 Reuse of Government Information Act of the Netherlands

In addition, the 2015 Reuse of Government Information Act provides that anyone can make

a request for the reuse of government-held information. The government of the Netherlands has provided a website that is used to proactively publish government information in a reusable format, i.e. data.overheid.nl

7.5 The legal framework for electronic government services in Uganda

i. The Constitution of the Republic of Uganda,1995 as amended: Functions of government

Functions of government are defined in the Constitution of the Republic of Uganda 1995,as amended. According to Article 189(1) of the Constitution of the Republic of Uganda, the functions and services that fall under the responsibility of the government are included in the Sixth Schedule to the Constitution.

The Sixth Schedule to the 1995 Constitution defines a range of functions and services for which the government is responsible, including taxation (4), passports and identity cards (5), transport and communications policy (16) making national plans for the provision of services and coordinating plans made by local governments (13).

These functions or services may be carried out by different government organisations, including national government agencies or, where provided for by law, by district councils or by the council of lower local government units (Article 189(2)).

i. Example: Uganda Citizenship and Immigration Control Act, Chapter 66

One example of statutory law that provides for the delivery of government services concerns the issuance of national passports and identity cards. The Uganda Citizenship and Immigration Control Act (Chapter 66) attributes the responsibility for the issuance of national passports and identity cards to the National Citizenship and Immigration Board. According to Section 16(3)(c) of the Act, the Board is responsible for the function of issuing Uganda passports and other travel documents. The Act establishes the function of a passport control officer that is responsible for issuing passports on behalf of the Board (Section 40).

Further rules for the manner, form and conditions for the delivery of the services are also provided for by the Act. In the Third Schedule to the Act, a standard template form is provided that should be used to apply for a passport (Section 40(5)). A number of requirements for the application of a passport are provided in Section 45 of the Act. Additional requirements regarding the form of applications can be provided for on the basis of Regulations that may be enacted by the responsible Minister (Sections 49 and 82).

ii. Example: Local Governments Act 1997, Chapter 243

Another example of statutory law that provides for the delivery of government services concerns the services delivered by local government councils. The 1997 Local Government Act attributes to local government councils the responsibility for all political and executive powers and functions within their area of jurisdiction (Section 30(1)(1)). The functions and services to be carried out by district councils are defined in Part II of the Second Schedule to the Act, including, for instance, the administration and licensing (Section 6) of trade licences (Section 5(n)). The functions and services to be carried out by urban councils are defined in Part III of the Second Schedule to the Act, including, for instance, the regulation and licensing of the use of the street for the purpose of carrying on any trade, business or profession (Section (3(1)).

ii. Electronic Transactions Act 2011

i. Aims and definitions

With the adoption of the 2011 Electronic Transactions Act, Parliament had the aim to, amongst other things, encourage the use of e-government services. According to Section 4(e), one of the objectives of the Act is to provide a legal and regulatory framework to, amongst other things, promote e-government services through electronic communications and transactions with the government, public and statutory bodies.

In Section 2 of the Act, e-government services are defined as a public service provided by computer means by a public body in Uganda.

Section 2 also defines a computer as any electronic device or a data storage facility or communications facility related to or operating in conjunction with such a device. Data is defined as electronic representations of information in any form. A data message is defined as 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.

According to Section 2, a 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.

ii. Types of electronic government services

Section 22 of the Act identifies three forms of delivery of e-government services, including that:

i. where a law provides that a public body may accept the filing of a document or requires that a document is created or retained, that public body may accept that document in electronic form,

ii. where a public body may issue a permit, licence or an approval, that public body may issue the permit, licence or approval in electronic form, and that

iii. where a public body may provide for the making of a payment, that public body may make or

iv. receive payment by electronic means.

iii. Specification of conditions for electronic services

Where a public body is offering e-government services as defined in Section 22, it may provide for a number of specifications regarding the application and delivery of the service.

Pursuant to Section 23(1) of the Act, the public body may 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 the 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 message or a payment, and

g. any other requirements in respect of the data message or payment.

Section 23(2) also indicates that a generic service provider is preferred where it is specified that an authentication service provider is to be used pursuant to Section 23(1)(e).

According to Section 23(1), a public body may notify these specifications in the Gazette.

iv. Electronic Transactions Regulations 2013

Regulation 8(1) of the Regulations obliges a public body to seek the approval of the Minister of ICT and National Guidance before giving notice of specifications for the delivery of e-government services on the basis of Section 23 of the 2011 Electronic Transactions Act.

Regulation 8(2) of the Regulations obliges the Minister of ICT to confirm that the specifications for the delivery of e-government services for which approval is sought are (a) consistent with the 2011 Electronic Transactions act, (b) are required by the 2011 Electronic Signatures Act where they involve the need to attach a signature to a data message and (c) not stifling the delivery of services to the public and promote the use of electronic communications.

v. National Information Technology Authority Uganda Act 2009

With the 2009 National Information Technology Authority Act, Parliament provided for the establishment of NITA-U, as well as for its objectives, functions, composition, management and finances and certain other related matters.

In Section 3(1) of the Act, NITA-U is established as an autonomous body. NITA-U is established as an agency of government under the general supervision of the responsible Minister (Section 3(3)).

In Section 4 of the Act, the objectives of the Authority are defined as, amongst other things, to (a) provide high quality information technology services to government, (b) 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 and (c) provide guidance and other assistance as may be required to other users and providers of information technology.

In Section 5 of the Act, the functions of the Authority are defined as, amongst other things, to (b) identify and advise the government on all matters of information technology development, utilisation, usability, accessibility and deployment, including networking, systems development, information technology security, training and support, (c) co-ordinate, supervise and monitor the utilisation of information technology in the public and private sectors and (h) promote and provide technical guidance for the establishment of e-government, e-commerce and other e-transactions in Uganda.

Section 39(1) of the Act authorises the Minister to make regulations to give effect to the provisions of the Act. According to Section 39(2), these Regulations may also provide for penalties in cases where the provisions as part of these Regulations are contravened.

iii. The National Information Technology Authority-Uganda (E-Governement) Regulations, 2015

With the National Information Technology Authority-Uganda (E-Government) Regulations 2015, the Minister of ICT provided further rules for the implementation of the 2009 National Information Technology Authority Act.

i. Aims and definitions

In Regulation 2 of the Regulations, e-government is defined as the use of information and communication technologies ICT to deliver public services in a convenient, efficient customer-oriented and cost-effective way. Integrated service delivery is defined as the provision of government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction. A government web portal is defined as a website or interface that offers a range of resources and services, including email, a search engine and an integration of websites.

In Regulation 3 of the Regulations, the objectives of the Regulations are defined as:

a) to promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens,

b) to promote the use of the internet to provide increased opportunities for citizen participation in government,

c) to promote interagency collaboration in providing public services by consolidating, rationalising and integrating related functions and using internal e-government processes to improve the service to citizens, efficiency and effectiveness of the processes,

d) to promote the use of the internet and other appropriate technologies within and across government agencies in providing government information and services,

e) to reduce the cost and burden for government and business entities in the provision of public services,

f) to improve access and sharing of government information and services.

In Regulation 4 of the Regulations, the Authority is charged with the responsibility to promote the establishment and maintenance of interoperable information systems with public bodies.

ii. Internet policies and infrastructure for e-government services

Regulation 5(1) of the Regulations obliges the Authority to establish, for the purpose of the promotion of e-government services, a national data centre for the provisioning of (a) hosting services, (b) data centre services and (c) disaster recovery services (Regulation 5(2)). The national data centre is to be linked with other data centres established by public and private bodies (Regulation 5(3) and (4)).

The Authority is also tasked to prescribe user rights and access levels, which have to be made applicable to the national data centre (Regulation 5(5)). User rights and access levels of other data centres established by public and private bodies have to be described by those other public and private bodies (Regulation 5(6)).

With Regulation 9(1), public bodies are obliged to develop an internet policy that provides for the use of computers, e-mail and the internet. Pursuant to Regulation 9(2), public bodies are required to provide for tools to enforce their internet policy.

In Regulation 10(1) public bodies are obliged to use a National Data Transmission Backbone (NBI) and Electronic Government Infrastructure (EGI) for the processing of government data, internet access and the delivery of voice services to support the collaboration between government organisations. The Authority is tasked with connecting public bodies to the National Data Transmission Backbone (NBI) (Regulation 10(2)). Public bodies are obliged to pay for the connection to and the use of the National Data Transmission Backbone (NBI), for which the Board of the Authority may set the rates (Regulation 10(3)).

The Board of the Authority may set and charge public bodies with rates for the connection of public bodies to the National Data Transmission Backbone (NBI). The Board of the Authority should consider market rates when setting rates for the connection of public bodies to the National Data Transmission Backbone (NBI) (Regulation 10(4)).

iii. E-Government websites and a government web portal

With Regulation 6(1) of the National Information Technology Authority, Uganda (E-Government) Regulations 2015, public bodies are obliged to establish and maintain a website to facilitate the use of e-government services. The website should be interactive (Regulation 6(2)) and should be updated regularly (Regulation 6(6)). The Authority is tasked with monitoring compliance with this obligation (Regulation 6(7)).

Where a public body fails to establish a website within six months from the entering into force of the Regulations, the Authority is obliged to establish a website for the public body (Regulation 6(3)). The public body will be charged for the costs of the establishment of the website by the Authority (Article 6(4)). In this situation, the public body is required to provide the information necessary for the establishment of the website by the Authority (Regulation 6(5)).

Regulation 7(1) of the Regulations provides detailed requirements for websites of public bodies, including that they need to state: (a) the name of the public body, (b) the vision, mission, mandate and the goal of the public body, (c) the national

coat of arms and the logo of the public body, (d) the services rendered by the public body, (e) the laws, policies, codes, standards, guidelines relating to the public body, (f) the contact details of the public body, including a site map to enable location of the public body and (g) the information about the organisational structure of the public body.

In addition, it is provided that the website needs to be established within the.co.ug domain (Regulation 7(2)), needs to have a search capability (Regulation 7(3)) and needs to be updated regularly (Regulation 7(4)).

The Authority is also required to establish and maintain a government web portal (Regulation 8(1)), which needs to contain all information relating to government services (Regulation 8(2)) and needs to be linked to the websites of public bodies that provide public services (Regulation 8(3)). In addition, the government web portal needs to be (a) interactive and (b) include services related to citizens, businesses and government (Regulation 8(4)).

iv. Information security standards for e-government services

To provide for information security, the Authority is obliged to establish a public key infrastructure (PKI) for e-government services (Section 11(1)) that is in line with the 2011 Electronic Signatures Act (Section 11(2)).

In addition, Section 12 obliges public bodies to (a) develop and enforce necessary security measures to safeguard the information collected or used for e-government services from unauthorised disclosure and (b) take all reasonable steps to ensure that every officer of the public body concerned with delivering services or collecting, posting or disseminating information or services is aware of and complies with the security measures regarding the management and protection of information.

v. Processing of personal information for e-government services

In Regulation 13(1) of the National Information Technology Authority, Uganda (E-Government) Regulations 2015, it is determined that both public and private bodies may share information for the provisioning of e-government services. The public and private body may prescribe the level of user rights and access rights for these purposes (Regulation 13(2)).

With Regulation 14, the use of personal information by public bodies is restricted by providing that personal data is (a) kept and used only for specified and lawful purposes for which the data has been collected and processed and (b) not kept for longer than necessary for the purposes for which the data has been collected and processed.

With Regulation 15(1), public bodies are prohibited from disclosing information that they obtained for the purpose of the delivery of e-government services without the consent of the person to whom the information relates.

Where the information is nevertheless disclosed without the consent of the person to whom the data relates, Regulation 15(2) provides for the criminal liability of the responsible public body or officer of the public body. The responsible public body or the officer of the public body may be liable to a maximum penalty constituting:

a) a fine of UGX 960, 000 and/or imprisonment of two years in case of a first offence,

b) a fine of UGX 1,440,000 and/or imprisonment of three years in case of a second or subsequent offence,

c) an additional fine of UGX 200,000 for each day on which the offence continues in case of a continuing offence.

vi. Example: the Traffic and Road Safety (Driving Permits) Regulations, 2005

In addition to the general rules on e-government, certain aspects of the delivery of electronic government services may also be regulated by means of specific regulations. One example of statutory law that provides for specific rules for the delivery of e-government services is the 2005 Traffic and Road Safety (Driving Permits) Regulations.

On the basis of the Traffic and Road Safety Act 1998, the Minister responsible for communications provided for the Traffic and Road Safety (Driving

Permits) Regulations 2005, to, amongst other things, introduce a computerised driving permit system.

In Regulation 2 of the Regulations, a computerised driving permit is defined as the type of driving permit that is machine-readable and whose features are as specified in the First Schedule to the Regulations.

In Regulation 3(1) of the Regulations, a computerised driving permit issue and management system is established (Regulation 3(2)) to replace the non-computerised driving permit system.

The form of the computerised driving permit is defined in the First Schedule to the Regulations (Regulation 4(1)) and the form for applying for a computerised driving permit is defined in the Second Schedule to the (Regulation 5(2)).

iv. Court decisions

No court decisions have been taken in relation to the delivery of e-government services.

v. Examples from other countries

i. Estonia

In the European Union, the 2017 Digital Progress Report identifies Estonia as the leading country for e-government service delivery. In Estonia, citizens can vote electronically in elections, file for income tax returns online and sign legally-binding contracts from anywhere in the world or open a bank account via video call. An electronic state portal allows citizens to see their own government-held records, check who has reviewed data and, in some cases, set limits to access.

The delivery of e-government services in Estonia is regulated by a legislative framework consisting of different Acts providing for the recognition of electronic signatures, and the protection of security, privacy and personal data. In addition, the 2000 Public Information Act establishes a system of government databases as part of a comprehensive state information system. The 2008 State Information Management System Regulations provide for further implementation on the basis of which government organisations can deliver public services.

ii. Denmark

In Denmark, the government aims for 80 per cent of all written communications between citizens and government to be in electronic form. Therefore, businesses and citizens are required to make use of a number of electronic services offered by the government. Based on the 2012 Digital Post Act, the Danish government established a mandatory digital mailbox for every citizen aged 15 or above, as well as for legal persons, which government organisations may use for their communications with those citizens. Certain categories of citizens or legal persons may be exempted from mandatory access, although they are allowed to voluntarily opt in.

Additional legislation enacted in 2012 introduced mandatory digital self-service for citizens. The Danish government determined a number of government services that can only be obtained by citizens or businesses when applied to using an electronic self-service solution, including for applications for admission to schools, applications for a passport and applications for adoption.

On that basis, a government body may decide not to process an application made in another form. In special circumstances, an application may be exempted from the obligation to make the request in electronic form, for example where the applicant does not have the skills or resources to do so. In those cases, government organisations are required to support applicants.

Design by: Revolve Tack Ltd
www.revolvetack.org

"Making access to justice and the Law readily available to 50 million people across Africa by 2030."

- the BarefootLaw BHAG

Call us Today: +256 392 177 405

 *barefootlawUG*

 *barefoot lawyers-uganda*

 *barefoot-law-uganda*

 *www.barefootlaw.org*