# UGANDA LAW REFORM COMMISSION

# A STUDY REPORT ON ELECTRONIC TRANSACTIONS LAW

**KAMPALA, UGANDA**

**2004**

**(LAW COM PUB. NO. 10 of 2004)**

## LOCATION.

The Uganda Law Reform Commission premises are located at –
Workers House, 8th Floor,
Plot 1, Pilkington Road,
Kampala, Uganda.

**The address for correspondence is –**

Uganda Law Reform Commission
P. O. Box 12149,
Kampala, Uganda

**Telephone:** +256-41-341138/ 341083/346200-2

**Fax:** +256-41-254869

**E-mail:** lawcom@infocom.co.ug
ulrc@ulrc.go.ug

**Web:** www.ulrc.go.ug

## FOREWORD

The Government of Uganda, basing on the findings of the commercial justice reform programme baseline study and in consultation with stakeholders developed a four year detailed strategy for the reform of the commercial justice system. The strategy focused on four essential areas; the commercial courts, the commercial registries, the legal profession, the commercial regulatory environment and commercial laws.

In furtherance of the programme, the Uganda Law Reform Commission (ULRC) with the support of the Justice, Law and Order Sector proposed to reform key selected commercial laws that affect the basic operating environment of businesses to promote private sector business operations.

It should be noted that the commercial justice system in Uganda has fared badly because commercial life has been encumbered for several decades. This has caused inadequacy in Government delivery and led to the slow development of the private sector.

The commission, having appreciated the fact that law cannot be adequately reformed without appreciating the political, cultural and socio-economic context in which it operates and as a measure towards operationalising the people's constitutional right to participate in the law making process carried out wide consultations with the relevant stakeholders and individuals with a wide range of expertise on policy and business issues. As a result of these involving endeavours, many proposed Bills have been drafted.

The commission appreciates the responses from the participation of all stakeholders and is indeed confident that the recommendations contained in this report and Bill will, due to the fact that the public have had an input, be easily enforceable in our society.

The commission acknowledges with special appreciation the work of the consultants, Nyanzi, Kiboneka & Mbabazi Advocates and the financial support given through the Justice Law and Order Sector.

Special thanks go to the various stakeholders from the judiciary, the Uganda Law Society, academia, the business community and all institutions and individuals who contributed by participating in the consultations carried out by the commission.

**Professor Joseph M.N. Kakooza,**
**Chairman, Uganda Law Reform Commission**

TABLE OF CONTENTS

## ACRONYMS/ABBREVIATIONS

| | |
|---|---|
| CJRP | Commercial Justice Reform Programme. |
| GOU | Government of Uganda. |
| JLOS | Justice Law and Order Sector. |
| LC | Local Council. |
| PEAP | Poverty Eradication Action Plan. |
| PERD | Public Enterprise Reform and Divestiture. |
| PMA | Plan for Modernisation of Agriculture. |
| ULRC | Uganda Law Reform Commission. |
| URA | Uganda Revenue Authority. |
| IT | Information Technology. |
| ICTS | Information and Communications Technologies. |
| EDI | Electronic Data Interchange. |
| VAN | Value Added Networks. |
| TICP | Transmission Control Protocol. |
| IP | Internet Protocol. |
| ATM | Automatic Teller Machine. |
| EFT | Electornic Funds Transfer. |

# LIST OF ACTS, LEGISLATION OF OTHER COUNTRIES, INTERNATIONAL CONVENTIONS AND INSTRUMENTS.

## List of Acts.

1. Business Names Registration Act, Cap.109.
2. Copyright Act, Cap.215.
3. Crimmal Procedure Code Act, Cap. 116.
4. Evidence Act, Cap. 6.
5. Income Tax Act, Cap. 340.
6. Magistrates Courts Act, Cap. 16.
7. Patents Act, Cap. 216.
8. Penal Code Act, Cap. 120.
9. Sale of Goods Act, Cap. 82.
10. Trademarks Act, Cap. 217.

## List of legislation of other countries, international conventions and instruments.

1. Berne Convention for the Protection of Literary and Artistic Works.
2. Computer Misuse Act, Cap. 50A, Singapore.
3. Computer Misuse Act, 1990, United Kingdom.
4. Crimes Act, 1914,Australia.
5. Data Protection Act, 1998, United Kingdom.
6. Defamation Act, 1996, UK.
7. Electronic Communiations and Transactions Act, No. 25 of 2002, South Africa.
8. Internet Tax Freedom Act, 1998.
9. Model Interchange Agreements.
10. United Nations Convention on Contracts for the International Sale of Goods (1980) (CISG).
11. World Intellectual Property Organisation Dispute Resolution Rules.
12. World Intellectual Property Organisation Performances and Phonograms Treaty (WPPT).

# PREFACE

## Establishment of the Uganda Law Reform Commission.

The Uganda Law Reform Commission was established in 1990 by the Uganda Law Reform Commission Act, Cap. 25. Prior to this enactment, law reform was the responsibility of the department of law reform and law revision of the Ministry of Justice, which had been set up in 1975. In 1995, with the promulgation of the Constitution, the commission became a constitutional commission by virtue of article 248 of the Constitution.

## Composition of the commission.

Under section 3 of the Uganda Law Reform Commission Act, Cap. 25, the commission consists of a chairman and six other commissioners, all of whom are appointed by the President on the advice of the Attorney General.

The chairperson and four of the commissioners are lawyers who are retired or sitting judges of the Court of Appeal or High Court of Uganda; or are lawyers qualified to be appointed as judges of the Court of Appeal or High Court of Uganda; or are senior practising lawyers or senior teachers of law at a university or similar institution of law in Uganda. The remaining two commissioners, as set out by section 4(2), are non-lawyers but persons who have distinguished themselves in disciplines relevant to the functions of the commission.

Additionally, section 12 empowers the Attorney General, on the advice of the commission, to appoint experts or consultants in any specific aspect of law reform undertaken by the commission.

The commission is serviced by a secretariat composed of an executive secretary and other staff. The commission has three departments which are: the law reform department, the law revision department and the department of finance and administration. The staff of the commission consists of lawyers and non-lawyers appointed by the Attorney General from among persons who are either public or non-public officers.

## Functions of the commission.

The main function of the commission as set out under section 10 of the Uganda Law Reform Commission Act, Cap. 25 is to study and keep under constant review the Acts and other laws of Uganda with the view to the making of recommendations for their systematic improvement, development, modernisation and reform with particular emphasis on-

(a) the elimination of anomalies in the law, the repeal of obsolete and unnecessary laws and the simplification and translation of the law;

(b) the reflection in the laws of Uganda of the customs, values and norms of society in Uganda as well as concepts consistent with the United Nations Charter for Human Rights and the Charter of Human and Peoples' Rights of the African Union;

(c) the development of new areas in the law by making the laws responsive to the changing needs of the society in Uganda;

(d) the adoption of new or more effective methods or both for the administration of the law and dispensation of justice; and

(e) the integration and unification of the laws of Uganda.

**Powers of the commission.**

In the performance of its functions, the commission may-

(a) receive, review and consider any proposals for the reform of the law which may be referred to it by any person or authority;

(b) prepare and submit to the Attorney General, from time to time, for approval, programmes for the study and examination of any branch of the law with a view to making recommendations for its improvement, modernisation and reform; and those programmes shall include an estimate of the finances and other resources that will be required to carry out any such studies and the period of time that would be required for the completion of the studies;

(c) undertake, pursuant to any such recommendations approved by the Attorney General, the formulation of draft bills or other instruments for consideration by the Government and Parliament;

(d) initiate and carry out, or, with the approval of the Attorney General, direct initiation and research necessary for the improvement and modernisation of the law;

(e) provide, at the instance of the Government, to Government ministries and departments and other authorities concerned, advice, information and proposals for reform or amendment of any branch of the law;

(f) encourage and promote public participation in the process of lawmaking and educate and sensitise the public on lawmaking through seminars, publications and the mass media; and

(g) appoint or empanel committees, in consultation with the Attorney General, from among members of the commission, or from among persons outside the commission, to study and make recommendations to the commission on any aspect of the law referred to the committees by the commission.

**Profile of the commission.**

**Vision.**

The vision of the commission is to promote, in Uganda, a legal system with just and up-to-date laws, easily accessible to all.

**Mission statement.**

To contribute to sustainable development, an equitable and just legal system through revision, harmonisation, development and reform of the law.

**Values of the commission.**

The commission-

(a) seeks to be impartial at all times in all dealings with its clients,

(b) endeavours to operate with integrity and in a professional way,

(c) is committed to equity and pragmatic diversity in the workplace,

(d) respects and values the contribution of the people, and

(e) endeavours to communicate consistently and effectively with its stakeholders in all its projects.

**Slogan.**
"Law reform for good governance and sustainable development".

**Justification for legal reform.**

The Ugandan society, like all societies, is in a constant state of change caused by political, social and economic factors yet there have been few changes in the law since the inception of English law in Uganda in 1902. In addition, there are emerging cultural patterns and gender relations, new Government policies such as decentralisation, privatisation, economic liberalisation, poverty eradication, private sector development and the modernisation of agriculture. However, there have been few changes in the law yet the law, at any given time, has to effectively respond to social changes and to the aspirations of the people. There is need for wide research including the need for extensive consultations with stakeholders when proposing reforms in any area of the law.

**Current members of the Uganda Law Reform Commission.**

**1. Professor Joseph Moll Nnume Kakooza.**

Professor Kakooza is a holder of the degrees of B.C.L. and LL.B. of the National University of Ireland, Dublin; LL.M. (Harvard); M.Litt. and a Postgraduate Diploma in Anthropology of the University of Oxford; Certificate in International Relations, of the University of Oslo; Barrister-at-Law, of the Inner Temple, London and Advocate of the High Court, Uganda.

Professor Kakooza served as a lecturer at the Faculty of Law, University College, Dar-es-Salaam, as a senior lecturer and founding head (later twice dean) and finally Professor of Law at Makerere University. He has been a visiting scholar at Harvard Law School; guest lecturer at the college of criminal justice, Northeastern University Boston and visiting professor, College of Law, University of Florida. He is currently teaching law at Kampala International University and medical jurisprudence in the Faculty of Medicine, Makerere University, part-time. He is widely published, particularly in criminal justice and family law and he is a member of many professional organisations. He is listed in the international publication of ***WHO IS WHO in Education*** and was given the award of ***MAN OF THE YEAR, 2003***, by the American Biographical Institute, Inc.

Professor Kakooza has, among other spells of public service, served as Ag. Judge of the High Court of Uganda, Ag. Solicitor General, President of Uganda Industrial Court; and commissioner of law reform. He was acting chairman of the commission from 2000 to 2002 when he became the chairman.

He has been in charge of the Domestic Relations Law Project and Labour Laws Project. He is currently in charge of the Intellectual Property Law Project, the Reform of the Accountants Act Project, the Living Law Journal Project, the Sentencing Legislation Reform Project and Community Law Reform Programme.

**2. Ms. Percy Night Tuhaise.**

Ms. Tuhaise is a holder of the degrees of LL.B and LL.M of Makerere University, Kampala; a Postgraduate Diploma in Legal Practice of the Law Development Centre, Kampala. She also holds various certificates in human rights teaching and research (Ottawa Canada 1991), (Strasbourg, France, 1995). She is the deputy director and a principal lecturer of the Law Development Centre, Kampala. She is also an advocate of the High Court of Uganda. Ms Tuhaise was appointed a part-time commissioner in 1995. She assisted commissioner Kibuka in the Rape and Defilement Project. She has been in charge of the Business Associations cluster of the Commercial Law Project and Succession Law Project, and is currently in charge of the Codification of the Contracts Law Project under the Commercial Law Project II and Simplification of the Penal Code Act

**3. Mr John Mary Mugisha.**

Mr. Mugisha holds the degree of LL.B of Makerere University and a Postgraduate Diploma in legal practice, LDC. He was appointed a part-time commissioner in 1999. He is a principal lecturer at the Law Development Centre, Kampala and an advocate of the High Court of Uganda. Mr. Mugisha is a former President of Uganda Law Society; Vice President of the East African Law Society; lead counsel for the Constitutional Review Commission; and deputy secretary general in charge of Eastern Africa, International Bar Association (IBA). He is also a member of the Law Council representing the Uganda Law Society. Mr. Mugisha has been the commissioner in charge of Secured Transactions and Fair Trade Clusters of the Commercial Law Reform Project. He is currently in charge of subsidies and countervailing measures, under the Commercial Law Reform Project II and Trial Procedures Reform Project under the Criminal Law Reform Project I.

**4. Dr. Lillian Tibatemwa-Ekirikubinza.**

Dr. Tibatemwa-Ekirikubinza is a holder of a PhD in law from the University of Copenhagen, Denmark; an LLM in Commercial Law from the University of Bristol, UK; an LL.B (Hons) degree from Makerere University and a Postgraduate Diploma in Legal Practice from the Law Development Centre, Kampala. She was the deputy dean of the Faculty of Law, Makerere University and is currently the Deputy Vice Chancellor in charge of academic affairs at Makerere University and a part time commissioner of the commission since 1999.

Apart from being a commissioner of the Uganda Law Reform Commission where she has been in charge of various projects namely: the Insolvency Cluster of the Commercial Law Reform Project I, the Domestic Violence Project, the E-Commerce, Computer Crime and E-Evidence Project under the Commercial Law Reform Project II. Dr Tibatemwa-Ekirikubinza has also held other positions of responsibility among which are: board member of the Uganda National Bureau of Standards, member of the academic board of Makerere University Business School, Nakawa and a complimentary member of the British Institute of International and Comparative Law.

**Former members of the Uganda Law Reform Commission.**

**1. Justice Sir Harold G. Platt.**

Justice Sir Harold Platt is a holder of MA of Oxford University after his first degree in India. He retired but was actively involved in various aspects of the legal field. He served in various capacities in East Africa including: Chairman Uganda Law Reform Commission 1994 -2000, where he was in charge of the Commercial Law Project among others; judge of the Supreme Court of Uganda 1989-1994, judge of the High Court and Court of Appeal Kenya 1968-1989; Government service, provincial magistrate Tanzania1962-1972, colonial legal service Tanganyika 1954 -1962 and in legal practice 1951-1954. Justice Sir Harold Platt was called to the Bar in 1952 after serving in the royal air force from 1942-1947.

**2. Professor Eric Paul Kibuka.**

Professor Kibuka holds a B.A and PhD of Makerere University. He was a director of the United Nations African Institute for the Prevention of Crime and Treatment of Offenders, Kampala. He was appointed a part-time commissioner in 1995. He is a retired lecturer of sociology at Makerere University. Professor Kibuka was in charge of the Rape and Defilement Law Project. He was also in charge of the Decriminalisation of Petty Offences Project as well as the Contracts Law Project.

**3. Ms. Hilda A. Tanga.**

Ms. Tanga is a holder of a B.A degree in education and a postgraduate diploma in Human Resources Management. She has been a graduate teacher at Kololo S.S.S; lecturer in business communication at the National College of Business Studies; Ag. registrar and deputy academic registrar at the Uganda Polytechnic Kyambogo. Ms. Tanga has also been an adhoc consultant with Management Training and Advisory Centre (MTAC) on management and training of trainers. She is currently an examiner with the Uganda National Examinations Board (UNEB) and National Business Examinations Council (Nakawa).

**4. Ms. Filda Mary Lanyero Ojok.**

Ms. Mary Lanyero was a senior lecturer and dean of the Faculty of Arts, Institute of Teacher Education, Kyambogo. She is also involved with various non-governmental organisations in various capacities. Ms. Lanyero holds certificates from the American Studies Winter Institute, USA. She holds a masters degree in international relations, Carleton University Ottawa, Canada and a B.A of Makerere University majoring in history and literature in English. Ms. Lanyero was a teaching assistant, University of Carleton, Ottawa Canada.

**5. Mr. Francis Butagira.**

Mr. Butagira was appointed commissioner on 22nd January 1996. He holds the degrees of LL.B Makerere University and LL.M (Harvard). He is an advocate of the High Court of Uganda and former principal lecturer at the Law Development Centre.

**6. Mr. Richard Aboku Eryenyu.**

The late Richard Aboku Eryenyu served as commissioner from 19th January 1996 until his death on 7th April 1999. He was an LL.B graduate of Makerere University and a chief magistrate.

# EXECUTIVE SUMMARY.

## 1. Background.

Electronic commerce (hereinafter referred to as e-commerce) is doing business electronically through an electronic medium where electronic data is interchanged between parties through information intermediaries on an information technology network. The convergence of technologies in telecommunications, broadcasting and computers has created a new market place with a two-way flow of information involving the processing and transmission of data, including text, sound and video in diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and after-sall servise. The new market place involves both products (e.g. consumer goods, specialized medical equipment) and services (e.g. information services, financial and legal services); traditional activities (e.g. healthcare education) and new activities (e.g. virtual malls).

Information Techinology (IT) networks have thus become the primary vehicle for consumer purchases, mass marketing, financial transaction, and on-line information, entertainment and government services. Electronic commerce is entirely a phenomenon of the technological revolutions in computers and information systems, telecommunications, banking systems postal and generally communications or delivery services. E-commerce is enabled by the use of Information and Communications Technologies (ICTs), which have led to the compression of time and space. Underpinning ICTs is digitisation that has enabled the convergence of telecommunications, broadcasting, information technology and publishing. Access to ICTs is the most basic prerequisite for e-commerce.

The Internet has facilitated the establishment of a "borderless" environment for communications and the electronic delivery of certain services. Convergence of technologies is the major driving factor that contributes to the exponential growth of electronic commerce. Convergence goes beyond the use of technology to develop new products and services and is seen as a vehicle to improve the quality of life of society in Uganda and the rest of the world. Convergence will open new opportunities for all as everyone gains equal access to information and the global markets. Small business will be able to compete on an equal footing with big business. What is needed is an environment that is conducive to conducting business and sharing information with confidence.

Electronic commerce has expanded from the closed world of business-to-business transactions between known parties to encompass a complex web of different activities involving large numbers of individuals, many of whom will never meet each other. This has the advantage of reducing the cost of transactions, reducing barriers to entry into business and in some cases removing the necessity for a physical presence in any particular market, as well as providing improved access to information to consumers.

When communications networks first became available, entrepreneurs were quick to recognise their value and use them to create business opportunities. Recent advances in telecommunications and computer technologies have moved computer networks to the centre of the international economic infrastructure. Among the principal activities that can be identified as contributing to global e-commerce are –

(a) government services and information;

(b) business-to-business wholesale and retail services and sales;

(c) business-to consumer (and consumer-to-consumer) retail sales and transactions;

(d) financial services and transactions;

(e) subscription and usage-based telephony, online and internet access services;

(f) subscription or transaction-based information services and software sales;

(g) advertising and marketing services; and

(h) ancillary functions contributing to business or commercial activities.

Electronic commerce presents important new opportunities as it diminishes existing advantages of cost, communication, and information, and can create huge new markets for indigenous products and services. Electronic commerce has created a brand new marketplace in which we must operate. It is, in many ways, a marketplace without conventional rules; a marketplace, indeed, that challenges many of our preconceived notions and practices. It is also a marketplace that may seem to defy regulation.

Doing business over the internet may seem to raise breathtakingly novel issues in business law, but the law of electronic commerce is actually as old as the telegraph. After the telegraph entered into widespread use in the United States, the first case was litigated in which a party tried to avoid liability by claiming that an agreement reached by an exchange of telegrams could not constitute a valid and binding contract (Wright and Winn, 1998). The courts in the United States and elsewhere in the world rose to the challenge to look beyond form and evaluate the substance of the transaction, whether the new form of agreement was telegram, telex, fax or email. The question how the law will adapt to the new business realities of internet electronic commerce can best be answered by looking at how the law adapted to earlier versions of electronic commerce - in particular, electronic data interchange or electronic contracting conducted over closed, proprietary networks, electronic funds transfer systems used by banks, and electronic settlement and clearing systems used in Wall Street.

An audit of all the legal issues raised by doing business from an internet site might include not just a review of commercial law issues but also patent, trademark and copyright law issues; advertising and consumer protection regulations including privacy law issues; antitrust and deceptive trade practices law issues; record retention and email policies; the design of security procedures and access controls; and tax law issues. While many of the issues raised by internet electronic commerce closely resemble issues raised by earlier generations of technology such as telexes and faxes, what may be unprecedented is the degree to which electronic commerce is changing some of the basic principles upon which business administration has been based for decades. The volume and magnitude of changes in business practice that are occurring now as a result of adopting electronic commerce systems are putting tremendous pressure on traditional commercial law doctrines to adapt and evolve. Legal institutions can respond to these pressures in a variety of ways, requiring an analysis of the costs and benefits associated with different techniques for adapting law to new business practices.

The most elementary way for business parties to adapt commercial law to new circumstances is through the use of contracts. Parties can depart from the terms of current standard form contracts to write new contracts describing new transactions and allocating new risks between the contracting parties. Failed transactions that result in litigation produce reported legal opinions that become case law, which in turn help parties to predict how effective their new contract terms are at regulating innovative business practices. The process of building new law through precedent can be slow and problematic as the outcome of litigation is always somewhat uncertain. As contracts become more innovative, their enforceability becomes less predictable as a result.

When the parties are no longer confident that their contracts will produce predictable legal outcomes, the need to enact statutes to resolve the uncertain issues inevitably arises. Under ideal circumstances, commercial law statutes should be reformed in response to significant changes in established business practices to reduce uncertainties that arise under existing law. Innovators start the process by using contracts to assign rights and responsibilities among themselves. Having lawyers individually negotiate and draw up contracts can be an expensive proposition, especially if the business party has to educate the lawyer about the basic business model the parties have developed as part of the drafting process, but it may be the only practical way for the

parties to reduce some of the legal uncertainties arising out of innovative business practices. As people gain experience and business practices that were once considered innovations become routine, parties to commercial transactions can standardize the terms of their contracts, minimizing or eliminating the role of lawyers in individual transactions.

When contract terms and business practices become very standard and routine, commercial statutes can be revised to incorporate what can be thought of as default terms based on these standard contract terms. If the parties to a commercial contract fail to specify all the operative terms of their agreements, then commercial law can act as a gap-filler, providing missing terms that should be substantially the same as those the parties would have agreed to if they had thought about the issue. In this manner, commercial law supports routine business practice and eliminates uncertainty among parties to a transaction without requiring lawyers to advise the parties on each contract.

Not all commercial law issues can be resolved through the slow accumulation of business custom and practice. Some issues, such as consumer protection issues, are generally resolved by the legislature acting to mandate what business parties must do in order to have legally enforceable agreements or to avoid legal sanctions. Regulatory approaches to commercial law may have a shorter incubation time than "freedom of contract" approaches that defer to standards chosen by commercial parties themselves, and often have less predictable outcomes for affected businesses as a result. Regulation often works best when it rectifies market failures, such as those caused by information asymmetries or unequal bargaining power in consumer transactions. For seeing/predicting market developments is hard enough for entrepreneurs, so the odds are generally even worse that legislators will correctly guess the outcome of current business innovations. Once an inaccurate prediction about what people in business will want to do in the future is locked into a statute, the law may become simply irrelevant, or worse and may distort the development of business practice into inefficient alternatives.

In the 1980s when contracting parties began adopting electronic data interchange (EDI) contracting systems, there arose the problem of harmonizing the exchange of email messages with the legal requirement of a signed writing. EDI systems set up in the 1980s were often based on the use of "value added networks" (VANs) that were closed, proprietary networks with enhanced security and data integrity features. Before the exchange of electronic quotes, purchase orders, acknowledgements and invoices could begin, the parties normally had to invest considerable time and energy in reengineering their information systems to permit the exchange of messages in standardized formats to take place. In order to draw the maximum benefit from establishing an EDI trading partner relationship, each party needed to take whatever steps were necessary to permit the automated processing of standard messages. Although the parties might reach a complete meeting of the minds with regard to how different messages would be processed as a matter of information system specifications, the issue of how the exchange of messages would be interpreted by a court remained beyond the power of the parties to resolve through technical standards.

A consensus emerged among many EDI trading partners and their attorneys that the best way to reduce uncertainty about the legal status of the EDI messages they planned to exchange would be to sign a traditional contract that would set out the ground rules for interpreting the significance of the electronic messages. This contract, referred to as an EDI trading partner agreement, reduced the uncertainty associated with how a court would treat email messages for statute of frauds purposes, because the trading partner agreement was a writing signed by the party against whom enforcement was sought. Should litigation later arise, the court could look to the trading partner agreement for an explanation of what legal significance the parties expected their electronic messages to have. If what the parties set out in their trading partner agreement was reasonable, a court could be expected to defer to the wishes of the parties. The effectiveness of a trading

partner agreement is not entirely without question, however, as a court might nevertheless still expect to see a signed writing for each transaction that takes place within the trading partner relationship, not just for the relationship as a whole.

A major strength of the trading partner agreement model for regulating electronic commerce is that it may eliminate the statute of frauds problem at the same time it defines the rights and obligations of the trading partners with regard to other issues as well. One weakness of this model is that the agreement cannot govern the rights and obligations of anyone other than the two parties who signed it, so each electronic contracting relationship must be governed by a separate contract. This administrative expense might not be significant in light of the large investments often required to harmonize the information systems of the trading partners. However, when the internet made electronic contracting between strangers with no prior relationship a practical reality, the expense of having the parties meet face to face and take pen in hand to sign a paper contract would in many instances more than offset the cost savings associated with using the Internet as a communications medium.

Another weakness of the trading partner agreement model is that it might require a fair amount of work on the part of attorneys to negotiate and draw up, and many EDI trading partners simply never bother to sign a trading partner agreement as a result. Yet there is no evidence available as to how a court would interpret an EDI trading partner relationship in the absence of a written contract. This is because there are no reported litigated cases involving EDI trading partner disputes, which is an astonishing fact in light of the enormous volume of EDI transactions taking place in the world today. One cannot be sure why no disputes between EDI trading partners ever reached the point of litigation.

It is possible that trading partner agreements provided the parties with such clear guidance as to the rights and obligations of the parties, that they felt litigation was unnecessary, although that can hardly have been the case with all the relationships that were not reduced to a written agreement. It seems more likely that the parties were unwilling to write off the large investment in information system reengineering required establishing EDI trading partner relationships, since the underlying business relationship would probably be irretrievably damaged if litigation were initiated. The absence of reported legal cases may indicate that EDI trading partners tend to work hard to find acceptable compromises to keep their relationship going when disputes arise.

Given that current laws do not generally treat electronic media as a functional substitute for paper documents, and that there is some uncertainty about how flexible in fact a court will be in interpreting what constitutes a signature in electronic communication contexts, there has been considerable attention focused on the question of law reform in this area. One approach to the problem might be to enact legislation that merely authorizes a court to treat an electronic record as writing and an electronic authentication as a signature under appropriate circumstances. Another approach might be to enact legislation that requires a court to so hold unless circumstances contrary. Such legislation would in effect focus on legal outcomes and not technical processes.

The most elementary approach would be to conduct a somewhat word "search and replace" exercise throughout the Statutes and replace all references to "writing" with references to "record". Record would then be defined as information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. The definition would be designed to be broad enough to cover both paper and electronic documents.

On the other hand a technology specific approach identifies one electronic commerce technology and provides that its use will have certain legal consequences. This has the effect of leaving other electronic commerce technologies struggling with the current uncertainty in the law, and focusing the attention of the public on one technology as having been endorsed by the legislature. Given the current state of rapid innovation in electronic

commerce, it is clear that a technology specific approach to legislation will hinder the development of electronic commerce generally.

Clearly, the setting for electronic commerce is different to that which exists for paper exchanges. This raises a number of legal issues, and challenges, of both domestic and international significance. As Johnson and Post point out-

> Cyberspace radically undermines the relationship between legally significant (line) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and (1) the power of the local government to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.

An issue of critical significance, often raised in the context of ensuring that electronic commerce reaches its full potential, is how to build business and consumer confidence in the security of electronic transactions which occur on the Internet between parties that do not have a pre-existing relationship. There must be confidence that the infrastructure which already exists for paper exchanges can also be established for electronic exchanges, so that: services and networks are secure and reliable; transactions are safe and private; there are ways to prove the origin, receipt and integrity of information received; there are ways to identify the parties involved; and there are appropriate redress mechanisms available if something goes wrong.

Since there are few cases or none at all decided in the courts dealing with the issues targeted as likely to cause problems in electronic commerce, it is difficult to judge the magnitude of legal problems being encountered, at least in terms of measuring them through recourse to traditional means of resolution or litigation, although it is clear that some action to remove obvious legal obstacles would certainly facilitate electronic commerce.

A number of tensions have emerged from the electronic commerce regulation debate with some proponents advocating for the enactment of an array of protective comprehensive statutes, tailored to meet the special host of issues presented by the new information technologies. It is doubtful that any particular suite of laws would be sufficient, or desirable as a legal response to the information age.

## 2. Scope of the study.

The scope of the study was to-

(a) examine, investigate and suggest any reforms to the laws relating to electronic evidence;

(b) examine the legal and policy framework of the proposed laws;

(c) establish ways for further development of the commercial legal framework in the above mentioned laws to facilitate operational and structural organization;

(d) improve the existing legal framework to foster business ventures within a competitive framework; and

(e) assess the ability of the relevant organisations, to implement and administer the proposed laws.

The commission also specifically undertook the following in the study-

(a) in relation to e-commerce, the study reviewed Uganda's international and regional commitments; and undertook a comparative analysis of laws and policies of other jurisdictions including countries whose economies are in transition;

(b) identified provisions in the laws of Uganda that affect e-commerce and to modified them so as to facilitate E-Commerce;

(c) held consultative meetings with taskforce members;

(d) held a consultative workshop;

(e) advised on the harmonisation with the stakeholders; relevant East African laws;

(f) advised on the applicability, to Uganda, of the UNCITRAL model law on e-commerce;

(g) harmonized -the law on e-commerce with other relevant domestic laws;

(h) proposed recommendations;

(i) initiated draft bills; and

(j) prepared a final report incorporating all the work done under the study.

A background paper was prepared comprising of a legal audit of the laws of Uganda in the context of e-commerce. Its findings and recommendations formed the basis of the draft report. The draft report was presented by the commission and was comprehensively discussed by the task force members. Their findings and recommendations are the basis of this report.

## 3. Defining electronic commerce.

Electronic commerce can be defined narrowly or broadly. Broader definitions include any kind of transaction that is made using digital technology, including open networks (the internet), closed networks such as electronic data interchange (EDI), and debit or credit cards. The narrower definition restricts electronic commerce to include only transactions using Transmission Control Protocol/Internet Protocol (TCP/IP) whereby electronic commerce is seen simply as an internet application or otherwise internet-based electronic commerce.

In this report the broader definition, viewing electronic commerce as encompassing the internet and closed networks, as well as hybrid network like the Intranets and the extranets. The internet is an international network of networks that allows different computer users to share information and communicate interactively. It allows computers and networks to communicate openly and effectively regardless of make, architecture, speed, manufacturer, connection or resources. EDI on the other hand is a standard for compiling and transmitting information between companies, often over private communications networks called "value added networks."

Electronic commerce encompasses three distinct types of transactions: between businesses, between businesses and consumers, and government services. These transactions are supported by the information technology infrastructure, consisting of hardware, software and enabling services. The European Commission ("EC") has defined E-Commerce as:

> "Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"

(forming part of the "information society services" as defined in the EU Directive 98/48/EC on "Transparency" dated 20 July 1998).

The World Trade Organisation ("WTO") has defined E-Commerce as:

> "the production, distribution, marketing, sale or delivery of goods and services by electronic means" (WTO Declaration on Electronic Commerce dated 25 September 1998).

Electronic commerce may therefore be defined broadly as:

> "The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within government or between the public and government and, last, between business and government "

This definition encompasses the many kinds of business activities that are being conducted electronically, and conveys the notion that electronic commerce is much more comprehensive than simply purchasing goods and services electronically. Electronic transactions are not limited to purchases of goods and services, but move along a spectrum beginning with information gathering and exchange, progressing to negotiation and decision to purchase, finally to completion of transaction and after sales support. In fact, at present, much of electronic commerce activity is concentrated in information gathering and exchange used to support purchase decisions. As electronic commerce grows, the importance of sales transacted on-line is expected to increase.

For clarity it is important to note that e-commerce transactions and instruments include the following-

(a) subscription for online and internet access,

(b) subscription to information services / software sales,

(c) Consumers retail sales e.g. computer equipment (internet based shopping mall) travel services / airline tickets audio /video recordings, books on-line, auctions,

(d) business-to-business wholesale and retail services and sales,

(e) advertising and marketing services,

(f) financial services and transactions e.g. EFT, ATM/credit cards, online brokerage, direct investment and stock trading and online banking and bill payment,

(g) government services and information systems for automatic access to website, filing documents, obtaining application, license application and permits, taxes (payment) and participating in the political process, and

(h) other or ancillary functions contributing to business or commercial activities comprising of elements of traditional business practices combined with the use of telecommunication e.g. email (virtual medium), file transfer.

In traditional business transaction an agreement/contract may be entered in a manner to show that there was an offer and acceptance, or conduct that recognises the existence of a contract. The same rule should apply to electronic contracts. A variety of procedures are available for forming electronic contracts. They include:

(a) e-mail: offers and acceptances may be exchanged entirely by e-mail, or can be combined with paper documents, faxes, and oral discussions.

(b) web site forms: in many cases a web site operator will offer goods or services for sale, which the customer orders by completing and transmitting an order form displayed on screen.

(c) Click through Agreements: A merchant may offer products, data, software or digitalcontent online, subject to a form agreement accepted by clicking on an "Accept" button. The user's conduct of downloading the content may constitute acceptance of the form agree-

(d) Electronic Data Interchange ("EDI"): EDI involves the direct electronic exchange of information between computers; the data is formatted using standard protocols so that it can be interpreted and implemented directly by the receiving computer. EDI is often used to transmit standard purchase orders, acceptances, invoices, and other records, thus reducing paperwork and the potential for human error.

(e) Electronic Agents: an electronic agent is software that is used independently to initiate an action or respond to electronic messages or performances without intervention by an individual at the time of the action, response or performance.

Like all other transactions, electronic transactions involve documents, usually referred to as "records" or "electronic records", and signatures, usually referred to as "electronic or digital signatures" that are created, communicated and stored in electronic form. They may be created through the manual efforts of an individual (e.g., typing an e-mail message), via the automated processing of computers (e.g., via electronic agents), or via a combination of human interaction with a computer agent (e.g., when an individual accesses a web-site and enters into a purchase agreement). They are communicated via an electronic medium, such as the internet or a private value-added network, and they are typically stored on a computer-readable medium, such as a disk, tape, CD-ROM, or DVD-ROM. Typically, evidence of electronic transactions never exists on paper unless there is a need to provide a copy or to introduce evidence to a court or other fact finder.

## 4. Recommendations.

**Recommendation 1.**

A national e-strategy in the context of the National Information Communications Technologies (ICTs) policy should be formulated to underpin and give efficacy to the electronic transactions legislation and should address the following issues-

(a) e-government services,

(b) research into the developments relevant to electronic communications and transactions in Uganda and internationally,

(c) continuous evaluation of the national objectives,

(d) consultations with the donor communities and the private sector,

(e) programmes and means to achieve universal access and human resource development,

(f) programmes and means to promote the overall readiness of Uganda in respect of electronic transactions,

(g) ways to promote Uganda as a preferred provider and user of electronic transactions in the international market,

(h) existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy,

(i) the resources required to achieve the objectives provided for in the national e-strategy,

(j) government should adopt e-government practice by 2005, through ensuring that the information and communication technology Infrastructure is in place in all its institutions. This should be in accordance with the Millennium Development Goals of the World summit on information society timeline,

(k) government should be urged to speed up the process of approving the ICT policy,

(l) the government should increase awareness among Ugandans especially the business community through public and private partnerships and Government agencies like the Uganda Investment Authority and Uganda Chamber of Commerce and industry, and the

(m) government should look within itself to identify the particular institution to spearhead the development of ICT.

**Recommendation 2.**

Legislation is the best option for removing the legal uncertainties identified.

**Recommendation 3.**

A comprehensive framework for electronic commerce legislation, which deals with the issues set out in the recommendations below and by which all other laws in Uganda will be interpreted, should be enacted.

**Recommendation 4.**

(a) Legislation should be based upon the principle of technology neutrality, recognising that in a number of instances, such as electronic signatures, pursuing neutrality will not necessarily limit the ability to ascribe specific legal consequences to the use of the mechanisms.

(b) Legislation should be broad in its operation, applying to data messages in trade and commerce or with government.

(c) Careful consideration needs to be given to what types of exceptions from the requirements of the legislation should be specified.

(d) Where provisions of the Ugandan law establish mandatory form requirements, which cannot be varied by agreement between parties to commercial or governmental transactions, that restriction should be maintained in adoption of the model law provisions. In situations where variation by agreement is permitted in paper-based transactions, that permission should be maintained in electronic transactions. Where variations are agreed between the parties reliance on a variation should be subject to a fairness and reasonableness test analogous to that applicable in the general contract law.

**Recommendation 5.**

(a) Legislation should contain a provision of general application based on Article 5 of the Model Law, which recognises that information, records and signatures in an electronic form should not be denied legal effect solely on the grounds that it is in an electronic form.

(b) The use of an electronic medium should not affect the laws that would ordinarily govern the transaction. In particular, the intended legislation should provide clarity on how electronic communications will satisfy requirements by law to the extent that:

(i) an electronic communication constitutes a document;

(ii) certain information be "in writing";

(iii) certain information be presented or retained in its "original" form;

(iv) certain documents, records or information be retained; and

(v) a document (electronic communication) is authenticated.

(d) The proposed legislation should prescribe the standards to which electronic documents must conform before qualifying as "writing" or "original"?

**Recommendation 6.**

A data message should satisfy any requirements for information to be in writing. The requirement in Article 6 of the Model Law for information to be "accessible so as to be usable for subsequent reference" establishes an acceptable basis upon which to develop functional equivalence.

**Recommendation 7.**

(a) In principle, Article 7 of the Model Law establishes an acceptable basis upon which to determine the minimum requirements for the functional equivalence of electronic signatures and ought to be incorporated in Uganda Legislation.

(b) Legislation on the recognition of electronic signature as equivalent to traditional signature should be enacted outlining the considerations that should be taken into account in determining the reliability of the method of author identity and content approval.

**Recommendation 8.**

(a) The requirements in Article 8 of the Model Law which focus upon information integrity as essential to the concept of originality form an appropriate basis upon which to determine functional equivalence.

(b) To ensure functional equivalence between data messages and paper documents, a provision allowing data messages to satisfy requirements for an original, subject to requirements about the integrity of the data message, should be enacted.

**Recommendation 9.**

(a) The law relating to computer-generated evidence should be modernized, clarified, and harmonized so that public and private sectors alike can make the best technical decisions possible about how to produce and keep records, with a minimum of uncertainty about how their legal rights will be affected.

(b) A law that provides clear guidelines on the admissibility and evidential weight of electronic records is required. Such law should possibly draw a distinction between computer evidence created with and without human intervention.

(c) Amendments in the current law should be made to provide for the admissibility and evidential weight of electronic communications and the considerations that should be taken into account.

(d) Statutory reform should be restricted to computer-generated evidence and not the entire field of documentary evidence.

(e) Statutory provisions should allow Courts to carefully scrutinize the foundation put before it to support a finding of reliability, as a condition of admissibility of computer-generated evidence. The nature and quality of the evidence put before the Court ought to reflect the facts of the complete record keeping process in the case of computer records, the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation.

(f) The statutory provisions should require the proponent of computer-generated evidence to demonstrate the compliance of its system and a general indication of the factors to be considered. The onus should be on the proponent seeking the introduction of computer-generated evidence. The statutory provisions should distinguish between records kept by a party and records kept by a non-party.

(g) Hearsay evidence should be left as it is in the statute and the evolving common law.

(h) The statutory provisions should deal with both optical imaging with other forms of computer-generated evidence and blend it with the existing law on microfilms, tapes and disks.

(i) In making proposals for law reform in the area of computer-generated evidence, there ought to be a balance of a number of factors: the nature of the threshold that should apply to the admissibility of electronic evidence; the burden of proof on the proponent or opponent of the evidence; and the procedural requirements to ensure a proper examination of electronic evidence adduced before the court.

**Recommendation 10.**

Article 10 of the Model Law prescribes an appropriate basis for the equivalence of electronic and paper based record retention requirements and is this regard should be adopted in Ugandan's legislation.

**Recommendation 11.**

(a) A provision covering the general statement of principle in article 11 of the Model Law is important to remove any uncertainty concerning the use and validity of data messages in contract formation, whether as a result of human intervention or otherwise.

(b) The provision should be clear that between the originator and the addressee of an electronic message, a declaration of will or other statement should not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication.

**Recommendation 12.**

(a) In general, issues of attribution and message integrity should be left to determination by agreement between the parties. Disputes can be determined by the courts.

(b) For cases where parties do not determine these issues by agreement, default provisions on attribution in the form of Article 13 of the Model Law, should be enacted.

(c) Due regard should be taken that legal presumptions, would apply only in the absence of contractual arrangements governing attribution e.g. the use of certification authorities

(d) Legislation should provide that where parties agree on rules of attribution and message integrity a party should not be allowed to rely on the agreed rules unless it is fair and reasonable to do so in all the circumstances.

(e) As the market develops there may be a need for the development of more detailed attribution rules

**Recommendation 13.**

The provisions of Article 14 should be enacted into our law to restate the common law rules and any other existing statutory provisions to apply in the context of electronic or data messages.

**Recommendation 14.**

To achieve certainty in the use of data messages for commercial transactions, rules on time and place of dispatch and receipt of data message should be developed. Article 15 of the Model Law provides a useful model, although an additional formulation of the rule with respect to time of receipt and a provision dealing with the potential ambiguity created by time zone differences would add value to the provision enacted.

**Recommendation 15.**

The preparation of statutory provisions covering all aspects of liability in relation to the use of electronic means of communication, including liability of the parties and of service providers, and the position of innocent third parties, is desirable to create legal certainty and facilitate the development of electronic commerce.

**Recommendation 16.**

To facilitate the implementation of electronic commerce, Uganda should actively promote consideration and wide adoption of the principles of the UNCITRAL Model Law internationally and take appropriate action in international area.

**Recommendation 17.**

(a) Review the issue of intermediary liability for defamation.

(b) Monitor progress of international discussions on uniform contract rules for electronic commerce, but make no changes for the time being.

(c) Review the matter of consumer protection, in both domestic and international transactions.

(d) Review the jurisdictional rules for service out of jurisdiction for contract, tort and restitution.

(e) Review the rules for interim relief and cross-border remedies for international litigation.

(f) Review the possibility of service of writ and other documents by electronic media.

# CHAPTER 1

# BACKGROUND.

In the world of e-commerce, commerce tends to be divided into three groups. The first group includes traditional business that have no particular Internet component. This group is commonly referred to as "bricks and mortar" businesses, highlighting the fact that these businesses have stores, factories, and buildings made out of bricks and mortar. The second category includes the pure e-commerce companies, sometimes known as the "clicks" (from the click of the mouse on a hyperlink), or, more commonly, the "dot-coms", based on their use of the top-level domain name ".com" in the address of their websites and names.

Examples include Amazon.com and any of the dot-com companies on which people have recently made and lost fortunes speculating on stocks. The third group is commonly referred to as either "clicks and mortar" companies or "bricks and clicks" companies. These businesses have taken portions of their traditional manufacturing or retail businesses onto the Internet and used their expertise, knowledge, branding and customer relationships to translate their businesses into an e-commerce model. Examples include online ticket sales by airlines.

Electronic commerce undoubtedly has a significant impact on general commerce but how significant that impact will be is a question to be determined by time. The betting seems to be that we are moving towards a new economy, or at least a mixed economy, where e-commerce becomes a significant commercial channel. One can therefore safely predict that we are seeing the beginning of a transition to a commercial reality where e-commerce is a very important and significant channel of commerce that includes perhaps 10% to 50% of commercial transactions. E-commerce is not merely a passing fad it will supplant traditional commerce as we move into a completely new economy.

There are a number of legal and policy issues raised by e-commerce, even in its relatively short history.

The tension that is created by e-commerce and the Internet as it pushes against traditional laws and traditional approaches to doing business raises some "big questions". These questions are-

(a) How do brick and mortar laws apply in a digital/electronic environment?

(b) Can brick and mortar laws apply in a digital environment?

(c) Why is e-commerce any different from plain old commerce?

(d) Does e-commerce really require a new field of law, new types of lawyers, and new laws?

(e) Is e-commerce simply a "flavor of the day" that allows lawyers to disguise existing practices as sophiscated happenings?

There is thus an undercurrent of concern whether existing law, or continuing evolutions of those laws, will adequately address the legal issues being raised by e-commerce. E-commerce is clearly different from plain old commerce in several important ways and these differences have significant implications for our legal system and the legal profession.

## 1.1 Paperless contracts or click through agreements.

One of the things that e-commerce can do is reduce the barriers and inefficiencies in transactions, or what is commonly called "the paperwork". E-commerce creates a "frictionless" economy. Take the example of ordering a book on the Internet from the famous Amazon.com. You have to visit the Amazon.com web site,

been shipped, and thereafter receive the book within a few days, all by visiting a web site and without leaving your home. One does not have to go to a bookstore to order for a book. One just has to wait for a few days for the book to arrive. The Amazon.com transaction is relatively frictionless because there is no paper contract.

The Amazon.com transaction would become much less attractive if, when one ordered for the book online, Amazon.com would first mail a ten-page contract to be signed and mailed back before the book is shipped. The foundation of this frictionless approach to commerce is the paperless contract. These paperless contracts have been referred to as shrinkwrap agreements, click through agreements, or mass market licences. Examples include visiting a web site or instaling software and being presented with the terms and conditions that apply to you. One has the option to accept those terms strictly as they are presented. There is no opportunity for negotiation. Unless one accepts the contract, he/she is not allowed to use the site, service or software. The contracts are presented on a take-it-or-leave it basis. Practically most agreements are accepted unread.

### 1.2 Acceptance and enforceability.

There are two important issues with paperless contracts. The first is acceptance and the second is enforceability. How do we know whether a party has accepted a contract and all of its terms? Are paperless contracts and their terms enforceable? If the courts were to rule definitively that these types of agreements were not enforceable, there would be significant negative ramifications for e-commerce. However, acceptance of these contracts can be a thorny issue. Some clickthrough contracts provide simply that you accept the contract by clicking your mouse on a button that says "I accept".

A customer may argue that he did not enter into this type of agreement or agree to its terms because he did not click on this button. In other words, he may claim that someone else did it or that perhaps his/her baby was playing with the keyboard and clicked on the button. The difficulty of proving acceptance with a simple click approach has led to formats in which the customer has to type "I Accept" rather than click on a button. Typing the phrase shows more intentional behaviour. It is also harder to argue that your baby was playing with the keyboard in such a way that it typed only the letters of "I Accept" in a correct order. In this regard the enforceability of paperless contracts continues to be an issue that needs to be resolved definitively.

### 1.3 Trans-border dimension.

In effect an e-commerce business has customers in different countries and all over the world. E-commerce business involves any number of activities that cross either countries or national borders. As a result, it is inevitable that border-related legal and policy issues will arise, ranging from jurisdiction questions to sales tax issues to import and export regulatory compliance.

### 1.4 New Forms of business entities or models.

The Internet gives rise to new forms of business entities hosted or located on websites that do business or engage in commercial activity using new methods of electronic communication. The global and simultaneous exposure of the website on the Internet to virtually any place in the world facilitates mass communication and/or individual communication between vendors and buyers. In essence, Internet technology allows both vendors and buyers to communicate with each other-

(a) transparently and simultaneously (i.e., from an individual to a group, or from a group to an individual);

(b) in real-time; and

(c) interactively

The new modes of communication have allowed vendors to launch new business models, such as co-shopping models, online auctions, reseller platforms, and agency services, etc., thereby creating the substance of the "new economy." Various categories of participants in e-commerce transactions have been identified. They are Business-to-Business ("B2B"), Business-to-Consumer ("B2C"), Business-to-Employee ("B2E"), Consumer-to-Business ("C2B"), Business-to-Government (B2G) and Government-to-Consumer (G2C) relationships. The distinction between these different groups is obviously essential where consumers are involved and raise specific legal issues concerning consumer and data protection.

Any e-commerce transaction can be described as either an "indirect e-commerce transaction" or a "direct e-commerce transaction." An "indirect e-commerce transaction" is where a vendor and a buyer conclude a contract via the Internet, but perform their contractual obligations (for example, the delivery of the goods and/or the performance of the services, and payment of the purchase price) by means other than through the Internet (i.e., off-line"). The purchase of tangible goods constitutes an indirect e-commerce transaction. The supply of tangible goods in connection with the delivery of a service (for example, the delivery of an airline ticket to a buyer) constitutes an indirect e-commerce transaction. A "direct e-commerce transaction" is where a vendor and a buyer not only conclude the contract, but also perform all their contractual obligations via the Internet, i.e., "on-line".

Such a direct e-commerce transaction is only possible if the goods purchased are intangible or the services are performed exclusively through the Internet or by other electronic means. For example, the purchase of software, films, music or information (such as the contents of a book), which are downloaded to the buyer via the Internet, will constitute a direct e-commerce transaction. Direct e-commerce transactions can be regarded as involving the supply of "virtual goods" or "provision of services".

Constantly developing technology, including accelerated data transportation and download times, is creating enormous potential for direct e-commerce (in particular with regard to B2B Transactions) including consulting, financial and telecommunication services (voice over the Internet, etc.). Similarly, vendors operating in the "old economy" are using such technology to improve the level of their support services (for example, hotline services, remote maintenance, etc.) in light of increasing global competition.

Internet technology enables B2B, B2C and C2B e-commerce transactions, in particular with regard to-

(a) the safe exchange of contractual information between the vendor and the buyer (including the proper registration and subsequent protection of data provided by a buyer when registering at a vendor's website, encryption and digital signatures);

(b) the safe and reliable download of technology in the case of direct e-commerce transactions;

(c) the security of the buyer's payment; and

(d) the availability of sufficient and easily accessible technology for alternative dispute resolution via electronic means.

Clearly, each evolutionary step in Internet technology raises new questions regarding the legal protection available to vendors and buyers. In the world of e-commerce, a commercial website constitutes a virtual shop-window display of products within the shop, allowing the shop-owner (the vendor) to display whatever contents it wishes to communicate from any place in the world to an Internet user (the buyer) virtually anywhere in the world. By its very nature, e-commerce has cross-border, international and potentially multi-jurisdictional exposure and impact.

The law, by contrast, has always been based on the principle of territoriality, defining the limits of the jurisdiction and legislation of each sovereign state. In other words, while the starting point of Internet technology and, therefore, potentially any e-commerce transaction, is its cross-border availability and accessibility, the starting

point of the laws that apply to and regulate e-commerce is diametrically opposed, being limited to a geographically defined territory.

This conflict between the reach of technology and the reach of law will inevitably create legal uncertainty for any e-commerce transactions with cross-border effect. From a legal point of view, the issue for determination is whether the website is (exclusively) subject to the laws of the country where the vendor is established or the laws of the country where the buyer accesses the website. On a global scale, this question is likely to remain unanswered for some time, until nations adopt international agreements. Ultimately, the issue of the governing law will remain difficult to solve from a practical perspective where a vendor operates a single website for direct e-commerce transactions (being fully effected in virtual reality).

Companies moving into e-commerce have developed many new and novel arrangements of doing business. These innovative approaches to business opportunities and technologies have given rise to non-traditional ways of doing business that pose a challenge to the present legal framework. Outsourcing is one of the many such ways. Essentially, the world of e-commerce is the world of outsourcing. Outsourcing simply means contracting for services from third parties that would ordinarily be done in-house. E-commerce companies outsource many aspects of their business to third party providers that would have been traditionally done by employees. In many cases, outside design firms handle the development of an e-commerce web site.

It is uncommon to find an e-commerce company that physically hosts its own e-commerce site. Shipping, distribution, warehousing, and marketing might all be handled by third party providers rather than internal employees. As a result, the relationship between these parties tends to be defined by the short-term exigencies of the situations at hand rather than as part of a long-term formal approach involving standard legal entities and employment relationships. Outsourcing arrangements may be long-term or short-term, and are often subject to change and development.

A large part of e-commerce revolves on the creation of "strategic partnerships". In any presentation by an e-commerce company, you are hearing of references to "strategic partners", "alliance partners", or similar terms. The term "strategic partnership" can have many different meanings. It generally refers to a form of marketing arrangement that can range from a very integrated and formalized resale or supply arrangement, to "co-branding" arrangements, to simply the right to publicise that the "partner" is a customer. As a result, the term "partner" is commonly used in e-commerce in ways that lawyers do not expect. The issue that arises under such arrangements is that, should partnership law principles be applied to such arrangements? As legal issues arise in these types of arrangements, there is certainly a possibility that traditional partnership law concepts and rules may be applied. Will new types of law grow to replace partnership law to cover these types of arrangements?

In e-commerce, non-traditional forms of co-venturing arrangements are often favoured over formal mergers of companies or creation of new corporations or other legal entities. These arrangements can be formed on an ad hoc basis, be tailored to the current situation, especially where there is a sense of trying out a venture on a trial basis, and last for a short period of time until it is determined that a more permanent arrangement or entity is appropriate. As a result, we are starting to see indications of new forms of business entities that may eventually over time develop into standard business formats. Issues will arise as co-venturing arrangements go sour and it becomes clear that traditional business entity law does not adequately cover these arrangements.

### 1.5 Domain names: a new form of property.

Domain names are the names given to web sites that point to the site's address on the web (e.g., mycompany.com). Are domain names a new form of property? Sometime back the domain name "business.com" was sold for 7.5 million dollars and other domain names were sold at high prices. Partly in

response to that sale, there has been a great deal of speculation in Internet domain names. It can reasonably be argued, that domain names constitute a new form of digital property. In a way, they can be seen as an undeveloped form of commercial property, much like undeveloped commercial real property. If it is permissible to buy land speculating that it will later become a valuable site for commercial development, it is reasonable to look at domain names in the same light. Do real property law concepts, therefore, apply to this new form of digital property? Do other traditional property concepts apply to domain names?

As a result there has emerged the syndrome of "Dot.Coms". There is now the "dot.comming" of nearly everything as e-commerce businesses attempt to get the appropriate dot-com domain name for their operations. The Dot.com is more like the goodwill in traditional businesses. Thus the domain name has become an integral part of e-commerce businesses. In other cases, the domain name may be the most valuable asset of a business. Claiming your domain name therefore becomes a major issue in e-commerce. One has to get his/her desired domain name before anyone else claims it. One's concern is to secure the great domain name that one wants and then get it registered. Registration of a domain name involves a number of considerations and procedures that must be complied with to get the domain name one wants.

In the event one does not get the domain name he wants or feels entitled to, his/her concern will be how to retrieve the domain name on basis of having a higher level of entitlement. In the early days of the Internet, it was common for people to register a domain name of a well-known company and then try to get the company to buy that name back from them at a high price. This practice became known as "cyber squatting" and created a number of inequities and problems. In the US there is an anti-cyber squatting statute that deals with this problem. In situations where one party has a higher entitlement to a disputed domain name (for example, having a well-established business name or a trademark), laws and procedures are now in place so that a party can readily retrieve the domain name from the party with a lesser interest who originally claimed it. In cases where higher entitlement cannot be established, people are faced with the choice of either paying for a domain name or coming up with a new domain name.

On the other hand there is interplay of domain name rights (if any) with trademark law. The traditional legal notion of trademarks has played an important role in the new area of domain names. Does a trademark owner have an overriding right to claim a domain name that is identical to the trademark? This question becomes more difficult because there is only one dot-com domain name available for a given name or phrase, and it is the dot-com domain name that is perceived to have the most value. To greatly oversimplify, under trademark law different parties may use the same or similar name if they are using them in different categories of goods or services or geographic areas and there is no likelihood of confusion. There is, however, only one dot-com domain name available for a particular word phrase and generally the first person to register a domain name gets the rights to it.

### 1.6 New value of information.

The use of personal information especially on the Internet is a matter of concern to the consumers and generally users. People routinely provide personal information on the Internet and will often give up detailed information in exchange for a chance to win a prize or receive discounts. This gives rise to issues of privacy. The primary instrumentality of privacy protection in e-commerce is the web site privacy policy. If you go to a web site, scroll down to the bottom and look carefully, you will probably see in small print the term "privacy policy". If you click on the hyperlink associated with the term, you will find a document that describes the privacy policies and procedures of that site.

Typically, this document will tell you how information is collected, what information is collected, and what uses are made with the data that is collected. The purpose of the privacy policies is to provide one with an accurate statement of the site's practices. The issue is whether such a policy is false or misleading. It is

important to understand the emphasis on accuracy because many people believe that the privacy policy is meant to provide privacy protection.

On the internet there is a value in personal information about customers. Information can be turned into money by selling customer data. In a standard e-commerce contract, whether it is for hosting or other aspects of e-commerce, a good deal of effort is concentrated on the treatment of customer data. The party who has the customer generally wants to make it clear that it owns the customer data and to place strong limitations on precisely how a hosting party or other party can use that customer data or release it to a third party. Businesses do not want to take a chance of alienating customers with whom they have built up goodwill over many years by cavalierly or inadvertently disregarding the privacy concerns of those customers.

The other party in an e-commerce arrangement will typically want as much access to the customer data as possible. The general compromise will often be that the personal data cannot be used by anyone other than the party who "owns" the customers, and that the other party can only use aggregate data, such as traffic data and other information that cannot be identified to individuals or to companies, for specified and limited purposes. There is thus need for privacy protection laws. Privacy legislation appears to be difficult to fashion. Enhanced privacy protection can also have unintended consequences of increasing the "friction" in e-commerce or making it difficult to police and stop criminal activity.

### 1.7 Rapid pace of technological development.

Both the Internet and the technology underlying the Internet change at an increasingly rapid pace. It is difficult to keep up with technological developments, let alone to explore and prepare for the legal consequences and implications of new ways of doing business, new ways of delivering information, and new ways of using technology. Efforts to make specific laws and specific legal provisions are often outstripped by technologies that can make these rules technologically irrelevant or obsolete within a short period of time.

Additionally, the Internet has the capacity to re-route around problems. The Internet has shown some tendency to treat legal roadblocks as problems to be routed around. New technologies and technological approaches are constantly being developed and used to produce arguably similar results while avoiding the specific legal prohibitions.

### 1.8 Information technology as a substitute to human endeavour.

In many fields of human activity, information technology is used to subsistitute for some or all of the functions previously undertaken by humans, or to perform functions that could not be previously performed at all. This has happened before for example ,the motor car has in part subsituted for walking but in each case the mechanism has remained largely under the control of the human user.The whole point of using information technology, however, is that the machine should control itself. The enhanced abilities of machines inevitably lead to increased expectations, and standards of performance that were accepted before the introduction of computer technology may well now fall short of what ought to be achieved. This is best exemplified by the public outcry after the 'hurricane' of 1987 in Europe, when many people complained that the Meteorological Office had failed to predict the violence and extent of the storm in spite of substantial investment in information technology. It has still to be decided how far the law's allocation of responsibility (mainly in tort and contract) should reflect these increased expectations.

## 1.9 The move from products to information services.

The first generation of computing technology concentrated on the electronic hardware used to process information; the second on the software, which controlled that processing. Today, it is possible to identify a clear shift from these discrete products to pure trade in information services. Uganda being a landlocked country would benefit from such a shift as illustrated in a UNDP Report of 2002 on e-business opportunities for Uganda. This report emphasised that Uganda's future benefits in electronic commerce lay in services.

This shift, however, generates a further fundamental challenge to the law. Services were previously the result of human effort or skill, and the quality of service to be provided could be judged against the standards expected from other humans. Now, computing technology provides most information-based services, and the human input is increasingly remote from the point of service delivery. As such it is clearly inappropriate to judge an automated bank teller by the standards to be expected of a human, consequently, the law has to determine the new quality and liability tests which should apply to services provided in this way.

## 1.10 Trading in information products.

Closely linked to the question of information, as property is the legal classification of trade in information products. This is particularly relevant to the supply of computer software, information services and entertainment products and services. Initially, when the only computers were mainframe systems and software was only available from the manufacturer, it was generally accepted that the relationship between the software producer and user could be classified solely as a license of intellectual property rights and thus as a supply of services for liability purposes. Information was marketed in two forms; products, which were static (such as books), and bespoke information (such as legal advice) which is not reusable. Entertainment either came in static form (e.g., an audio tape), or was supplied in real time in a reasonably fixed form (e.g., theatre performances or television broadcasts).

Today, we have entered into an age of mass customisation. Most software products are multi functional and capable of further extension and customisation by downloading additional elements. On-line delivery of information and entertainment allows the 'product' to be modified to the recipient's exact requirements. The relationship between the producer of these information products and the ultimate consumer is often remote, with new types of intermediary springing up to make information products and services available on the market. It is now far harder to say exactly what is being traded – goods, services or something entirely new that does not fit into any existing classification?

## 1.11 Paperless and people-less trading.

Already in the business-to-business transactions, computers are selling and buying on behalf of their owners without any human intervention or decision-making. Many industries and commercial sectors undertake automated trading. In the near future, this phenomenon will extend to the business-to-customer market. Automated agents will search the Internet for bargains, negotiate an agreement within the parameter set by their human principal and arrange for payment in electronic form. These activities do not always accord with the existing legal and regulatory framework. The law of contract assumes the meeting of human minds, and requirements to undertake business transactions by written and signed documents are ground in every country's laws. Major legislative reform is required to assimilate these transactions within an extended legal structure, and the most relevant proposals are presented in the recommendations of this report.

## 1.12 Convergence of national laws.

The information technology industry, and the dissemination and consumption of information products and services, transcends national boundaries. Differences in national treatment of these phenomena can result in major distortions of the market for example; the current tax treatment of electronic commerce often discriminates in favour of exporters of information products and against the domestic supplier.

In the long term it is possible to detect a natural trend towards convergence of national laws-indeed, countries whose laws take a different trend towards convergence trend may be forced by the requirements of the global market to enact amending legislation. One of the earliest examples was the Australian amendment to its copyright laws following the High Court's decision that no copyright subsisted in object code. A particularly strong force towards convergence is the Internet and the commercial and non-commercial activities it allows. These impose substantial pressure on national legislators to eradicate the differences between their own laws and those of other states.

Convergence also reduces the severe difficulties of enforcing laws and regulations against an on-line actor, as compliance with the actor's home State laws is likely to mean that it is also compliant abroad. The trend is towards recognition of a basic principle that information processing activities should primarily be regulated in their home countries, which in its turn requires that laws converge. Convergence can happen in any of the following ways-

(a) through the mechanism of international conventions- normally too slow a process for computer law issues;

(b) through harmonization of national laws, as the result of a conscious decision of a national government to remove the differences between them. The European Union provides the classic case study for harmonization,

(c) where powers to enforce the adoption of new laws are lacking, harmonisation of national laws through bilateral or multilateral agreement is a possible alternative; and

(d) through what might be described as accidental or fortuitous convergence, driven by pressure from information technology enterprises and influential policy organizations.

Globalisation is a phenomenon that is not limited to trading activities but also drives legal innovation, and computer law is more strongly affected than most areas of law.

## 1.13 ICT policy framework for Uganda.

The nature of information technology is such that it is continuously evolving. Although Uganda was one of the first sub-Saharan African countries to obtain full Internet connections, its ICT penetration has remained minimal. Last year an E-readiness study in Uganda with the following 6 benchmarks was carried out-

(a) information infrastructure including the density and level of penetration of the different methods of connectivity like dial-up, wireless, VSAT and radio communication accessibility;

(b) internet availability; the number of service providers (ISPs), and the number of public access points which include Tele-centres and Internet cafes available;

(c) internet affordability; the cost of Internet access which includes the cost for basic telephony and ISP services;

(d) internet speed and Quality; available bandwidth both for individual local access and community connection to the Internet backbone, the quality of the network including servers;

(e) hardware and software, the number of hard ware and software suppliers as well as the a range of options including ICT solutions tailored to local needs plus the pricing mechanisms having a significant effect on access to the network; and

(f) technical services and support; availability and quality of technical support to offer after sales services for both the hardware and software.

Focusing on the government, NGOs, the private sector, learning institutions, the policy and regulatory framework it was found that ICT penetration was fair. However it remains apparent that this was only in the urban areas. The present state of affairs explains the existing state of infrastructure on three levels-

(a) the rural sector and commerce which have not yet registered the ICT presence;

(b) a perception that most ICT initiatives are donor driven, not co-coordinated, adversely competitive and not concerned with local needs; and

(c) lack of a conscious focus and harmonisation of all efforts towards a specified national goal.

Thus, a national e-strategy becomes a prerequisite for entrenching e-commerce in Uganda. This strategy has to take into account the national goals, the economic and social aspirations of the people. This would require an aggressive and country wide sensitisation campaign encouraging the people to appreciate the changes electronic technology would bring in his or her life. In particular, institutionalisation of e-government would require all the necessary personnel in virtually all government departments. In view of these infrastructural requirements, a broad national e-policy would of necessity be a prerequisite to the proper functioning of the ICT infrastructure. To ensure that the e-strategy is and remains on course, the government would have to carry out periodical baseline surveys evaluating the relevance and implementation of the national e-strategy.

The formulation of a national e-strategy in Uganda would have to be done in consultation with all the stakeholders. The question of funding remains paramount in effectively designing and implementing the national e-strategy. The source of funding must and should be assured in a large measure once it is declared a national priority. Thus the minister should be given wide latitude in sourcing funding for the national e-strategy. The success of a national policy would only be possible with an institutionalised system of checks and balances. Thus the minister would be required to report to Cabinet and parliament on the progress of the national e-strategy. This should not merely be a formality but the minister must account for the failed targets. He or she must consult the stakeholders on the relevance of the given provisions in the national e-strategy and on why they should be amended. Ultimately, the national e-policy should not be subject to a lot of bureaucracy that may affect its effectiveness.

It would also be important to include in the national strategy a national broadness that is not biased by the Government's strategic political interests but also takes into account the needs of the rural areas. This is important because e-readiness in Uganda seems to be concentrated in very few urban centres leaving the rest of the entire population unconcerned and oblivious of the emerging electronic transactions.

The development of human resource in Uganda will be as central to the implementation of the national e-strategy as the provision of the necessary infrastructure for electronic commerce. There must be a very serious and aggressive effort incorporated in the national e-strategy to comprehensively cover all the loopholes envisaged in the whole superstructure to genuinely assume the responsibility of ensuring the development of a human resource base that can ably handle the effect of electronic Commerce in Uganda.

The need for a tailor made policy on electronic transactions in Uganda is important and has been crafted. The draft ICT policy has taken into consideration the national aspirations, the EAC strategic demands, the entire regional aspirations and the international basic standards. The policy is alive to the available infrastructure and expected developments.

**Recommendation 1.**

A national e-strategy in the context of the National ICT policy should be formulated to underpin and give efficacy to the Electronic Transactions Legislation and should address the following issues-

(a) e-government services;

(b) research into the developments relevant to electronic communications and transactions in Uganda and internationally;

(c) continuous evaluation of the national objectives;

(d) consultations with the donor communities and the private sector;

(e) programmes and means to achieve universal access and human resource development;

(f) programmes and means to promote the overall readiness of Uganda in respect of electronic transactions;

(g) ways to promote Uganda as a preferred provider and user of electronic transactions in the international market;

(h) existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy;

(i) the resources required to achieve the objectives provided for in the national e-strategy;

(j) Government should adopt E-Government practice by 2005 through ensuring that the information and Communication Technology Infrastructure is in place in all its institutions. This should be in accordance with the Millennium Development Goals of the World summit on information society timeline;

(k) Government should be urged to speed up the process of approving the ICT policy;

(l) the Government should increase awareness among Ugandans especially the business community through public and private partnerships and Government agencies like the Uganda Investment Authority and Uganda Chamber of Commerce and industry; and

(m) Government should look within itself to identify the particular institution to spearhead the development of ICT.

## 1.14 E-commerce in the context of the legal framework.

How the law is applied to e-commerce or otherwise paperless transactions leads to uncertain results. When a person engages in an electronic transaction, the law will apply to such a transaction as hereunder-

(a) regulation of the website as a commercial/business entity for the exchange of commercial/ business information, including domain name, and generally liability for website content;

(b) contractual issues including the conclusion of contractual agreements to effect an e-commerce transaction - ("conclusion of e-contracts");

(c) performance of contractual obligations i.e. the delivery of the goods and/or the performance of services, the payment for such goods or services, and the remedies available for a breach of contract - (performance of e-contracts);

(d) data protection and security;

(e) determination of the appropriate jurisdiction and application of the rules conflicts of law; (private international law);

(f) dispute settlement and enforceability;

(g) protection of intellectual property rights; and

(h) taxation of e-commerce transactions.

## 1.15 Legal audit of the current legal framework.

In the background paper we carried out a legal audit of the current legal framework in order to determine its adequacy in the context of electronic commerce. We highlighted the gaps existing in the laws and further identified the legal and policy issues arising in the context of e-commerce. In the background paper we made a number of findings, which included among other things that the current legal framework is tailored for paper-based transactions. In this Report we shall state in summary the issues identified and make an analysis of whether the issues need to be resolved. We shall then present the various options for the resolution of the issues through an analysis of the form of possible electronic transactions legislation in the context of the adoption of the UNCITRAL Model Law and laws of other jurisdictions regarding electronic transactions, electronic signatures, e-evidence and cyber crime.

### 1.15.1 Basic principles in the formation of e-commerce legislation.

The Internet makes it easy to operate across conventional country borders. This poses new challenges for the laws of the country. The new laws intended to regulate e-commerce therefore ought to have an international perspective that includes negotiating new rules and common standards of practice that are relevant in the global environment. Additionally e-commerce is not taking place within a legal vacuum for which a totally new legal framework needs to be created. There is a need to adapt existing laws and regulations to accommodate e-commerce. It is important therefore that in shaping the legal framework for e-commerce, there is need to formulate basic principles to underpin the formation of e-commerce legislation. Hereunder are the principles formulated for purposes of this report:

The legislation ought to facilitate electronic commerce within a framework of international standards. The proposed legislation must be uniform and conform to existing international standards and rules like the UNCITRAL Model Law and laws of other jurisdictions.

The legislation ought to maintain both the traditional paper medium and the electronic medium and ensure that commercial transactions can be effected either through paper or electronic means without presenting uncertainty

The legislation should increase the overall efficiency of commercial transactions. The proposed legislation should not be cumbersome, but should minimize the regulatory burden on business and government, and keep litigation and costs to a minimum.

The legislation should ensure that any laws that are enacted are expressed in a technologically neutral manner, so that changes in the law are not restricted to existing technology but can also apply equally to new and future technology.

Guided by the above principles we formulated the following questions for policy consideration-

(a) Should the Ugandan legal framework be guided by the model set by UNCITRAL?

(b) There are other legal frameworks that are currently being formulated that are country specific. Which countries have a legal framework that is significantly useful in Uganda's legal framework?

(c) What laws are extremely critical to shape Uganda's e-commerce legal framework that need to be addressed?

(d) Does the Uganda legal system have private international law legislation on conflict of laws rules?

(e) In view of the changing nature of technology, how flexible should the laws that are being proposed be, in order to accommodate future changes?

In answering the above questions we evaluated the need for electronic commerce legislation and formulated the objectives hereunder-

(a) Not to re-invent the wheel. Build on the extensive work that has already been done by international organisations and other jurisdictions.

(b) Conform to international standards. Uganda can enact the "Best" e-commerce laws in the world, based on international best practice; while at the same time retaining its legal independence.

(c) Enabling and not regulatory legislative intervention. Introduce legislation that seeks to give equal status and recognition to both electronic and traditional (non-electronic) commerce.

(d) Allow for contractual freedom and self-regulation. Introduce legislation that allows contractual freedom or flexibility in shaping the commercial relationship.

### 1.15.2 Options for resolution of issues identified.

The issues identified raise questions of the application of common law rules and legislation. There are a number of ways of responding to them in the context of facilitating electronic commerce, including-

(a) encouraging parties to resolve these issues by contract, as far as it is possible;

(b) leaving it up to the courts to determine, on a case by case basis as to how existing law may adapt to the new technologies through a liberal interpretation and application of existing law; or

(c) enacting legislation to update the law in order to remove the barriers to electronic commerce.

### 1.15.2.1 Contract.

Contractual rules can be relied upon to govern a number of individual relationships, particularly commercial ones. In a closed system, contracts or a series of contracts (often referred to as Trading Partner Agreements) can be used to create and define the rights and obligations of the parties to a given transaction. In effect those conducting business through these systems are given assurance of the identity and authority of the transacting parties and the benefits of closed network security procedures. Typically, parties to transactions in a closed system have prior and established business relationships and operate within a bounded context, such as the banking community. The legal issues arising within a closed system are generally less ambiguous than those prompted by an open system, and the agreement between the parties enables them to be better resolved.

In an open system or specifically on the Internet, whereas contracts may govern the terms of individual transactions between the parties, there are generally no contracts that govern the ongoing rights and obligations of the parties more broadly as a trading partner agreement would do in a closed system. It is moreover impractical to enter into a series of such contracts in isolated or one-off transactions. Securing transactions, which occur over this infrastructure, is of particular importance, and cannot be realised only by contractual means. A more generally applicable legal approach is needed.

While contractual relationships have been used to regulate many aspects of electronic commerce to date, as an option for resolving the issues herein identified, they however are of limited application, and are unlikely to satisfy on a broad scale the conditions of ensuring certainty, and minimising costs and litigation. While a contractual approach could be equated with minimising regulatory burdens upon government and business, any potential benefits of this are likely to be outweighed by the level of uncertainty created and the need for resolution of the issues by the courts.

### 1.15.2.2 Determination by the courts.

We are not aware of any court cases in Uganda dealing with the issues identified herein above. It may therefore be concluded that parties so far have adopted appropriate contractual means of preventing such problems arising. When and as they do arise, disputes could be left to the courts to resolve on an individual basis. One of the disadvantages of this approach is that while certainty will be achieved in respect of particular factual situations, it will be only after litigation, the results of litigation are likely to be piecemeal and may not be able to be applied uniformly. While the courts play a significant role in interpreting the law and adapting it to change, such as recognising the increased use of faxes in forming contracts, the widespread scale and impact of the electronic environment will make it very difficult for the issues to be addressed on a case by case basis. Where existing law mandates paper-based concepts, the courts may find it very difficult to make the extensions necessary to accommodate electronic communications. After all, while a fax can be characterised as a different form of paper-based communication, a data message clearly is not.

It is our view that this option cannot achieve the certainty and confidence needed in the market to facilitate the implementation of electronic commerce, nor would it minimise either costs or litigation.

### 1.15.2.3 Legislation.

A legislative option includes a comprehensive statutory and regulatory framework specifying the form and scope of legislation to resolve the issues identified. The statutory and regulatory framework is directed at establishing certainty of the legal effect and building business and consumer confidence in the security of electronic transactions, which occur on the Internet between parties that do not have a pre-existing relationship. Essentially what is needed is a non-regulatory, market-oriented approach that facilitates the emergence of a predictable legal environment to support business and commerce. There is need to develop a domestically and

globally uniform commercial legal framework that recognises, facilitates and enforces electronic transactions worldwide. However, achieving this goal does not necessarily require new legislation but a clarification that provides the certainty that is necessary to engage in business.

Legislation facilitates electronic commerce through the resolution of the issues identified herein by enabling the legal framework to address the issues in question. In effect legislation can do the following-

(a) directly remove legal impediments to the implementation of electronic commerce;

(b) ensure certainty as to the application of the law to electronic commerce and enhance business and consumer trust and confidence;

(c) minimise costs and litigation;

(d) be applied to a wide range of transactions, facilitating both related and un-related transactions;

(e) satisfy the objective of minimising regulatory burdens upon government and business by adopting a minimal approach and simply ensuring functional equivalence between paper-based and electronic transactions;

(f) provide a vehicle for the harmonisation of laws applicable to electronic commerce; and

(g) facilitate the cross-border recognition and enforcement of electronic transactions and signatures.

An important point in considering the legislative option is the requirement of neutrality or non-discrimination in the treatment of businesses engaged in traditional physical commerce and those engaged in electronic commerce. Businesses engaged in electronic commerce should be treated similarly and be subject to arrangements equivalent to those affecting businesses engaged in physical commerce. What is needed is that the infrastructure which already exists for paper exchanges should be maintained to apply to electronic exchanges, so that-

(a) services and networks are secure and reliable;

(b) transactions are safe and private;

(c) there are ways to prove the origin, receipt and integrity of information received;

(d) there are ways to identify the parties involved; and

(e) there are appropriate redress mechanisms available if something goes wrong.

Government policy in this area should promote a competitive market for new technologies by clearing obvious legal obstacles, rather than trying to ensure that unknown obstacles do not arise. As the market develops, legislation or regulation can be developed to deal specifically with market failures and other issues that may emerge with respect to consumers, corporate market needs, law enforcement and other public concerns. Affirmatively providing regulatory benefits to specific players in the electronic commerce environment risks enshrining in legislation what may prove to be incorrect guesses about best technology and business practices and may have serious unintended consequences.

In choosing the legislative option to facilitate electronic commerce, flexibility and neutrality should be major considerations. Where possible, a principled approach should be followed, omitting the detail, which might otherwise necessitate constant updating of the legislation.

**Recommendation 2.**

Legislation is the best option for removing the legal uncertainties identified.

## 1.16 Form of legislation.

Most of the legal and regulatory mechanisms currently being applied by governments to commercial activity were conceived in an era before the advent of advanced electronic communications systems. They generally have a national orientation and, in terms of frameworks of commercial policy, law and regulation are oriented to trade in tangible goods. In contrast, electronic commerce has the propensity to ignore national boundaries, while tending to emphasise the intangible aspects of commerce, rather than the tangible.

### 1.16.1 Legislative options.

Many of the laws which apply to the issues identified encompass both statutory and the common law. Where legislation is needed to resolve the application of this body of law to electronic commerce, there are a number of possible options on how it can be implemented-

(a) amending all provisions in the Statutes, which are inapplicable to electronic commerce and new technologies; or

(b) enacting a framework electronic commerce legislation by which all other laws will be interpreted.

Implementation of option (a) would potentially be a very large task and would require a major survey of existing legislation, to identify relevant impediments. The sheer size of that task renders it inappropriate. Option (b) creates a uniform and common framework with harmonized regulatory provisions bringing the benefit of a single solution to the legal issues raised by electronic commerce. It can amalgamate all the changes needed to facilitate the development of electronic commerce and, if necessary, provide a vehicle for future updating of the law in response to technological development.

**Recommendation 3.**

A comprehensive framework electronic commerce legislation, which deals with the issues set out in the recommendations below and by which all other laws in Uganda will be interpreted, should be enacted.

## 1.17 Content of legislation.

### 1.17.1 General issues.

In proposing reforms of the law to facilitate electronic commerce, we categorised the laws into the following-

(a) Laws concerning form requirements of writing and signature and admissibility in evidence. These laws facilitate electronic commerce by dealing with actual or perceived obstacles presented by existing legal form requirements for written records and written signatures and any other impediment to admission in evidence of electronic records and signatures. Typically these laws provide-

(i) That an electronic record (broadly defined) satisfies any legal requirement that there be a document or a writing;

(ii) That an electronic signature (broadly defined) satisfies any legal requirement that there be a signature; and/or

(iii) That electronic records and electronic signatures are admissible in evidence.

(b) Laws, which distinguish between different types of electronic records or signatures for the purpose of attributing different legal consequences to the different types. These laws involve two elements-

(i) A means of distinguishing different types of electronic records or signatures and this may be:

(A) a definition provision-

(B) a general statement of standards which the method for creating, transmitting and storing the record or signature must meet, to be flushed out by court decisions, by decisions of a regulatory agency or standards body or by subordinate legislation; or

(C) detailed legislative standards that the method for creating, transmitting and storing the record or signature must meet.

(ii) the assigning of certain legal consequences to only those electronic records or signatures, which meet the definition or standards. These consequences may include-

(A) the satisfaction of existing form requirements of writing and signature and evidential admissibility;

(B) a legislative presumption of the authenticity of an electronic signature; or

(C) a legislated allocation of rights and duties and risk of loss among users of the electronic records or signatures that meet the standards.

(c) Laws, which regulate the detailed structure of particular electronic record and signature methods, their users and intermediaries. For example, Digital signature legislations normally provide for an extensive regulation of digital signatures based on asymmetric public key encryption, including the rights and duties of subscribers for certificates, persons who rely on certificates and the licensing and liability of certification authorities.

(d) Laws which seek to extend or adapt existing regulation of commercial activity to cover analogous aspects of electronic commerce, for example laws concerning taxation, interception of communications, privacy, banking, consumer protection, bills of exchange.

We have addressed the issues raised by categories (a), (b) and (c). We have decided that category (d) laws involve areas of law and policy that, in our view, fall outside the Terms of Reference.

### 1.17.2 Technology neutrality.

A preliminary issue in any discussion of laws in categories (a) and (b) is whether they should distinguish between different types of technology. We have already argued in favour of adopting a technologically neutral approach to electronic commerce legislation, which does not discriminate between forms of technology, including paper. In the context of forms of electronic signatures, the principle of technology neutrality is relevant, in terms of the means by which functional equivalence is established and the legal consequences attached to those functional equivalents.

A number of States in the United States have adopted digital or electronic signature legislation. Some States, including Utah, have adopted a comprehensive statutory scheme, which amongst other things adopts a particular technology - asymmetric cryptography -, which is the foundation of digital signatures, a specific form of electronic signatures. Other States, such as Massachusetts, are proposing short statutes, which give recognition to the use of electronic, rather than specifically digital, signatures and deal with evidentiary questions. The argument for specifically adopting asymmetric cryptosystems is that a detailed regulatory system can be developed which should provide not only certainty, but also allow for infrastructure development.

The argument in favour of remaining technologically neutral is flexibility; allowing for new technologies to be developed and gain a foothold in the market. Further, we are not in position today to predict the future with respect either to technological or legal developments. Many authentication technologies are so new that currently we cannot rationally make recommendations that discriminate between one technology and another. Rather than facilitating electronic commerce, picking winners may have the opposite effect of supporting a technology, which at a particular point in time is the best answer to a particular problem but which, with the speed of technological development, is rapidly overtaken by something better.

Two important qualifications on the arguments in favour of technological neutrality must be considered. First, if pure technological neutrality is endorsed, there are significant limits on the scope to ascribe detailed legal consequences to electronic authentication mechanisms, if those consequences depend upon assumptions about reliability or security, which may be true of some, but not other, authentication mechanisms. For example, if a statute recognised all electronic authentication mechanisms as sufficient to satisfy form requirements of writing and signature, it would be difficult to responsibly create a legislative presumption that the use of such authentication mechanisms was authorised by and binds the person issued with the mechanism. The difficulty arises because the same legal consequence is then ascribed to authentication mechanisms as diverse in their security and reliability as a four digit PIN, a private key based on asymmetric key cryptography and a retinal scan. In effect, generality in the class of acceptable authentication mechanisms limits the ability to ascribe specific legal consequences to the use of the mechanisms.

Secondly, many statutes that appear to be technologically neutral on their face do not ascribe the same consequences to all authentication technologies. They require some discrimination among different technologies but the implementation of this discrimination occurs outside the terms of the statute. The statutes deal with the difficulty of ascribing detailed legal consequences to a diverse variety of authentication mechanisms by-

(a) delegating a standards setting or case by case approval role to an administrative body; or

(b) by stating general standards for authentication mechanisms and leaving it to the courts in the event of a dispute to determine in any case whether a particular mechanism satisfied the legislative standard.

De facto option (b) means the courts will determine which authentication technologies are more or less reliable and acceptable in practice.

It is therefore, desirable to have a two-level approach in legislation. The first and broad level would be technologically neutral, accepting all or most electronic authentication mechanisms for some purposes such as satisfaction of form requirements. The second level would be technologically neutral in the sense of not mandating particular technologies, but it would permit technological discrimination in the sense of requiring that authentication mechanisms meet particular legislative standards or pass an approval process before their use is invested with other legal consequences. An administrative or judicial process may determine the satisfaction of legislative standards.

These same arguments are applicable in respect of electronic commerce generally. In choosing to update legislation to facilitate electronic commerce, flexibility and neutrality should be major considerations. Where possible, a principled approach should be followed, omitting the detail, which might otherwise necessitate constant updating of the legislation.

### 1.18 Scope.

In most jurisdictions where electronic commerce legislation has been or is being undertaken, the issue of scope has proved to be difficult. The types of data messages to which the legislation will apply needs to be considered carefully in two respects: the broad types of messages to be covered by the legislation and specific or class exclusions from that broad type.

### 1.18.1 Broad types of data messages to be covered.

At the broadest level, a distinction ought to be drawn between data messages of parties to a transaction and data messages kept for purely personal or domestic purposes, such as diary notes and personal letters. Within the broad category of messages which form part of transactions with other parties, further distinctions can be drawn according to the nature of the other party, for example, between commercial, consumer and governmental transactions. With respect to the definition of commercial transactions, the approach adopted in the Model Law has been followed in the proposed legislation with some slight amendment. The limitation on the scope of the proposed law to commercial and governmental transactions eliminates the need to specifically exclude laws relating to wills as these would not generally arise in the context of such transactions.

### 1.18.2 Specific or class exclusions from a broad type.

If exceptions to the scope of legislation are needed, by what criteria should they be assessed? Exceptions could stipulate particular transactions such as wills and negotiable instruments, or they could be based upon a generic category of exception to be determined later in Regulations. Electronic commerce legislations of other jurisdictions have provided for exclusions or exemptions in their laws by limiting the application of the Statute as hereunder;

> The Act shall not apply to the extent that:
>
> Its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement that information be "in writing", "written", "printed", "signed", or any other word that specifies or requires the use of a particular medium of presentation, communication or storage shall not, by itself, be sufficient to establish such intent.

With such drafting, Courts have to consider whether the rules of law can operate consistently with the Act and, if they cannot, the rules of law prevail over the Act. For example, where a provision of a Statute requires "writing", a court would have to determine whether the purposes of that provision are satisfied by a data message. This provision picks up the "repugnance test" that is intended to be a broad catch-all to assure that where a rule of law manifests a clear intent for a paper writing or an ink on paper signature it will not be overridden by the Statute.

Although, the provision does not state what would satisfy the test of clear inconsistency or repugnance, it is however implied from the provision that more than a mere requirement for writing, signing or printing is required for that inconsistency or repugnance to be made out. For example an electronic message or signature would not be repugnant in the context of a statute requiring a signed writing for purposes of creating a perceivable record, providing an evidentiary base for the transaction, permitting retention of a record of the transaction, or requiring application of a signature to indicate assent to the terms in the writing.

Electronic records and electronic signatures can ably accomplish these functions. In addition to the general repugnance clause the said laws include a specific exemption for "any record that serves as a unique and transferable physical token of rights and obligations including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title." Included in specific exceptions, the proposed law should promote party autonomy by making provision allowing the parties to establish reasonable requirements with respect to the methods adopted by a party to sign a contract.

The process of determining what exceptions are needed should involve a careful analysis of the more complex form requirements, particularly the underlying policy reasons for their existence in the paper world. It is appropriate to question the continuing validity or usefulness of some of those underlying policies in the light of

the changes technology will bring, to the conduct of commercial transactions. The functions of some of the legal formalities governing the paper-oriented transactions require an evolution and to be re-engineered in order to include electronic commerce. Where a data message cannot easily satisfy the test of functional equivalence, and an exception is required, that exception should be drafted as broadly as possible on the basis of principle.

A general provision ultimately may be more flexible than a series of exceptions, which specify particular transactions, such as, wills, because it allows for the development of technology, which may address some of the underlying policy justifications for the maintenance of those specific exceptions. Where a general exception is adopted, the circumstances in which it applies should be clearly circumscribed. While the draft Bill is clear that a mere reference to writing and so on is not sufficient for the exception to apply, it is hard to see where the tests of repugnance and inconsistency can be applied. This seems to beg the question and a clearer provision is obviously desirable. Where there is doubt, it will only be resolved by reference to the courts, a result that does not create the necessary certainty.

We have not developed a definitive set of exceptions, because we do not subscribe to the general repugnancy exception. A general repugnancy exception should only be considered if it is not possible to examine all possible laws, which justify a specific exception before the enactment of legislation. Alternatively, exceptions to the legislation could be dealt with by the inclusion of a specific regulation making power. This would allow all the specific exceptions to be determined by regulation and provide flexibility for the addition of future specific exceptions to cover unforeseen cases as the need arises. However, we recognise that exceptions should be clear on the face of the legislation and using regulations to create exceptions to legislative requirements may not be appropriate.

It is our view that the issue of exceptions to the legislation needs to be considered further. Consideration should be given to the following types of exceptions: a general exception, such as the repugnancy provision and specific exceptions related to particular instruments or transaction types (for example, wills, powers of attorney, negotiable instruments, title documents and some consumer transactions). However, in our view a general exception is less desirable than specific exceptions. It may also be desirable to provide for a regulation making power to include other categories of exceptions to cover unforeseen cases, although we do not express a view as to the best legislative mechanism to provide for exceptions.

### 1.18.3 Variation by agreement.

In determining the scope of legislation, we have considered the nature of the provisions in relation to the purpose of the legislation. The nature of the provisions, raises issues of whether the provisions are mandatory, directory or default rules in application and interpretation - that is, are they to be-

(a) mandatory rules;

(b) default rules which only operate where the parties have not otherwise specified; or

(c) rules, which are provided for guidance only and from which parties can derogate.

Article 4 of the Model Law recognises the principle of party autonomy in the context of set out as mandatory form requirements, although derogation is permitted in certain articles where a specific exception paragraph is included.

There is need to strike a balance between the extent to which legislative provisions should be subject to variation by agreement between parties to a commercial transaction and the extent to which they should be mandatory. The balance struck by the Model Law has not been adopted in every jurisdiction. A permissive approach to variation by agreement allowing all provisions to be varied by agreement between parties, excepting certain obligations and liabilities may be adopted.

Similarly, the law may allow all the provisions therein to be varied by agreement, except the offence provisions and those relating to consumer transactions. However, the agreement between parties should not be allowed to affect the limitations to the right to vary by agreement. Additionally, the standards set by the proposed legislation should only be minimum standards so that if the parties agree to set higher standards they should not be prohibited from doing so.

In our view the balance struck by the Model Law between provisions that are mandatory and those that can be varied by agreement between the parties is acceptable. Provisions based on articles 5 to 10 should provide mandatory minimum standards where the parties are allowed to agree on higher standards, while provisions based on articles 11 to 15 may be varied by agreement between the parties. However, where the parties agree to any variation of the standards, reliance on the variation should be subject to a reasonableness test analogous to the ordinary contract law of liability for breach of conditions or warranties. There is need to set a criteria to determine whether reliance on a term of a contract is fair and reasonable. The law also ought to place the onus of proving that reliance on the variation is fair and reasonable in all the circumstances on the party seeking to rely upon the variation.

**Recommendation 4.**

(a) Legislation should be based upon the principle of technology neutrality, recognising that in a number of instances, such as electronic signatures, pursuing neutrality will not necessarily limit the ability to ascribe specific legal consequences to the use of the mechanisms.

(b) Legislation should be broad in its operation, applying to data messages in trade and commerce or with government.

(c) Careful consideration needs to be given to what types of exceptions from the requirements of the legislation should be specified.

(d) Where provisions of the Ugandan law establish mandatory form requirements, which cannot be varied by agreement between parties to commercial or governmental transactions, that restriction should be maintained in adoption of the Model Law provisions. In situations where variation by agreement is permitted in paper-based transactions, that permission should be maintained in electronic transactions. Where variations are agreed between the parties reliance on a variation should be subject to a fairness and reasonableness test analogous to that applicable in the general contract law.

# CHAPTER 2

# LEGALITY AND ENFORCEABILITY OF COMMERCIAL TRANSACTIONS.

## 2.1 Introduction.

Business and consumer transactions require assurances of trust - trust that transactions are secure and private, that transactions are supported by complete and accurate information, and that consumer redress is available. We have shown that measures that were developed for conventional commerce are inadequate to provide trust in the digital economy. For example, while once data were held securely within an organisation, either in paper-based files or in internal computer systems, now the Internet and hybrid forms such as extranets and intranets allow for potentially widespread information access. Issues of security once related only to law enforcement, not to protecting on-line transactions.

Key issues, such as the verification of the identity of parties and the determination of transaction jurisdictions within a global context remain unaddressed. The overriding need is to remove barriers to the use of electronic commerce by clarifying how these rules apply to the digital economy and updating them where necessary. The objective is to ensure that equivalent treatment is provided for digital and non-digital transactions in a consistent and predictable manner. Clarifying marketplace rules in effect becomes a top priority.

For anyone desiring to conduct business transactions online, the goal is to ensure that each electronic transaction is legally valid, binding and enforceable. This requires consideration of three fundamental legal issues-

(a) Is the transaction enforceable in electronic form? In other words, under the applicable law, can the transaction in issue (e.g., contract, security interest, negotiable instrument, etc.) be done in electronic form, and if so, has the transaction been properly effected so as to be legally enforceable?

(b) Do the parties trust the message? Are the parties to the transaction sufficiently comfortable with the authenticity and integrity of the electronic documents comprising the transaction such that they are willing to ship their products, transfer funds, provide services, change their position, or otherwise act in reliance on electronic records communicated over the Internet, especially when asked to do so in a real-time environment? In many respects, this boils down to the question of whether the details of the transaction are ultimately provable and enforceable in a court of law.

(c) What rules govern executing the transaction in electronic form? What are the rules that govern the conduct of the parties with respect to executing the transaction in electronic form, including rules regarding the time a message is sent, the time the message is received, the place the message is sent from and received at, incorporation by reference, the creation and record-keeping relating to the transaction, etc? Will rules applicable to paper-based transactions also be applicable to the same transactions in electronic form, or do new and/or different rules apply in an electronic environment?

E-commerce therefore requires legal norms (for example, contract enforcement, consumer protection, liability assignment, privacy protection, intellectual property rights) and technical standards (e.g. regarding the way payments are accepted and products are delivered to the final user, security, authentication, digital signatures, and connectivity protocols). The basic question that ought to be addressed is –whether the transaction in question will be legally valid and enforceable if done in an electronic form? We therefore have to focus on the requirements for enforceability that arise solely because of the electronic nature of the transaction.

Parties therefore have to focus on the following issues-

(a) Authorisation. Does the law allow this type of transaction to be conducted in electronic form?

(b) Consent. Have the parties consented to conduct this transaction in electronic form?

(c) Signature. Have the signature formalities required for this transaction (where applicable) been satisfied with a legally recognised form of electronic or digital signature?

(d) Record Accessibility. Are the records or copies of the records comprising the transaction available to all the parties?

(e) Record Keeping. Will the electronic records of this transaction satisfy applicable legal requirements?

Issues fundamental to establishing the validity, recognition and enforcement of electronic commerce in contracting have been identified in the United Nations Commission for International Trade Law Model Law document on electronic commerce as follows-

(a) Ensuring the legal recognition for a data message

(b) Admissibility and evidential weight of electronic messages

(c) Formation and validity of contracts and the recognition of electronic documents by parties

(d) Attribution of electronic documents

(e) Time and place of dispatch of electronic communications

(f) Signature

Currently Ugandan law recognizes verbal agreements as legally binding, and that writing is not essential for the contract to be deemed valid. However, if each of the involved parties, or if a statute requires writing with or without signature, the contract will be deemed valid if there is compliance with such requirements. It therefore it is important to attain equality between electronic and traditional commerce.

## 2.2 Ensuring the legal recognition of electronic communications.

As a general rule, commercial transactions need not be concluded in writing to become valid and enforceable. As in most countries, commercial laws in Uganda were developed in a paper-based environment, and as a result, the current laws contain provisions and terms ordinarily associated with paper-based documents and actions. These laws include words such as “document”, “writing”, “signature”, “original”, “copy”, “stamp”, “seal”, “register”, “file”, “deliver”, etc.

In terms of the ordinary rules of construction, the definitions of these terms may be confined to a paper-based environment. Some of the terms are irrelevant or not applicable in e-commerce based transactions. Since some laws locally and internationally require compliance with terms such as “original”, “duplicate”, “copy”, “registration”, “filing”, “certification”, “seal”, “stamps”, “authentication” etc either to establish or enforce an agreement. Non-compliance with these requirements may directly or indirectly affect the validity or enforceability of a transaction.

Article 5 of the UNCTRAL Model Law is essentially meant to ensure functional equivalence between electronic and other forms of communication. Similarly, Article 12 is intended to ensure that electronic messages have the same legal effect as other forms of communications in situations where they have been used between two parties to communicate a statement that may be legally binding but is not contractual. Article 12 is thus a specific example of the principle underlying Article 5.

In this Report we have recommended that the proposed legislation should provide for a general recognition of the principle that data messages should not be denied legal effect solely on the basis that they are in an electronic form of communication (subject to any necessary exceptions). However, it is our view, particularly when article 12 is considered, that for avoidance of any doubt the legislation should contain a provision of general application recognising the principle set out in article 5. If the legislation contains such a provision it does not also require a provision dealing with article 12.

**Recommendation 5.**

(a) Legislation should contain a provision of general application based on Article 5 of the Model Law, which recognises that information, records and signatures in an electronic form should not be denied legal effect solely on the grounds that it is in an electronic form.

(b) The use of an electronic medium should not affect the laws that would ordinarily govern the transaction. In particular, the intended legislation should provide clarity on how electronic communications will satisfy requirements by law to the extent that-

(i) an electronic communication constitutes a document,

(ii) certain information be "in writing";

(iii) certain information be presented or retained in its "original" form;

(iv) certain documents, records or information be retained;

(v) a document (electronic communication) is authenticated.

(c) The proposed legislation should prescribe the standards to which electronic documents must conform before qualifying as "writing" or "original"?

## 2.3 Requirement of writing.

Data messages ought to satisfy any requirements for information to be in writing. In imposing conditions on functional equivalence, article 6 requires that for a data message to satisfy a requirement for writing, the information be "accessible so as to be usable for subsequent reference". The definition of record as information "retrievable in perceivable form" would satisfy such a requirement just as a restatement of the general principle in article 6 that an electronic record can satisfy a rule of law requiring writing.

In General Usage for International Digitally Ensured Commerce (GUIDEC), the International Chamber of Commerce uses the phrase "human-readable form" which it defines as "a presentation of a digital message such that it can be perceived by human beings." The clarification notes that the information processed by nearly all computer-based information systems is fundamentally imperceptible and readable by human beings unless the system presents the information as symbols such as letters, numerals, punctuation marks and formatting.

This definition contains no assurance that the information system has accurately translated the message from its basic digital form into a human readable form, or that the human-readable form is the same as another form perceived by the maker of the message. The same point would apply to article 6, which simply deals with accessibility and usability. It does not deal with issues of authenticity, originality or message integrity. The formulation proposed in article 6 - that is, "accessible so as to be usable for subsequent reference" - is to be preferred.

**Recommendation 6.**

A data message should satisfy any requirements for information to be in writing. The requirement in article 6 of the Model Law for information to be "accessible so as to be usable for subsequent reference" establishes an acceptable basis upon which to develop functional equivalence.

## 2.4 Requirement of the "signature" generally.

As a general rule, written agreements need not be signed to become binding. However, when legislation or the parties require signatures, this requirement must be complied with for the agreement to be valid or enforceable. Signatures, in whatever form, serve primarily to-

(a) confirm or endorse the intent;

(b) identify the signatory and

(c) authenticate and confirm the integrity of the document signed.

In the faceless, impersonal environment of the Internet, these objectives play a vital role in creating confidence in e-commerce transacting. Technology has been developed (generally referred to either as electronic or digital signature) to accomplish these objectives. The following distinctions between electronic and digital signatures need to be noted:

Electronic signature is a generic, technology neutral term that refers to all the various methods by which one can "sign" an electronic record. Electronic signatures can take many forms and can be created by many different technologies. Examples include a name typed at the end of an e-mail message by the sender; a digitised image of a hand-written signature that is attached to an electronic document; a secret code or PIN; a code that the sender of a message uses to identify herself; a biometrics based identifier e.g. a fingerprint; and a digital signature created through the use of public key cryptography.

Digital signature is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to "sign" a message. For our purposes, we will use the same distinction between digital and electronic signatures hereinafter.

It is unclear whether the Ugandan law would give all forms of electronic signatures the same legal recognition and evidential weight as hand-written signatures. In the absence of specific requirements prescribed by legislation, the law generally appears to be flexible enough to regard any mark or symbol applied by a contract party signifying her or his intent to be contractually binding and therefore constituting a signature. However, in the absence of a court ruling, parties may continue using electronic signatures with some degree of legal risk. Moreover, some legislation may be drafted such that it confines signature requirements to a hand-written ink-on paper format to accommodate electronic signatures. The question arises then whether electronic signatures should be regulated to ensure the adherence to certain standards. In the absence of electronic signature standards, whether legislated or not, the general rule is that the party relying on an electronic signature would have to prove to a court that the underlying technology achieves the objectives.

In general, governments may elect to follow one of the following options with regard to digital or electronic signatures-

(a) no regulation or standards;

(b) private sector regulation;

(c) compulsory adherence to legislated standards; or

(d) voluntary registration in terms of legislated standards.

Signatures are perhaps the most complex of the form requirements and raise a number of issues additional to the general issues discussed above: How should the law deal with different methods of authentication? There are various options-

(a) to simply establish some objective criteria or formal requirements (such as author identity, content approval) that a method of authentication must provide in order to satisfy the legal requirements for a signature. In determining this criterion, what is the threshold? Should message integrity, for example, be included as a requirement?

(b) to provide for rules of law that currently require additional attributes such as identity and content approval. For example, signatures on wills are subject to requirements about the place and time of signature and the presence of witnesses; instruments of title raise negotiability issues; and some laws impose requirements for witnessing (which, however, may simply be a technology issue, and not require a change to the law)?

(c) to provide for the approval, specification and/or recognition of particular technologies, thus allowing some flexibility while providing a guide to the courts as to what particular types of signature technology will satisfy a legal requirement for a signature at any given time?

(d) Alternatively, to provide that any recognition of forms of electronic signature should specifically provide for variation by agreement? Should electronic marks (for example, "(signed) Mohmed Mbabazi") have any validity if the signer intended them to be a signature, even if they do not meet the formal requirements for an electronic signature? How will electronic signature laws relate to authentication and certification procedures agreed by contract?

Article 7 deals with (a) hereof by setting out formal requirements. It establishes the threshold for establishing functional equivalence at identification of the author of a data message and approval of the content of the message by the author, and also requires in relation to the method of identification that it be as reliable as was appropriate for the purpose for which it was used. However, while it does not impose any requirements in relation to the integrity of the message, we note that the concept of message integrity is integral to some technologies, such as digital signatures, which use a message digest. Legislations of other jurisdictions make provision for the formal requirements which an authentication technology ought to satisfy, although the requirements are different to those imposed by article 7. For example-

(a) the Uniform Bill requires author identity, content approval and message integrity;

(b) the Illinois Bill contains only a particularised application of the general provision in article 5. It does not contain a provision along the lines of article 7, but a more complex series of provisions dealing with secure electronic records and signatures, which repeat in various forms the requirements for author identity and message integrity, but not content approval;

(c) the Massachusetts Bill deals with electronic signatures, which it defines to mean "any identifier or authentication technique attached to or logically associated with an electronic record

that is intended by the person using it to have the same force and effect as a manual signature". This definition would potentially cover a very broad range of signature functions without establishing a threshold for functional equivalence; and

(d) GUIDEC, which uses different terminology, treats a message as "ensured" if acceptable evidence indicates the identity of the ensurer and that the message has not been altered since it was ensured; it does not specifically refer to the ensurer's approval of the message (to ensure a message is to record or adopt a digital seal or symbol associated with a message, with the present intention of identifying oneself with the message). It also provides for appropriate practices for ensuring a message, and sets out factors to be taken into consideration in determining what would be reasonable in the circumstances (analogous to the requirement in article 7 to be "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances"), including:

(e) the value or importance of the ensured message;

(f) the course of performance between the parties, both within the transaction in question and in previous transactions between the parties, and the available indices of reliability or unreliability corroborating the ensured message; and

(g) trade usage, where trade is conducted by technologically reliable information systems.

The issue raised in (b) is whether legislation should deal with other attributes of signatures. The imposition of additional requirements upon electronic signature technology is discussed in detail in the next sub-section. The issue in (c) is whether a mechanism should be established to provide for the approval, specification and/or recognition of particular technologies. Such a mechanism would provide a guide to the courts about appropriate electronic signature technology, although it is also a matter for the marketplace to assess the available electronic signature products and determine which products are acceptable. In other jurisdictions, approval schemes have been established under legislation.

Generally, the formulation proposed in Article 7 of the Model Law, that as a threshold issue -authentication technology must ensure author identity and approval of content to achieve functional equivalence - is sufficient to provide for the legal recognition of electronic signatures. The issue in (d) is whether parties should be able to vary the signature form requirements. We hold the same view earlier expressed that the form requirements set out in Article 7 should be mandatory minimum requirements, with the parties being able to adopt more stringent requirements by agreement. However, these minimum standards are only relevant where the transaction in question is required to satisfy particular form requirements. There should be nothing in the law, which prevents parties from agreeing to use any method of authentication as between themselves where there are no relevant form requirements.

**Recommendation 7.**

(a) In principle, Article 7 of the Model Law establishes an acceptable basis upon which to determine the minimum requirements for the functional equivalence of electronic signatures and ought to be incorporated in Uganda Legislation.

(b) Legislation on the recognition of electronic signature as equivalent to traditional signature should be enacted outlining the considerations that should be taken into account in determining the reliability of the method of author identity and content approval.

## 2.5 Requirement for an "original".

The requirement that certain information or documents be presented in an original form creates an obstacle to the development of electronic commerce. The concepts of "writing", "signature" and "original" are closely interlinked; the requirement is often for a written, signed, original paper document. An original may be required in order to ensure the integrity of a document and that the information presented in a document has not been altered. In the context of documents of title and negotiable documents, such as bills of lading, where rights are attached to the physical possession of the document, it is essential to ensure that the original document is in the hands of the person claiming the title to the goods represented therein. In an electronic environment the distinction between an original and a copy is an artificial one. If a message is transmitted from one computer to another, the bit string, which might be called the original, and the one, which is the copy, cannot be distinguished.

What is essential in an electronic context is that a data message, which has been created by a particular person, has not been altered; in other words, it is essential to establish the integrity and authenticity of the data message. Various techniques are now available (such as digital signature technique) to confirm the integrity and authenticity of a data message. To overcome the uncertainties arising from the requirement for an original under national laws, the UNCITRAL Model Law specifically addresses the subject in Article 8. Similar to the approach adopted in relation to the requirements of "writing" and "signature", Article 8 (1) sets out the minimum acceptable form requirements to be met by a data message for it to be regarded as the functional equivalent of an original. Paragraph 3 goes on to set out the criteria for assessing the integrity and reliability of a data message.

Article 8 of the Model Law focuses upon the integrity of information and the ability to present it where this is a requirement. In assessing integrity, the provision requires that the information should be complete and unaltered and that the reliability of the assurance as to integrity should be assessed on the basis of the purpose for which the information was generated and all relevant circumstances. In some cases, this reliable assurance may need to include assurance as to certain physical attributes, where those attributes in the original document may be material. It should be noted that the provision is intended to cover the situation where information was first composed as a paper document and subsequently transferred on to a computer (this principle is also relevant to retention of data messages under Article 10).

Article 8 emphasizes the importance of the integrity of the information for its originality and sets out the criteria for assessing the integrity by reference to systematic recording of the information, assurance that the information was recorded without any omission and protection of data against alteration. It links the concept of originality to the method of authentication. It is based on the following elements: a simple criterion as to 'integrity' of the data; a description of the elements to be taken into account in assessing the integrity; and an element of flexibility, i.e., a reference to circumstances". Under paragraph 3 (a), the necessary additions to a data message, such as endorsement and notarisation, do not affect the originality of the data message, as long as the information contained in the message remains complete and unaltered.

Article 8 permits enacting States to exclude certain situations from its application. This approach, which is meant to promote wider acceptability of the Model Law, should not be used to establish blanket exceptions, frustrating the objectives of the Model Law. Articles 6 to 8 on "writing", "signature" and "original" contain fundamental principles, which require general application. The existence of numerous exclusions from their scope would create obstacles to the development of electronic commerce. Some model interchange agreements specifically address the issue of originality of data messages. For example, under the ABA Model Agreement any document properly transmitted pursuant to the Agreement "when containing, or to which there is affixed a signature ('signed document') shall be deemed for all purposes (a) to have been signed and (b) to constitute an 'original' when printed from electronic files or records established and maintained in the normal course of business".

The test of "reliable assurance as to integrity" is perhaps too vague and some jurisdictions have formulated an alternative of the electronic record "being shown to accurately reflect the information set out". This formulation is close to the language in Article 10 of the Model Law, which permits, in the context of record retention, retention in "a format, which can be demonstrated to represent accurately the information generated, sent, or received". A provision requiring the electronic record to "accurately reproduce the original record as it existed at the time in question" would be advisable.

In our view the requirements in Article 8 by which integrity is assessed form a satisfactory basis for determining information integrity.

**Recommendation 8.**

(a) The requirements in article 8 of the Model Law which focus upon information integrity as essential to the concept of originality form an appropriate basis upon which to determine functional equivalence.

(b) To ensure functional equivalence between data messages and paper documents, a provision allowing data messages to satisfy requirements for an original, subject to requirements about the integrity of the data message, should be enacted.

## 2.6 Evidence or evidential value of data messages.

### 2.6.1 General overview of evidence.

The Ugandan Evidence law is governed by the Evidence Act,Cap 6 which was adopted from India and modified to fit the social, economic and political realities of Uganda of 1964. The proliferation of computers has created a number of problems for this law. Many legal rules assume the existence of paper records, signed or original records. The law of evidence traditionally relies on paper records as well, though of course oral testimony and other kinds of physical objects have always been part of our courtrooms too. As more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate the legal rights that flow from them.

The issue of the admissibility and evidential weight of electronic messages in judicial and administrative proceedings plays a central role in the development of electronic commerce. In the Background paper we highlighted the various statutory provisions in the law that relate to the admissibility and evidential value of electronic records. It can generally be concluded that the rules for admissibility of evidence and the requirements relating to evidence under the current laws are a potential obstacle to the development of electronic commerce.

In this Report we have therefore made a review of the legal rules and principles affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission, to be assured that the rules are consistent with developments in technology, and to provide appropriate means for a court to evaluate the credibility of the data contained in these records. Electronic evidence otherwise called computer-generated evidence differs from traditional documentary evidence. Documents created electronically (e.g. by word processor) have different attributes than paper-based documents. Electronic data or information is in a form of encoded sequence bits of ones and zeroes. These bits are stored on a magnetic medium such as tape or disk, where they take the form of magnetised and demagnetised portions of the medium, or on an optical medium such as a CD-ROM, where they take the form of pitted or smooth portions of the CD's surface. By its nature, data of this sort cannot be directly interpreted by humans, they have to be transformed by the computer system into something a human can perceive, whether on a screen or on a piece of paper.

The transformation of the information into a documentary format is an issue of concern in evidence law. The information is normally processed by a program and printed out, to produce what is called a "computer-generated document". The admissibility of this document in evidence thereby becomes an issue for determination by the courts. Is the printout a "copy" (secondary evidence) of the "original" electronically stored version? A printout is based on information in the memory of a central computer, is the computer's memory therefore a "record" under the law. Is it an original or a copy? Is the printout then a "copy"? Can it be said a printout is "a new type of copy made from a new type of record"? Alternatively, can't the printout itself be the record in as much as it is a transformation or collation of information originally placed in the computer memory.

If the answers to these questions are in the affirmative, then there is need to read the words "record" and "copy" in a broad and functional manner that emphasizes the diversity of record-keeping systems and how printouts are created. In effect for a computer-generated document to be admissible in evidence, the proponent would have to lay a fairly detailed foundation as a precondition to admission. The question then becomes one of authentication, whereby the issues of "original" and "copy" have little relevance to computer records.

In applying the traditional rules of evidence to electronic records, there is bound to arise confusion between the common term "reliability" and the principles of authentication, best evidence, hearsay and weight. Essentially the whole of the law of evidence is concerned with the means of proving the facts that are in issue. Within that broad sense there are rules that relate to the way in which the material is to be presented to the court, and those concerned with the content. In all cases evidence ought to be authenticated in some way.

A document or other thing cannot authenticate itself at common law, but must be introduced to the court or tribunal by a human being whose task it is to explain its identity, its nature, its origin and its relevance. Only if these matters are satisfactorily put before the court and found acceptable to it can such a thing be admitted in evidence. The establishment of such foundations is necessary, and the rules governing this process constitute the rules relating to the authentication of things considered in evidence.

The application of the rules of authentication to evidence derived from computers is indeed very difficult. In most cases the evidence is produced from the custody of a party to the proceedings, who has an interest to serve and may be tempted to tamper with the evidence. In case of a document being produced, it quite often is a printout that would have been printed for the purposes of the proceedings. Any alteration will have taken place not on the thing produced in court, but on the storage medium from which it has been derived. This storage medium may well itself be, or be derived in its turn from, a record on a magnetic disc. The whole point of such discs is that they should be easy to alter, and unless specific precautions are taken they normally keep no record of having been altered. This means that much less weight can be given on the question of authentication to the appearance of the thing itself, and much more must depend upon the testimony describing the operation of the computer system and the origin of the particular things before the court.

The principal difficulty in presenting electronic records to a court or tribunal is ensuring that they are accurate. Electronic records as we understand them today, are more vulnerable than paper records to undetectable modification- intended or unintended. In this respect the law of evidence presents two difficult issues for electronic records: admissibility and weight resultant from the nature of electronic records.

### 2.6.2 Admissibility

There are three questions traditionally asked when a document is tendered as evidence-

(a) Authentication: What is this document? Where did it come from? Who or what created it?

(b) Best evidence: Is this document the original? If not, is it a copy that is admissible under an exception to the original document rule?

(c) Hearsay: Is the document offered for the truth of the assertions it contains? If so, is it admissible for its truth under an exception to the rule against hearsay?

In the context of electronic records the above questions constitute three major hurdles to the admissibility of electronic documents-

(a) Authentication: Is the record what it purports to be? The record must be identified and linked to its source.

(b) Best Evidence Rule: How close is the record to its "original" version? Has its integrity been maintained or are there differences between the record and its "original" version?

(c) Hearsay: Can the document be relied on as evidence of the truth of its contents? Does it meet the tests of reliability and necessity?

There is need to comment about the word "reliability" in the context of the questions raised above. The nature of "reliability" varies with the rule under consideration. For authentication, reliability means that the record is what it purports to be. For the best evidence rule, reliability means that the record is accurate or has integrity. For hearsay, reliability relates to the truth of the contents of the record.

In the context of computer-generated documents the answers to the above questions would be based on an idea of how documents are created The application of the existing doctrine to determine the admissibility of computer-generated documents raises two dangers: on the one hand, a strict reading of the existing doctrine may exclude reliable and probative evidence simply because it does not meet a requirement designed before computers were routinely used to store and process information; on the other hand, a lenient reading of existing doctrine may give insufficient attention to the problems of authentication that are relevant to computer-generated documents. For purposes of brevity, we shall hereunder consider each of the three questions:

### 2.6.3 Authentication.

As with traditional documentary evidence, many of the concerns about electronic evidence are on authentication. Authentication of any record requires the presence of a live witness under oath and available for cross-examination who testifies about the identity of the records. Authentication is therefore a test of identity and not integrity. The usual procedure for authenticating a record works equally well for paper or electronic records. To be admissible, both the traditional document and the computer record require authentication by a witness.

Traditional documents can be forged or altered; so can computer records although an alteration or forgery of computer records may be a lot harder to detect than comparable operations on traditional documents. The focus of authentication of a computer-generated document is not only on the origin of the piece of paper itself, but on the security, reliability, and accuracy of the system that placed the marks on the piece of paper. In effect the requirement that the proponent ought to satisfy the burden of establishing the authenticity of his or her evidence by the introduction of evidence capable of supporting a finding that the record is what its proponent claims it to be, need to be maintained.

### 2.6.4 Best evidence rule.

The best evidence rule requires the proponent of evidence to produce the best evidence available to that party, which has traditionally meant in practice the closest to an original document. This presents two challenges for electronic records. First, ordinary data records do not have a meaningful "original", and certainly do not have an original that is distinguishable from their display on a screen or by printout. Neither is "closer" to the electronic

Second, those who transfer paper records to electronic images often want to destroy the paper originals, to save storage costs. Some people worry that deliberate destruction of originals may lose the sympathy of a court for presenting electronic images of them, because the originals are not available as a result of a deliberate act of the party wanting to rely on the record. Solutions, which have been devised to deal with paper-based records, are not readily applicable to electronic records. Attempts to characterize printouts as originals, or as duplicates of an original (computer disk) or reliable copies or the creation of a category of "duplicates" to photocopies, certified true copies and electronic images as equivalents to the original for the purpose of satisfying the best evidence rule have only created artificial differences. The focus should be to search for the principle behind the best evidence rule.

The "function" of the best evidence rule is to ensure the reliability or the integrity of the record to be produced in evidence. It is practically easier to tell that an original paper record has been altered than to determine any alteration by viewing a copy. In the electronic world, there may or may not be any original paper version of the electronic record. Therefore, the search for integrity of an electronic record has to proceed in another way. The law should move from "original" to "system" or from the dependence upon proof of the integrity of the original business document to a dependence on proof of the integrity of the record-keeping system. In effect the best evidence rule has to lose most or all of its attributes in application. In other words the integrity of the record-keeping system is the key to proving the integrity of the record, including any manifestation of the record created, maintained, displayed, reproduced or printed out by a computer system. Legislations of other jurisdiction require that, the integrity of the records be demonstrated as a condition of being admitted. The legislations require evidence of the reliability of the system that produced the records in question.

The next question is whether the reliability of the system should be demonstrated when the evidence is to be admitted or after admission, when determining its evidential value. The integrity of the record to be admitted is relevant both on admission and in determining its weight. In determining the stage at which the issue of integrity should be determined, the following ought to be taken into consideration:

Computer records are inherently unreliable that it is unfair to apply rules of admissibility to electronic records, which are less stringent than rules applied to paper-based records or to eliminate altogether any rules regarding integrity at the admissibility stage.

Information on the integrity of the records is within the knowledge of the proponent of the evidence so it is not unduly difficult to have to support them. On the other hand it would be unfair to admit them when the (potential) opponent has no information that would permit a successful challenge.

Requiring the proponent to demonstrate integrity at the admission stage would require "foundation" evidence that the opponent could cross-examine. If the proponent is not required to adduce foundation evidence to support admission of the electronic record, then the opponent would have to call its own witnesses to challenge the integrity of the record. The best or even the only witness who could testify to the integrity of the proponent's system would be an employee of the proponent. If the opponent called such a witness, the opponent could not cross- examine him or her. Therefore, if the proponent is required to give foundation evidence at the admissibility stage, a fairer test of the record can be made.

The need to call foundation evidence is likely to encourage responsible record- keeping, since anyone wishing to introduce electronic records will have to be able to withstand cross-examination on the integrity of the system.

In conclusion, it is our finding that there is an urgent need to dispense with the "best evidence" rule in its usual formulation when applied to computer-generated documents. A statutory regime appropriate to computer-generated records ought to merge the "original document" rule with the requirement for authentication. The

rationale for the original document rule was that, where the document was offered either for the legal effect or for the truth of its words, it was important to avoid the errors that inevitably creep into the processes of copying and transcription. This rationale is equally applicable to computer-generated documents, because errors can creep into the copying, processing and transcription of computer files. The focus however, should be on the overall security and reliability of the computer system that produced the document. In functional terms, this focus leads to the consideration of the same factors for authenticating computer-produced documents.

### 2.6.5 Hearsay.

A document is hearsay because it is a second-hand representation of information about a matter to which the statements in the document relate, as opposed to statements made by an eyewitness who can be cross-examined. Hearsay is inadmissible unless it falls into either the statutory or common law exceptions. In the context of electronic commerce, there are notably two exceptions to the hearsay rule - the business records rule and the general exception to the rule against hearsay.

The business record rule was developed at common law to the effect that if a record is created in the ordinary course of business and is (a type) relied on in the business, then it is admissible. The record must have been created more or less at the same time as the event recorded, and by a person with a duty to record it. The theory is that these circumstances give the record sufficient assurances of the truth of its contents that it may be admitted. The rule does not require separate proof of the truth of a record's contents. The making and the use of the record in the course of business provides sufficient guarantee of the truth of the record's contents to support admission. The second exception is through the evolving common law of hearsay. There is a trend that any evidence shown to be reliable as to the truth of its contents and necessary to the determination of an issue will be admitted.

Electronic evidence does not demand any change to the rules on hearsay. The character of the record can be sufficiently demonstrated under existing law to meet the exceptions, regardless of the medium of the record. This equally applies to other rules providing for the admission of hearsay like in the case of public records and bank documents.

### 2.6.6 Weight.

The weight of evidence is traditionally not the subject of statute. It depends very much on the facts of the case. Once the record is admitted, it can be challenged on a number of grounds, including its lack of integrity, lack of truthfulness and lack of relevance to the issue. Has it been tampered with? How is the security to be demonstrated? Has the data degraded over time? Proving such deficiencies is up to the opponent of the evidence, who bears the burden of proof. The proponent of the evidence in turn has the burden to lead evidence in rebuttal to support the weight of the record. If the proponent were not required to support the integrity of the record to have it admitted, the opponent could be in a difficult position in challenging the weight of the electronic record. The best-suited person to give evidence on the reliability of the proponent's system is probably the systems manager of the proponent, who if called by the opponent to testify, cannot be cross-examined.

To provide guidance to States in removing obstacles to the use of electronic-based evidence, the UNCITRAL Model Law lays down provisions addressing both the admissibility and the evidential value of data messages in legal proceedings. Article 9 provides as follows:

(a) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(i) on the sole ground that it is a data message; or,

(ii) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(b) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor."

Paragraph (1) clearly states that data messages should not be denied admissibility on the sole ground that they are in electronic form. The reference to the best evidence rule (which requires that only the original documents be presented as evidence) is considered necessary for certain common law jurisdictions. As stated in the Guide to the Enactment of the Model Law, "the notion of 'best evidence' could raise a great deal of uncertainty in legal systems in which such a rule is unknown. States in which the term would be regarded as meaningless and potentially misleading may wish to enact the Model Law without reference to the 'best evidence' rule contained in paragraph (1)".

Paragraph (2) establishes the principle that due evidential weight must be given to information presented in the form of a data message. It sets out certain criteria to be applied in assessing the evidential weight of a data message, including the reliability and credibility of the method by which the data message was generated, stored, communicated or maintained, as well as the method of identification of the originator and any other relevant factors.

### 2.6.7 Trading partner agreements.

Parties usually address the admissibility of EDI messages in their interchange agreement. Model interchange agreements adopt varying approaches to the questions. They often provide that the parties accept electronic messages as evidence, or that they agree not to contest the admissibility of electronic evidence, or to give the same evidential value to electronic evidence. Such "trading partner agreements" often provide that records that comply with the agreed standards may not be challenged on the ground that they are electronic in form or otherwise unsatisfactory under the rules of evidence. Are such agreements valid, in as much, as they appear to contract out of the rules of evidence? Can parties validly agree to certain facts whose existence is owed to following processes prescribed in their agreement?

It should be noted, that the validity of contractual agreements between parties to an interchange agreement on the admissibility of electronic evidence depends on the nature of the rules of evidence in a particular jurisdiction. To the extent that provisions regarding evidence are mandatory, contractual arrangements will not be effective. Again, such contractual provisions cannot be relied upon in litigation involving third parties that are not privy to the agreement. Similarly, contractual provisions will not be effective where there is a legal requirement for a written document for tax, accounting or other regulatory purposes, unless there is special permission by the public authorities regarding the use of electronic records. These general agreements should however be enforced, as between the parties only but any attempt to enact a private code of evidence should be discouraged.

Some model interchange agreements address specific domestic rules of evidence. For example, the ABA Model Agreement addresses the "hearsay evidence rule" and the "best evidence rule" found in some common law jurisdictions, which may constitute obstacles to the admissibility of electronic evidence. It provides that:

"Neither party shall contest the admissibility of copies of Signed Documents under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Signed Documents were not originated or maintained in documentary form." (Section 3.3.4)

The European Model EDI Agreement and the ECE Model Interchange Agreement clearly acknowledge the limit of the parties' agreement to the extent permitted by national law. The former states:

> "To the extent permitted by any national law which may apply, the parties thereby agree that in the event of dispute, the records of EDI messages which they have maintained in accordance with the terms and conditions of this Agreement, shall be admissible before the Courts and shall constitute evidence of the facts contained therein unless evidence to the contrary is adduced."

The commission has recommended that the proposed legislation should authorize private agreements on how to deal with evidence arising out of electronic transactions between the parties to the agreements.

### 2.6.8 Conclusion.

The key to thinking about computer-generated evidence is to get away from the paper-document model that underlies the existing rules. For a computer generated document, the issue is not whether the piece of paper (or other form of information) is an "original" or is a "copy" of an original; the issue is whether the information on the piece of paper accurately reflects the intentions of the persons who use the computer system that generated it. Therefore, the focus of admissibility for a computer-generated document should be on the security and reliability of the computer system that handles the records. The rules should not make admission of computer records excessively difficult, but should not completely immunize them from scrutiny. At the same time, a statutory framework for this sort of evidence should not be so specific that it is unlikely to be able to cope with future changes in computer technology.

There is need to amend the law to ensure that the quest for an original electronic record is abandoned, or the original of an electronic record. The demand for reform on a statute-by-statute basis should also disappear. Users will face the need to establish the integrity of their records, based largely on the reliability of their systems in maintaining the records. We have not proposed any particular industry standard for reliability in this report to provide for greater flexibility and accommodate technological innovation.

Reforms in the law of evidence should address the following issues-

(a) the presence of a (low) barrier at the time of admission;

(b) the abolition of the search for original records or some other format as good as an original;

(c) authority of the court to judge the integrity of a record by the integrity of the system that produced such record, either for admissibility and weight, or for weight alone.

**Recommendation 9.**

(a) The law relating to computer-generated evidence should be modernized, clarified, and harmonized so that public and private sectors alike can make the best technical decisions possible about how to produce and keep records, with a minimum of uncertainty about how their legal rights will be affected.

(b) A law that provides clear guidelines on the admissibility and evidential weight of electronic records is required. Such law should possibly draw a distinction between computer evidence created with and without human intervention.

(c) Amendments in the current law should be made to provide for the admissibility and evidential weight of electronic communications and the considerations that should be taken into account.

(d) Statutory reform should be restricted to computer-generated evidence and not the entire field of documentary evidence.

(e) Statutory provisions should allow Courts to carefully scrutinize the foundation put before it to support a finding of reliability, as a condition of admissibility of computer-generated evidence. The nature and quality of the evidence put before the Court ought to reflect the facts of the complete record keeping process in the case of computer records, the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation.

(f) The statutory provisions should require the proponent of computer-generated evidence to demonstrate the compliance of its system and a general indication of the factors to be considered. The onus should be on the proponent seeking the introduction of computer-generated evidence. The statutory provisions should distinguish between records kept by a party and records kept by a non-party.

(g) Hearsay evidence should be left as it is in the statute and the evolving common law.

(h) The statutory provisions should deal with both optical imaging with other forms of computer-generated evidence and blend it with the existing law on microfilms, tapes and disks.

(i) In making proposals for law reform in the area of computer-generated evidence, there ought to be a balance of a number of factors: the nature of the threshold that should apply to the admissibility of electronic evidence; the burden of proof on the proponent or opponent of the evidence; and the procedural requirements to ensure a proper examination of electronic evidence adduced before the court.

## 2.7 Retention of data messages.

The requirements for storage of certain documents or information in paper form for evidence and other legal or administrative purposes e.g. accounting, tax, audit constitute is abound in various laws that were examined in the Background paper. These requirements constitute barriers to the development of electronic commerce. There is need for a uniform approach to retention and management of electronic records. The UNCITRAL Model Law provides legislative guidance for removing such barriers by ensuring that the keeping of electronic records is given the same status as the keeping of paper records.

As a starting point, record retention requirements should apply equally to information in paper or electronic form. Record management systems should be standardised at a technical and policy level, based as far as possible on a common definition of what constitutes an electronic record and the criteria to be satisfied in terms of accessibility, integrity and identification. Article 10 of the Model Law provides an appropriate basis for development of such provisions.

Additionally, Article 8 sets out the basic requirements for storage of information as data messages: accessibility; integrity; and retention of transmittal information so as to enable identification of the data message. This provision makes provision for information to be retained in a format, which can be demonstrated to represent accurately the information generated, stored or received. Therefore the information does not have to be retained in the form in which it was generated, stored or received.

However care must be taken where physical attributes are integral to the information being retained. Additional requirements for record retention need to be considered including a requirement for an accurate reproduction of the original record, as it existed at the time in question and retention for as long as required by law.

Article 10 is clear on all these points. Subparagraph (a) sets the same requirements as in the case of "writing", namely that information contained in data messages must be accessible and usable for subsequent reference. Subparagraph (b) provides that a data message must be retained either in the same format as it was generated, sent or received, or in any other format so long as it accurately reflects the information as it was generated, sent or received. It does not require that data messages be stored unaltered since data messages are usually decoded, compressed or converted in order to be stored. Sub-paragraph (c) aims at covering all the information that may be stored in addition to the data message itself, namely certain transmittal information necessary for the identification of the message in terms of its origin, destination and the date and time it was sent or received. Thus, there is no obligation to store those elements of transmittal information which have no relevance to the data message and "the sole purpose of which is to enable the message to be sent or received". Article 10 (3) provides that the services of an intermediary or any other third party may be used in meeting the obligations set out in paragraph (1), provided that the conditions imposed by subparagraphs (a), (b) and (c) are met.

Most interchange agreements address the question of recording and storage of EDI messages. Article 8 of the European Model EDI Agreement provides that:

> 8.1. A complete and chronological record of all EDI messages exchanged by the parties in the course of a trade transaction shall be stored by each party, unaltered and securely, in accordance with the time limits and specifications prescribed by the legislative requirements of its own national law, and, in any event, for a minimum of three years following the completion of the transaction.
>
> 8.2. Unless otherwise provided by national laws, EDI messages shall be stored by the sender in the transmitted format and by the receiver in the format in which they are received.
>
> 8.3. Parties shall ensure that electronic or computer records of the EDI messages shall be readily accessible, capable of being reproduced in a human readable form and of being printed, if required. Any operational equipment required in this connection shall be maintained.

Some model agreements go further by requiring the parties to ensure that the person responsible for the data processing system or a third party certifies the correctness of the trade data log and of its reproduction. Others require that the parties must take precautions to ensure that EDI messages are stored in such a way that they can later be printed out on paper.

**Recommendation 10.**

Article 10 of the Model Law prescribes an appropriate basis for the equivalence of electronic and paper based record retention requirements and is this regard should be adopted in Ugandan's legislation.

## 2.8 Formation and validity of contracts.

As a general rule, a contract is formed when the parties reach an agreement on its terms and conditions, unless specific formalities such as document, signature, attestation or execution are required by law. Thus, a contract concluded orally is equally valid under the law. It follows, therefore, that a contract concluded by an electronic means of communication should, in principle, be valid. However, a number of questions and uncertainties arise in the context of the use of electronic communication techniques for concluding a contract.

Questions arise as to the validity of such contracts, especially where there are legal requirements for writing, signature etc., the time and place of formation of such contracts, the proof of the terms of the contract in case

of dispute, and so on. The time when the contract is formed is important in determining the passing of property and transfer of risk of loss or damage in case of sale of goods. The place where the contract is concluded may determine which national law is to govern the contract in the absence of an effective choice of legal provision as well as the establishing jurisdiction in case of litigation.

In effect a contract or other transaction can be concluded by electronic means wherever writing is not required. The issue associated with the determination of the time and place of conclusion of operations performed by electronic communications is the most difficult obstacle to the development of electronic commerce. One solution is to follow the theory of receipt, to the effect that the contract is concluded at the time and place where the offerer receives the acceptance of the offer. The other solution commonly adopted is the dispatch rule, to the effect that the contract is concluded at the time and place where the acceptance of the offer is sent by the offeree to the offerer. Although the parties to a contract are free to agree on the rules as to the conclusion of their contracts, the law on the subject would apply if the parties fail to make specific provisions concerning certain issues. To promote increased certainty and uniformity with regard to the conclusion of contracts through the use of electronic means, the Article 11 of the UNCITRAL Model Law includes specific provisions on formation and validity of such contracts.

This provision is meant to remove any uncertainty existing as to the validity of contracts concluded by electronic means. It deals, in addition, with the form in which an offer or acceptance may be expressed. Although other articles of the Model Law establish legal validity and effectiveness of data messages, specific provisions in the context of contract formation were considered necessary. According to the Guide to Enactment of the Model Law, "the fact that electronic messages may have legal value as evidence and produce a number of effects does not necessarily mean that they can be used for the purpose of concluding valid contracts". Article 11, however, does not impose the use of electronic means of communication on the parties. The use of the term "unless otherwise agreed by the parties" in paragraph (1) clearly recognizes the parties' freedom of contract. Similarly, article 11 is not intended to overrule the various laws that prescribe formalities for certain contracts, such as attestation, notarisation or other requirements for "writing" for public policy reasons. Paragraph (2) therefore permits the exclusion from the application of paragraph (1) in certain specified cases.

The Model Law does not include specific provisions as to the time and place of contracts formed through electronic means. However the provisions of Article 11 together with those of Article 15, dealing with the time and place of dispatch and receipt of data messages, can best cater for uncertainty regarding the time and place of formation of contracts where the offer or the acceptance is expressed electronically.

Some Model Interchange Agreements do not include provisions on the subject of contract formation in their contractual terms. Others specifically address the topic. Provisions are frequently included expressing the intention of the parties to enter into binding obligations by exchange of electronic messages. The ABA Model Interchange Agreement states:

> This Agreement has been executed by the parties to evidence their mutual intent to create binding purchase and sale obligations pursuant to the electronic transmission and receipt of documents specifying certain of the applicable terms.

The European Model EDI Agreement defines the time and place of the formation of the contract by stating that:A contract effected by the use of EDI shall be concluded at the time and place where the EDI message constituting acceptance of an offer reaches the computer system of the offeror.

In our opinion, when determining the time and place of contracts concluded where arties are not in the presence of each other, the application of the "reception rule" is a better option. This is moreover in line with the provisions of the United Nations Convention on the International Sale of Goods. This rule avoids, to a large extent, the risk of conflicts of laws in connection with the use of electronic communications.

While there may be instances where it is not certain whether the particular elements required for the conclusion of a valid contract by means of data messages exist, the issue is ultimately one of fact. Special reference is made to the conclusion of contracts without human intervention references i.e. contracts formed by either two electronic agents or one electronic agent and a person. This process of contract formation and automated conclusion of the contract raises an issue; is there need for specific provisions concerning automated transactions?

This additional detail is unnecessary in view of Article 11 which is sufficiently broad to address the formation and validity of contracts, whether as a result of human intervention or otherwise.

**Recommendation 11.**

(a) A provision covering the general statement of principle in article 11 of the Model Law is important to remove any uncertainty concerning the use and validity of data messages in contract formation, whether as a result of human intervention or otherwise

(b) The provision should be clear that between the originator and the addressee of an electronic message, a declaration of will or other statement should not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication.

## 2.9 Attribution of data messages.

Certain "default" rules or presumptions have been developed by the law over many years in terms of how the court, in certain circumstances, will deem a purported state of affairs to be a fact or the truth unless proven otherwise. In the absence of these presumptions, a party trying to prove a contract or a certain state of affairs may find it unduly burdensome or even impossible to prove or defend a claim. There may be a question as to whether an electronic communication was in fact sent by the person who is indicated as being the originator. In the case of a paper-based communication, the question would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, unauthorised person may have sent the message but the authentication by code, encryption or the like, might be accurate.

Due to the impersonal (not face-to-face) and instantaneous nature of e- commerce transactions, commercial practice requires the law to provide some measure of certainty in this regard. The law ought to deal with the issue of attributing an electronic communication to its purported originator by establishing a legal presumption that in certain circumstances a communication would be considered as a message sent or authorised by the originator. Such a presumption must be qualified where the addressee knew or ought to have known that the electronic communication was not that of the originator.

In traditional transactions, no express presumption of attribution exists. However, in terms of the doctrine of "estoppel", a purported originator who never sent nor authorised a communication to be sent, may nevertheless be held bound in law if his negligent conduct, whether by action or omission, induced a reasonable belief of authenticity in the mind of the addressee, which caused the latter to act thereon to his/her peril. Due regard should be taken that legal presumptions, if any, would apply only in the absence of contractual arrangements governing attribution, for example, the use of certification authorities.
Article 13 of the Model Law creates rules entitling the addressee to assume that a data message is that of the apparent originator (attribution) and that the data message as received is the same as that sent (message integrity). Although article 13 does not directly assign responsibility for unauthorised messages or messages altered in transit, the effect of the article 13 rules, is to allocate the risk of loss arising from unauthorised or altered messages to the apparent originator rather than the addressee. These issues are considered further below.

### 2.9.1 Article 13(1) and (2) -attribution rules.

Paragraph (1) and paragraph (2)(a) reflect the existing common law that a data message is to be treated as that of the originator if it was sent by the originator itself or by a person who had the authority to act on behalf of the originator in respect of that data message. Paragraph (2)(b) expands on existing agency law concepts by binding an originator to messages sent by information systems programmed by or on behalf of the originator. This seems too broad, as it appears to make the originator responsible even if the programming or the data on which the program operates is altered by a third party or a computer virus. The rule in paragraph 2(b) ought to be limited to data messages that are sent automatically in accordance with the originator's programming.

### 2.9.2 Paragraph (3)(a) -attribution to originator on basis of use of and reliance on a previously agreed authentication mechanism.

Paragraph (3)(a) provides that the addressee is entitled to regard a data message as being that of the originator where the addressee properly applied an authentication procedure previously agreed to by the originator. In other jurisdictions, which have a similar attribution rule, the rule is limited to authentication procedures that meet stipulated standards of security and reliability. These standards focus on the physical and logical security of the access device through which the authentication procedure is operated because the access device may be the weakest point in the authentication security chain. Such a limitation is preferable because a presumption of attribution for any and all authentication procedures cannot be justified when the security and reliability of such systems varies so markedly as to prevent a factual basis for such a presumption.

The question of how standards of security and reliability are to be established and administered need to be addressed. The options include: setting standards in legislation and/or a form of delegated instrument; allowing a body to approve authentication procedures as conforming to the set standards by a prescribed body or leaving the courts to determine after the fact whether the procedure used in the particular case met the standards and should obtain the benefit of the attribution rule.

### 2.9.3 Paragraph (3)(b) - attribution to originator because of unauthorised sender's relationship with originator or agent.

Paragraph (3)(b) entitles the addressee to regard a message as being that of the originator if the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own. While it is not clear from the drafting of paragraph (3)(b), the UNCITRAL Guide to Enactment makes it clear that this provision is only intended to apply where there is negligence on the part of the alleged originator and is not intended to impose a strict attribution rule

### 2.9.4 Paragraph (4) -displacing theparagraph (3) attribution rules.

Paragraph (4)(a) provides that paragraph (3) does not apply as of the time that the addressee had notice from the originator that the data message is not that of the originator and had reasonable time to act accordingly. This is a reasonable qualification on the paragraph (3) rules.

Paragraph (4)(b) provides that paragraph (3)(b), does not apply at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator. Paragraph (4)(b) should also apply to the attribution rule in paragraph (3)(a). If it did not, the law would condone unconscionable conduct or at least wilful blindness.

### 2.9.5 Paragraph 13(5) - message integrity.

Message integrity in this context means that the content of the message received is the same as the content of the message sent. Article 13(5) provides that where the data message is that of the originator or is deemed to be that of the originator, then the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

Paragraph (5) places the risk of alteration in transit of a data message (for any reason including error, malfunction or fraud) on the originator or deemed or presumed originator. However, this result is not conditioned on the use by the originator and addressee of a procedure designed to ensure message integrity (such as a digital signature that uses a message digest). For example, in the case of article 13 the procedures, which give rise to a presumption of attribution, must relate to identifying the originator but need not relate to message integrity. The use of a procedure that satisfies the attribution requirements of article 13 creates no factual basis for the message integrity rule in paragraph (5).

Legislation should not create a rule allocating the risk of error or fraud in transmission to the originator unless the originator has used a procedure for establishing message integrity, the addressee has properly applied that procedure to the data message and reasonably relied on the results of that procedure, and, as discussed above in relation to attribution, the procedure meets minimum standards of security and reliability.

The use of signatures on paper for commerce at a distance (by mail or facsimile) involves the risk of forged or unauthorised signatures. The law of agency will often entitle the addressee in the case of unauthorised application of a genuine signature to assume that the apparent signer is bound. The presence of the apparent signer's name or letterhead or other indicia of authority will usually be good evidence that the signature is genuine. But the apparent signer is free to adduce evidence of forgery or unauthorised use and, in general, the addressee takes the risk that the signature was a forgery and therefore not binding on the apparent signer.

Attribution rules agreed on by the parties in specific contexts are more likely to produce efficient and fair allocations of risk than general legislative rules which apply to a wide variety of data messages and authentication methods. However, we are mindful of the need to protect parties in a significantly disadvantaged bargaining position from having unfair attribution and risk allocation rules imposed on them through contract. This problem can be dealt with by providing that parties can establish their own attribution and risk allocation rules by agreement but that a party cannot rely on agreed rules of attribution unless it is fair and reasonable to do so in all the circumstances. A non-exhaustive list of matters relevant to evaluating fairness and reasonableness includes:

(a) the reliability and security of any procedures which are used by the originator and addressee to authenticate the originator of the data message or to ensure that the content of the message received is the same as that which was sent;

(b) the reliability and security of the access device used by the originator to operate such procedures.

Addressees should be able to rely on the rules of agency and should be free to adduce evidence of forgery or unauthorised use. The legislated attribution rules should not go beyond restating the common law. This means that, as in paper-based commerce, addressees will have to manage the commercial risk of forgery or unauthorised signature. They can do this by requiring reliable authentication methods or seeking additional authentication indicia, which create a strong evidential basis that, the apparent originator did send the data message. Where an addressee and originator regularly exchange messages they can agree on specific attribution rules for their communications in a trading partner agreement.

**Recommendation 12.**

(a) In general, issues of attribution and message integrity should be left to determination by agreement between the parties. Disputes can be determined by the courts.

(b) For cases where parties do not determine these issues by agreement, default provisions on attribution in the form of Article 13 of the Model Law, should be enacted.

(c) Due regard should be taken that legal presumptions, would apply only in the absence of contractual arrangements governing attribution e.g. the use of certification authorities

(d) Legislation should provide that where parties agree on rules of attribution and message integrity a party should not be allowed to rely on the agreed rules unless it is fair and reasonable to do so in all the circumstances

(e) As the market develops there may be a need for the development of more detailed attribution rules.

## 2.10 Acknowledgement of receipt.

This issue is specific to the use of data messages, although analogies can be drawn with other rules of law. Article 14 of the Model Law deals with a number of the legal issues arising from the use of acknowledgments in electronic commerce. It does not deal with the legal consequences that may flow from the use of an acknowledgment of receipt, apart from establishing receipt of a data message. In cases where there is a failure of acknowledgment, the Model Law treats a data message as if it had not been sent. To the extent that existing legislation or common law deals with these issues, we propose to restate the existing legislation by enacting a provision of Article 14 of the Model law.

**Recommendation 13.**

The provisions of Article 14 should be enacted into our law to restate the common law rules and any other existing statutory provisions to apply in the context of electronic or data messages.

## 2.11 Time and place of dispatch and receipt of data message.

To test and enforce compliance with the existing rules of law, it is important to ascertain the time and place of receipt of information. The use of electronic communication techniques makes it difficult to ascertain the time and place of contracting. It is not uncommon for users of electronic commerce to communicate from one country to another without knowing the location of any information systems through which the communication is effected. Furthermore, the location of certain communication systems may change without either of the parties being aware of the change. The question is whether the law should take into account the location of information systems and their components; or whether there are more objective criteria, such as the place of business of the parties, that should be considered.

In terms of Ugandan law, there are both statutory and common law methods applied by courts to establish the time and place of contracting. The basic distinction in either method is the mode of delivery or communication used. In postal communications the transaction is concluded at the place and time of postage. In the other mode of direct and interactive communication, (e.g. the telephone) the transaction is concluded at the place and time of acceptance. A question arises whether these rules provide adequate solutions or guidance where parties contract by electronic means (e.g. by exchange of email)? The time when and place where an e-commerce contract is concluded are fundamental to determining whether Ugandan courts have jurisdiction to adjudicate a dispute involving both local and foreign nationals and, if so, which country's laws our courts would apply. There is thus uncertainty as to how rules applying to dispatch and receipt of paper documents are applicable to data messages. Specific rules are required to ensure uniformity and certainty.

Article 15 recognises that for the operation of many existing rules of law it is important to ascertain the time and place of dispatch and receipt of information. The test with respect to time of dispatch under article 15 relies upon the data message entering an information system outside the control of the sender. The approach in article 15 should be followed.

With respect to time of receipt, article 15 sets out a series of rules, which apply in different circumstances depending upon agreement between the parties to the communication and whether or not a particular information system had been designated for the purposes of that communication. The basis test, in the case where an information system has been designated, is that the information has entered the designated system and is retrieved by the recipient. Where no information system has been designated, the test is when the information enters an information system of the recipient. A simpler formulation, which in the first instance relies upon the recipient's ability to retrieve the information and, as a fall back position, upon the information coming to the attention of the recipient, is preferable for purposes of interpretation and application. This approach is preferable to the approach in article 15.

The Unidroit Principles of International Commercial Contracts contemplate "receipt" of an offer by an addressee's computer, fax or telex. Although it is not quite clear what would constitute such "receipt" in the case of a computer, the notes do indicate that the particular communication in question need not come into the hands of the addressee. It is sufficient that it be placed in the addressee's mailbox or be received by the addressee's fax, computer or telex. This is presumably analogous to a message entering an information system of the recipient, but nothing further is required. It is our view that the simpler and preferable approach is adopt a provision, where reliance is upon the recipient's ability to retrieve the information and, as a fall back position, upon the information coming to the attention of the recipient.

Regarding the place, Article 15 reflects the fact that the location of information systems is irrelevant to the use of electronic communications and adopts a more objective criterion, namely the place of business of the parties. A similar approach is adopted basing the place of dispatch and receipt on the place of business. Similarly, the Unidroit Principles of International Commercial Contracts focus upon place of business or mailing address for the giving of notices and place of business for the performance of a contract. The approach in article 15 should be followed.

Where the originator and the addressee are in different time zones, the tests set out in article 15 have the potential to create the situation where a message could be deemed to have been received by the addressee before it was sent by the originator. Accordingly, all time should be referenced to Universal Time/Greenwich Mean Time.

**Recommendation 14.**

To achieve certainty in the use of data messages for commercial transactions, rules on time and place of dispatch and receipt of data message should be developed. Article 15 of the Model Law provides a useful model, although an additional formulation of the rule with respect to time of receipt and a provision dealing with the potential ambiguity created by time zone differences would add value to the provision enacted.

## 2.12 Allocation of liability.

The allocation of risk and liability arising in connection with the use of electronic technology, as well as the limitation of liability, is not addressed in the Model Law. An earlier draft of the UNCITRAL Model Law contained a provision on liability, under which the parties were held liable for direct damages arising from

circumstances beyond their control. This provision was later deleted, as it was considered by the Working Group that the Model Law did not introduce duties additional to those existing under the applicable law and the contractual agreements of the parties. Although it was agreed that the issues of liability and allocation of risk in electronic communications would need to be reconsidered in the context of future work, it was considered premature to engage in a general debate on those issues in the context of the Model Law.

The preparation of statutory provisions covering all aspects of liability in relation to the use of electronic means of communication, including liability of the parties and of service providers, and the position of innocent third parties, is desirable to create legal certainty and assist the development of electronic commerce. The contractual provisions on allocation of liability are only effective as between the parties. Furthermore, the enforceability of certain contractual rules, like exclusion clauses, may be limited by the applicable national law. The absence of a provision on attribution of liability nor about any limitation of liability creates where in the event of any damage arising directly from a breach, the liability will 'lie where it falls'. It was not considered necessary when drafting to limit a party's liability to the detriment of another.

There is thus a need for a set of uniform rules, which would clearly set out the liability of the parties, as well as that of service providers and intermediaries, and protect the interests of innocent third parties. On the other hand, the allocation of risk and liability arising in connection with the use of EDI, as well as the limitation of liability, is addressed in some interchange agreements. Questions such as liability for breach of obligations imposed by interchange agreements, communication failure, system breakdown, error in communication, liability of third party service provider, exclusion from liability for indirect or consequential damages, and cases of *force majeure* are covered to a varying degree by some interchange agreements.

Some interchange agreements include provisions making the parties liable for any loss or damage directly caused by their failure to perform their obligations under the Agreement, subject to certain exclusions. Article 11 of the European Model EDI Agreement states:

> 11.1 No party to this Agreement shall be liable for any loss or damage suffered by the other party caused by any delay or failure to perform in accordance with the provisions of this Agreement, where such delay or failure is caused by an impediment beyond the party's control and which could not reasonably be expected to be taken into account at the time of conclusion of the Agreement or the consequences of which could not be avoided or overcome.

The parties are usually held liable for any loss or damage directly arising from the act or omission of an intermediary engaged to perform certain services. Article 11 of the European Model EDI Agreement, for example, provides:

> 11.3 If a party engages any intermediary to perform such services as the transmission, logging or processing of an EDI message, that party shall be liable for damage arising directly from that intermediary's acts, failures or omissions in the provision of said services.
>
> 11.9 If a party requires another party to use the services of an intermediary to perform the transmission, logging or processing of an EDI message, the party who required such use shall be liable to the other party for damage arising directly from that intermediary's acts, failures or omissions in the provision of the said services.

Some interchange agreements impose an obligation on the sender to ensure the completeness and accuracy of data messages sent. The sender is not, however, held liable for the consequences of an incomplete or incorrect transmission if the error is reasonably obvious to the recipient, in which case the recipient must immediately inform the sender. Other agreements impose an obligation on the receiving party to notify the sender if any

transmitted message is received in an unintelligible or garbled form, provided that the sender can be identified from the received transmission.

**Recommendation 15.**

The preparation of statutory provisions covering all aspects of liability in relation to the use of electronic means of communication, including liability of the parties and of service providers, and the position of innocent third parties, is desirable to create legal certainty and facilitate the development of electronic commerce.

## 2.13 International framework.

The inherently global nature of today's network environment challenges the abilities of national governments to address issues of electronic commerce on their own. In fact, uncoordinated, inconsistent national policies for electronic commerce, no matter how well intentioned could be worse than no action at all, and it is generally agreed that an internationally co-coordinated approach is needed.

**Recommendation 16.**

To facilitate the implementation of electronic commerce, Uganda should actively promote consideration and wide adoption of the principles of the UNCITRAL Model Law internationally and take appropriate action in international area.

# CHAPTER 3

# JURISDICTION ISSUES IN ELECTRONIC TRANSACTIONS.

The intersection between substantive rights and liabilities in traditional commercial transactions, electronic commercial transactions and international transactions raise key legal issues. The areas that are problematic involve substantive liabilities in areas of contract, tort, and general civil law rights. The international issues covered are: jurisdiction; natural forum; jurisdiction clauses; interlocutory remedies; and the enforcement of foreign judgments and arbitral awards.

## 3.1 Jurisdiction in personam.

Before a Ugandan court can adjudicate over any dispute and issue a legally binding decision, it ought to have jurisdiction over the parties. Courts generally assume jurisdiction over defendants when the originating process issued by the court are served upon them. In international disputes, the same procedure may be used when the defendant is either physically present in the jurisdiction, or has submitted to the jurisdiction by agreement with the plaintiff, or by his own conduct in setting up a counterclaim, filing a defence, or by taking any other step that is inconsistent with his denial of the jurisdiction of the court over him. In all other cases, leave has to be granted by the court to serve the writ outside the jurisdiction. There are many grounds for the service of writ out of the jurisdiction, with the principal grounds commonly invoked in commercial transactions being:

(a) the connection between the defendant and Uganda: where the defendant is domiciled, resident, carrying on business, or has property in Uganda or where the defendant is a necessary party to proceedings already within the jurisdiction of the court;

(b) the connection between the contract and Uganda: where the contract is made within the jurisdiction and is governed by Uganda law, contains a Uganda jurisdiction clause or where the breach of the contract is committed in Uganda; and

(c) the connection between the cause of action and Uganda: where the cause of action arises in Uganda; or where a tort has been committed in Uganda, or some damage is suffered in Uganda in respect of a tort wherever occurring.

The bases of jurisdiction are generally adequate for global commercial transactions. However, there are a few specific difficulties:

## 3.2 Contract.

There are two aspects of this ground of jurisdiction – the legal test and the factual test. The first question that needs to be answered is determine the issue of which law determines where the contract is made i.e. by the law of the forum (*lex fori*), or the law governing the contract (the *lex caus*ae), or some other law (e.g., in the case of a contract governed by the Vienna Convention, (the Convention itself). The law that governs the question of formation will set out rules on when the contract is formed, and the final point of contact determines where the contract is formed. This will usually be either the point where the acceptance is sent or where it is received.

In the context of electronic commerce, the agreement may be formed using variety of technology, e.g. electronic mail, cgi-bin, JavaScript or a java application. Where the processing of communications is done becomes rather arbitrary. For example, in electronic mail, the receipt is through a mail server and finally the client machine, and the processing may be done either at the mail server or the client end. In cgi-bin, the processing is done on the server. In JavaScript and java, the processing is done at the client end. The processing may include some criteria testing to determine whether to make an offer/accept an offer, make a counter-offer, etc. It will therefore be arbitrary where the actual point of acceptance takes place.

If one were to apply the factual test the question would be "were significant [or essential] steps taken within the jurisdiction to conclude the contract"? This contrasts with the legal test, which focuses on issues of legal formation, and goes back to the question of factual connections with the jurisdiction. Additionally, in traditional commercial transactions, it was the practice that contracts were concluded face to face and therefore the place where the contract was made had a close connection with the dispute. This test is now outdated and a factual test would be more appropriate.

### 3.3 Tort.

The Uganda court may grant leave for service out of jurisdiction "where the claim is founded on a tort committed in Uganda". In case of defamation on the Internet, when can a tort be said to have been committed in Uganda? Under common law, leave can be granted, "where the claim is wholly or partly founded on, or is for the recovery of damages in respect of, damage suffered in Uganda caused by a tortuous act or omission wherever occurring". There are two aspects, which can cause problems in respect of a tort committed in the context of global electronic commerce. The first problem arises from the placement of the phrase "wholly or partly", which grammatically qualifies only the claim that is founded on damage suffered, but does not apply to the claim for the recovery of damages in respect of damage suffered in Uganda.

Some torts are founded on damage (e.g., negligence), and in such cases, so long as significant damage is suffered in Uganda wherever the tort has occurred, the court has jurisdiction to hear the case and grant damages for all damage suffered anywhere in the world as a result of that tort. Other torts (e.g., defamation) are not founded on damage, and so must necessarily be a claim for the recovery in respect of damage suffered in Uganda. Because the phrase "wholly or partly" does not apply to this type of claim, the jurisdiction to adjudicate is restricted to the claim for losses incurred in the jurisdiction. A provision phrased in such a way that treats both types of claims consistently would be preferable. A simple change of wording to "the claim is, wholly or partly, founded on, or for the recovery of damages in respect of damage suffered in Uganda caused by a tortuous act or omission wherever occurring".

The second problem occurs in a case where significant acts can be said to occur within the jurisdiction, but neither the tort nor any damage occurred in Uganda. In such a case, Uganda has an interest in adjudicating the case, but there is no provision for any service out of jurisdiction.

### 3.4 Natural forum.

Even if the court would otherwise have jurisdiction to hear the case, it may decide not to hear the case if the action is so closely connected to another jurisdiction that it thinks that, under all the circumstances, it is not the most appropriate forum to hear the case. Hence, the satisfaction of either the common law or statutory grounds of jurisdiction still leaves the Ugandan courts with discretion to decide whether the case should proceed in Uganda.

### 3.5 Jurisdiction clauses.

The jurisdiction clause is an important technique in drafting international agreements. Most courts in the world will give effect to such a clause. The advantages of having such a jurisdiction clause is that it provides certainty of the forum. However, jurisdiction clauses may be onerous, especially in consumer contracts. It is possible to evade consumer protection laws by getting the consumer to agree to have the case heard in a jurisdiction where such laws would not apply (generally, in conjunction with a choice of foreign law to govern the contract). There is no specific protection against unfair jurisdiction clauses. There are, however, instances where courts may decline to enforce such clauses where giving effect to the clause would amount to avoiding the mandatory provisions of the legislation.

### 3.6 Civil liability.

Under this section we have made a brief survey of the civil liabilities that are likely to arise in the context of

electronic commerce, focusing on contract and tort (defamation).

### 3.7 Contract.

As a general rule, the common law contractual rules can be applied to electronic commerce without great difficulty. Contracts made on the information highway are the same as contracts made through traditional means. The methods of contracting and performance are different, so the application of the rules will also necessarily be different.

The UN Commission on International Trade Laws Working Group on Electronic Commerce proposed that the rules on incorporation by reference be standardized. Another area proposed for study was the application of terms like "offer', "acceptance", "delivery" and "performance" in the context of electronic commerce. Yet another area that has been proposed for future study by the Working Group is that of the standard of liability of service providers in the absence of express party agreement: including the scope of responsibility assumed; the effect of such agreements on third parties; the allocation of risks of unauthorised actions; and the extent and effect of mandatory warranties.

These proposals, like any project on standardising commercial rules of conduct on a global scale, are laudable efforts, and the progress should be monitored. However, these proposals may involve fundamental changes to some contractual rules that have been in effect for centuries in the common law. If we are going to alter the common law, we want to make sure that whatever we put in its place meets with internationally acceptable standards. Hence, the international situation should be monitored, and a satisfactory level of international acceptability must be attained before the law should be reformed.

#### 3.7.1 Formation.

It is important to understand when a contract has been formed in the context of jurisdiction issues discussed above. What determines where the contract is formed for jurisdiction purposes? The place where the contract is concluded also has some bearing on the implied choice of governing law. The question of formation is essential, if any of the parties dispute the existence of an agreement, and the point of formation can also be important if there has been a purported revocation of the offer. In general, common law systems take an almost universal view that a contract is formed when the acceptance has been communicated to the offeror.

The common law system also adopts the postal acceptance rule, which states that an acceptance is deemed to be communicated to the offeror once it is posted, on the assumption that the postal system is infallible. For instantaneous communication, the general rule of receipt of acceptance by the offeror still applies. What is not certain are the intermediate types of communication like unmanned faxes, faxes sent after office hours, electronic mail, and modern unmanned communication paradigms like cgi-bin, JavaScript, and Java applications. The rules of offer and acceptance are concerned with allocation of risk. We have proposed the adoption of the UNCITRAL Model Law Article that set out rules on when messages are considered sent or received which we believe may be helpful in the meantime as the international situation is monitored.

### 3.8 Defamation.

One problem with defamation on electronic medium is whether the statement amounts to libel or slander. Is Internet communication broadcasting in the conventional sense? Another problem transpires where the defamation occurs outside the jurisdiction. The Uganda courts have jurisdiction only in respect of losses suffered in Uganda, even though the same publication may have resulted in losses elsewhere. However, the place where the financial damage is suffered does not necessarily coincide with the place of publication. What of defamation in cases where the publications have occurred in many different jurisdictions.? Each publication is considered a different tort, and the court has no power to consolidate actions outside its jurisdiction.

A significant problem that arises in the context of electronic defamation is the liability of the intermediary, who may be the access provider, service provider, web administrator, web mall operator, licensees, etc. Are they common carriers, publishers and distributors immune from liability? In the common law system, the immunity

of the common carrier in defamation law is an unknown concept, as publishers equally liable like the author. There are two aspects of the common law in this respect that require clarification. The first is whether an intermediary is a publisher or a distributor. This causes tremendous difficulty for the new age of electronic communications, as the paradigms established in the physical world of printing in the last century are not very helpful in the electronic context. Secondly, if the intermediary is a distributor, how is the defence of innocent dissemination applicable to it?

Again there are difficulties because the law was established for physical medium where the level of control over information flow is much higher. Much concern has been expressed about the effect of intermediary liability on the viability of the Internet as a commercial medium. There are a few policy options at different levels. First, the question is whether to reform the law of defamation generally, or just for electronic commerce or electronic media. On the one hand it is to distinguish technically as well as on policy grounds, the traditional and the new media. On the other hand, the policy implications for the liability of the players in the traditional media must also be considered. Secondly, whether to overhaul the law or to make sufficient modifications to raise the level of confidence of the intermediaries.

The UK approach (Defamation Act 1996) is to modify the law for all media (i.e. traditional print and broadcast, as well as new electronic media), make no fundamental changes to the rules of liability, but to add a new defence of absence of responsibility for publication. Basically, the defendant can invoke the defence if he can show that he was not responsible for the publication. Responsibility is defined in a negative way: if he is not the author, editor, or publisher, had taken reasonable care in the publication, and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement, then he has a defence. What is attractive about the Act is that it specifically addresses questions arising in electronic communications contexts. There is little harm in adopting similar legislation, and if it has the effect of boosting confidence in electronic commerce, then it would be a good thing.

### 3.9 Consumer protection.

Uganda has little by way of consumer protection law. There are implied terms in the Sale of Goods Act, on warranty of title, merchantability and fitness of purpose, but they can be excluded by agreement, or by the simple expedient of a foreign proper law. The Act also does not apply to services. This may be an important point for electronic commerce, as the prevalent judicial view appears to be downloaded software is a service and not a good. However, any consideration of consumer protection should be done as a matter of general policy, and there is no reason to restrict the protection to electronic commercial transactions. If any review is done, the territorial scope of the protection should also be borne in mind.

**Recommendation 17.**

In summary, the following recommendations are made-

(a) Review the issue of intermediary liability for defamation.

(b) Monitor progress of international discussions on uniform contract rules for electronic commerce, but make no changes for the time being.

(c) Review the matter of consumer protection, in both domestic and international transactions.

(d) Review the jurisdictional rules for service out of jurisdiction for contract, tort and restitution.

(e) Review the rules for interim relief and cross-border remedies for international litigation.

(f) Review the possibility of service of writ and other documents by electronic media.

# CHAPTER 4

# ELECTRONIC SIGNATURE LEGISLATION.

## 4.1 Why do you sign electronic documents.

Traditionally, a signature is any symbol that is made with the intent to sign a document. The definition of "signed" includes "any symbol" so long as it is "executed or adopted by a party with present intention to authenticate writing. The primary focus is on the "intention to authenticate" a document. To understand the importance of signature to an electronic transaction, it is important to consider why a signature might be necessary. Essentially, there are four reasons why an electronic signature might be appropriate for use in connection with an electronic transaction. They can be summarised as follows-

(a) Expression of intent - First and foremost, we sign documents to evidence our intent to authenticate the document. The nature of the signer's intent will vary with the transaction, and in most cases can be determined only by looking at the context in which the signature was made. A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate's request for funding of a project, confirmation that a signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.

(b) Legal requirement - Second, we sign documents because there is some law or regulation that requires the presence of a signature before the document will be considered legally effective.

(c) Identity - With paper transactions, signatures are sometimes used to identify the person agreeing to be bound by the document, although this is not normally true (e.g., you sign a check to authenticate it, but not necessarily to identify yourself, since your name is typically printed on the check). In the electronic environment, however, where the parties are remote and often not otherwise known to each other, a signature frequently serves the purpose of identifying the signer.

(d) Integrity - A signature can also be used to ensure document integrity - that is, to ensure that the document has not been altered since it was signed. It is for this reason, for example, that parties to a multi-page contract will sometimes initial each page of the contract. However, on a 10-page paper document, a signature on page 10 does not verify the integrity of the first 9 pages. In the electronic environment, by contrast, certain types of signatures (e.g., digital signatures) can play an important role in verifying the integrity of the entire document.

In electronic transactions, the signature functions of identity and integrity are a key requirement. When transactions are automated, and conducted over significant distances using easily altered digital technology, the need for a new way to ensure the identity of the sender and the integrity of the document becomes pivotal. Thus, electronic signatures are often used even when not otherwise required by law. Unlike the world of paper-based commerce, where the requirements of a signed writing most frequently serves the function of showing that an already identified person made a particular promise, in the e-commerce world, a requirement of a signed electronic message serves not only this function, but the more fundamental function of identifying the person making the promise contained in the message. This function is very critical in e-commerce because there are few other methods of establishing the source of an electronic message.

## 4.2 What is an electronic signature and how can you sign an electronic record.

There are many different methods by which one can "sign" an electronic record. In all cases, electronic signatures are represented digitally (i.e. as a series of ones and zeroes), but they can take many forms, and can be created by many different technologies. Examples of electronic signatures include

(a) A name typed at the end of an e-mail message by the sender;

(b) A digitised image of a hand-written signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics);

(c) A secret code, password, or PIN to identify the sender to the recipient (such as that used with ATM cards and credit cards);

(d) A unique biometrics-based identifier, such as fingerprint, voice print, or a retinal scan;

(e) A mouse click (such as on an "I accept" button);

(f) A sound (e.g., the sound created by pressing "9" on your phone to agree).

(g) A "digital signature" (created through the use of public key cryptography).

For clarity a digital signature is simply a term for one technology-specific type of electronic signature that involves the use of public key cryptography to "sign" an electronic record. An electronic signature is essentially a "process". The "process" of clicking a mouse can qualify as a signature e.g. standard Web page click-through process. For example, when a person orders goods or services through a vendors' web site, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks "I agree," the person has adopted the process and had done so with the intent to associate the person with all the record of that process.

We cannot give an exhaustive list of all the methods by which one can electronically sign a document. There are other ways of signing an electronic document, and presumably many more will be developed in the future. However, all forms of electronic signature must be trustworthy. It is now a truism, that beyond the threshold issue of legal enforceability, the second primary concern of parties to an electronic transaction is the pivotal question of trust.

To say that an electronic transaction is enforceable is one thing and to have a sufficient degree of trust in an electronic message is another. Trust is essential to electronic commerce, and it varies from transaction to transaction, largely depending on how high the stakes are. For example, the level of trust required for an online merchant to ship $200,000 worth of tires is higher than what is required for an online bookstore to ship a $20 book. Likewise, a bank will require even greater assurances before it will make a multimillion-dollar funds transfer in real time in reliance on an electronic message.

The importance of trust for the success of e-commerce is widely recognised. For example, the Commission of the European Communities noted that:The first objective is to build trust and confidence. For e-commerce to develop, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce.

Trust, of course, plays a role in virtually all commercial transactions. Regardless of whether the deal is struck in cyberspace or in the more traditional paper-based world, transacting parties must trust the messages that form the basis for the bargain. Trusting a message, from a legal perspective, requires consideration of the authenticity and integrity of the message, as well as an assessment of whether the message is non-repudiable by the sender in the event of a dispute.

### 4.3 Authenticity - who sent the message.

Authenticity is concerned with the source or origin of a communication. Who sent the message? Is it genuine or a forgery? A party entering into an online transaction in reliance on an electronic message must be confident of the source of that message. For example, when a bank receives an electronic payment order from a

customer directing that money be paid to a third party, the bank must be able to verify the source of the request and ensure that it is not dealing with an impostor.

Likewise, a party must also be able to establish the authenticity of its electronic transactions should a dispute arise. That party must retain records of all relevant communications pertaining to the transaction and keep those records in such a way that it can show that the records are authentic. For example, if one party to a contract later disputes the nature of its obligations, the other party may need to prove the terms of the contract to a court. A court, however, will first require that the party establish the authenticity of the record that the party retained of that communication before the court considers it as evidence.

### 4.4 Integrity - has the message been altered.

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage? The recipient of an electronic message must be confident of a communication's integrity before the recipient relies and acts on the message. Integrity is critical to e-commerce when it comes to the negotiation and formation of contracts online, the licensing of digital content, and the making of electronic payments, as well as to proving the transactions using electronic records at a later date. For example, consider the case of a consultant who submits his/her bid proposal to a client online. The consultant must be able to verify that the proposal has not been altered. Likewise, if the client ever needs to prove the amount of the consultant's bid, a court will first require that the consultant establish the integrity of the record he retained of that communication before the court will consider it as evidence in the case.

### 4.5 Non-repudiation - can the message be proved in court.

Non-repudiation is the ability to hold the sender to his communication in the event of a dispute. A party's willingness to rely on a communication, contract, or funds transfer request is typically contingent upon having some level of comfort that the party can prevent the sender from denying that he sent the communication or from claiming that the contents of the communication as received are not the same as what the sender sent.

With paper-based transactions, a party can rely on numerous indicators of trust to determine whether the signature is authentic and the document has not been altered. These include using paper (sometimes with watermarks, coloured backgrounds, or other indicia of reliability) to which the message is affixed and not easily altered, letter head, handwritten ink signatures, sealed envelopes for delivery via a trusted third party (such as couriers and postal deliveries) or personal contract between the parties. With electronic communications, however, none of these indicators of trust are present. All that can be communicated are bits (0s and 1s) that are in all respects identical and can be easily copied and modified.

This has two important consequences. First, in many cases it is difficult to know when one can rely on the integrity and authenticity of an electronic message. This, of course, makes difficult those decisions that involve entering into contracts, shipping products, making payments, or otherwise changing one's position in reliance on an electronic message. Second, this lack of reliability can make proving one's case in court virtually impossible. For example, while a typewritten name appended at the end of an e-mail message may qualify as a signature under applicable law, that name could have been typed by anyone, and if the defendant denies the "signature", it may be virtually impossible for the plaintiff to prove the authenticity of that signature. As a result, non-repudiation is not assured in such a case, and owing to the great risk of repudiation involved, parties will take the risk of entering into e-commerce transactions.

In many respects, trust is a key element of the measurement of risk. And the need for trust can vary significantly, depending on the risk involved. Selling books on the Internet, for example, may not require a high level of

relatively low (e.g., a $20 book). On the other hand, entering into long-term, high dollar value contracts electronically may require a much higher level of trust. At a minimum, the risk of a fraudulent message must be acceptable given the nature and size of the transaction.

Thus, where the amount at issue is relatively small or the risk is otherwise low, trust in an electronic message's authenticity and integrity may not be a critical issue. If e-commerce is to reach its full potential, however, parties must be able to trust electronic communications for a wide range of transactions, particularly where the size of the transaction is substantial or the nature of the transaction is of higher risk. In such cases, a party relying on an electronic communication will need to know, at the time of reliance, whether the message is authentic, whether the integrity of its contents is intact, and, equally important, whether the relying party can establish both of those facts in court if a dispute arises i.e., non-repudiation.

### 4.6 Establishing trust through security procedures.

Establishing trust in an electronic transaction typically involves the use of a security procedure. A security procedure is a procedure employed for the purpose of verifying that an electronic signature, record, process or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or call-back or other acknowledgement procedures. Because they are designed to either verify the identity of the sender of an electronic record, or to detect an error in or alteration of an electronic record, security procedures can also have a legal effect. There are a number of security procedures that can be used to assist in establishing trust for electronic communications. These include:

(a) a digital signature;

(b) replies and acknowledgements;

(c) repeat-back acknowledgements;

(d) the use of a process or system that produces a demonstrably trustworthy document;

(e) date/time stamping;

(f) the use of trusted third parties; and

(g) encryption.

### 4.7 A digital signature.

A hand-written signature on a paper document purporting to originate from an identified source can authenticate a communication if that signature is shown to be genuine. Of course, an electronic communication cannot bear a traditional hand-written signature, but it may bear a digital signature or other digital equivalent. If a digital signature can be verified using a public key that is reliably associated with the sender, the recipient can obtain a high degree of assurance that the communication must have come from the sender.

Only the sender's public key can decrypt a digital signature encrypted using the sender's private key. Furthermore, assuming the sender's key has not been lost or compromised, the sender cannot deny having sent it. Thus a digital signature can provide a means of identifying the source of a communication and preventing a sender from repudiating that communication. A digital signature can also be used to verify the integrity of an electronic communication. If the recipient can verify the sender's digital signature, the integrity of the communication has been shown.

### 4.8 Replies and acknowledgements.

Computer systems are particularly well suited to screening incoming communications and sending a return acknowledgement to the purported sender. A log showing what was received, the identified sender, the fact that an acknowledgement was sent to the sender, and that the acknowledgement was not rebuked will help authenticate the source of a communication. Sending and retaining records of acknowledgements as well as of any responses repudiating those acknowledgements can also enhance the authenticity of communications. A reply to an earlier communication in effect authenticates the reply. This technique works equally well for paper-based and electronic communications.

### 4.9 Repeat-back acknowledgements.

The technique of sending an acknowledgement to establish an electronic communication's authenticity can be taken one step further to establish the integrity of a communication. With electronic communications, it is a simple matter not only to send an acknowledgement, but also to repeat the entire contents of the communication back to the purported sender. If the repeat-back acknowledgement is different than the original communication, the sender can alert the recipient. The sender will want to be sure to create and retain a record of the communication as received, the repeat-back acknowledgement, and any repudiation of the repeat-back acknowledgement it received or a notation that none was received.

### 4.10 Process or system.

Because electronic communications do not always have the same identifying characteristics as paper communications, it is helpful to resort to other techniques for establishing authenticity that are specially suited to electronic communications. These techniques all involve the use of a computer system to perform automated record keeping functions. For example, one can configure his/her computer to automatically archive an electronic record copy of the communications it creates and receives, which helps to establish that the records of those communications are genuine. Adopting system security controls that limit access to archival copies can further ensure the authenticity of such archival record copies. The use of such system security measures can help one to demonstrate the integrity of its records.

Another technique is to configure the user's computers to create a log of all incoming and outgoing communications and to cross-reference this log information to archived records. Log information showing the source of the record and the time of its creation or receipt provides further proof of its authenticity.

### 4.11 Date or time stamping.

A digital date/time-stamp provides another way to verify that a communication has not been changed. A date/time-stamp is issued for a message digest of the communication. This fixes the content of the message digest as of a certain date. To later verify the integrity of the communication another message digest is created for the communication. If it matches the date/time-stamped message digest, the communication has not been changed.

### 4.12 Trusted third-parties

A party can establish the integrity of a communication by sending and receiving all of its electronic communications through a neutral third party that can retain a copy of each communication. Assuming that this third party is trustworthy, each party can then rely on the third party in the event that the integrity of a record of a communication is questioned.

## 4.13 Encryption.

A sender, who wants to send an electronic communication to a recipient and keep it confidential, can encrypt the communication. The security measures that can be taken to help ensure that electronic communications and records are trustworthy may not yet be readily accepted, but their legal effectiveness is already being recognised. A person who wishes to transfer funds electronically can do so by transmitting an electronic message, called a payment order, to his bank. Security procedures can be used in the message instead of the traditional ink signature or other paper-based security measures. The bank receiving a payment order needs something objective on which it can rely in determining whether it may safely act on that order. The bank can rely on security procedures as a substitute for the traditional time-tested requirement of a signature. The "security procedures" rather than "signatures" can be used for verifying transactions and apportioning liability.

## 4.14 The law and trust in e-commerce/legislative approach.

A trustworthy electronic signature is a precondition to enforceability as a signature. This approach typically requires that electronic signatures possess four attributes i.e.

(a) it must be unique to the person using it;

(b) it must be capable of verification;

(b) it must be under the sole control of the person using it; and

(c) it must be linked to the data in such a manner that if the data is changed, the signature is invalidated.

If all of these requirements are met, the electronic signature will be deemed to be a signature in conformity with the statutory and regulatory signature requirements within the scope of the statute and such electronic signature will be enforceable.

Other statutes have adopted a different approach. They provide that almost any form of electronic signature can be enforceable and meet legal signature requirements, They however recognise the fact that some electronic signatures are more trustworthy than others. This approach is premised on the argument that electronic signatures, like traditional signatures of ink on paper, have varying degrees of security e.g. a signature under seal or an attested or notarised signature. These signatures under the current law are more trustworthy, and equally when dealing with electronic signatures, there is need to categorise signatures into those that are more secure than others. These statutes therefore define a secure signature or otherwise a trustworthy signature. To encourage the use of those electronic signatures deemed to be more trustworthy, and to provide message recipients with an enhanced level of assurance at the time of reliance regarding the authenticity and integrity of messages using such signatures, these statutes typically provide a legal benefit in the form of an evidentiary presumption regarding the sender's identity and/or the integrity of the document.

Some statutes take a technology-neutral approach in identifying the class of trustworthy electronic signatures that qualify for such a legal benefit. An electronic signature that qualifies as a secure electronic signature enjoys a rebuttable presumption that the signature is that of the person to whom it correlates. Other technology-neutral electronic signature legislation incorporating rebuttable presumptions limited to certain types of transactions e.g. tax-related or health care usages have been enacted.

To ensure that the digital signature possesses a level of trust sufficient to warrant enhanced legal recognition, these statutes impose a regulatory structure on certification authorities who voluntarily elect to be licensed. Based on the apparent assumption that all certificates issued by licensed certification authorities are trustworthy, and that a digital signature that is created using the private key corresponding to the public key listed in such a certificate is a trustworthy signature, such legislations bestow attributes of trust to messages verifiable by such certificates

For electronic transactions, presumptions of the signer's identity and of message integrity can help to provide the necessary assurances to relying parties, thereby enabling them to engage in online commercial activities with confidence that their transactions will be easier to enforce in court if that should be necessary. Such presumptions can provide the predictability and trust necessary to rely on a message, and act accordingly, in real time. Such presumptions are based on the trustworthiness of the security procedure used to create the electronic signature, and the fact that the purported sender is more likely than the recipient to possess the information necessary to prove or disprove the validity of the signature.

Yet the use of presumptions in electronic signature legislation is an issue that has generated rather extensive controversy. Criticism has centred on concerns that consumers and small businesses that lack an understanding of the sophisticated technologies used to create the secure electronic signature may unwittingly find themselves in a situation where their failure to protect the security of their signature device (e.g., their private key) will expose them to substantial liability for unauthorised transactions made by persons who unlawfully obtained access to their signature device.

Further, it is argued that such presumptions accord greater legal status or effect to the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

An analysis of the electronic signature legislation currently enacted or under consideration reveals that electronic signature legislation is essential to facilitate e-commerce. The legislation ranges from a minimalist approach that simply authorises the use of electronic signatures in very limited circumstances, to legislation that establishes some evidentiary presumptions and default provisions that parties can contract out of, to a very formal and highly regulatory approach governing the manner in which digital signatures may be used and certification authorities may operate.

The essential question with regard to electronic signature legislation are: How far down the road will it take us in Uganda? Can the various types of legislation move e-commerce in the right direction, or might they cause unintended detours? Should we simply wait for disputes to arise and leave it to judges to transform the legal landscape? Do the laws that work remarkably well and provide predictability in the traditional, paper-based commercial world translate line for line and serve as adequate mile markers for companies blazing trails to more efficient commerce on the new electronic frontier? Given the explosion of e-commerce activity, is legislation even necessary, or are there inherent limits to the growth of e-commerce that legislation could help to overcome?

Enacting legislation designed simply to remove barriers, while an important and worthwhile endeavour, may not move us far enough toward the ultimate goal. Conversely, enacting laws or imposing regulations that force the market to use a specific business model or specific technology, or that protect against perceived problems that have not yet surfaced, might preclude the pursuit of more promising e-commerce avenues. Yet, if done properly, electronic signature legislation can, and perhaps should, be designed and enacted to accomplish two goals:

(1) to remove barriers (actual and perceived) to e-commerce, and

(2) to enable and promote the desirable public policy goal of e-commerce by helping to establish the "trust" and the "predictability" needed by parties doing business online.

These two goals might be best accomplished by enacting legislation that preserves freedom of contract while recognising that, because parties dont always resolve all issues by prior contractual agreement, limited default rules should apply when such unresolved issues arise.

Although the courts will certainly play a key role in establishing the rules that will govern online transactions, we should not automatically discount the positive contributions and early guidance that legislation can provide. Likewise, while the goal of technology neutrality is important from the standpoint of not stifling development or unfairly favouring one technology over another, we must be careful as we draft electronic signature legislation not to let neutrality become an excuse to avoid addressing legitimate new issues raised by a unique technology, or worse, use neutrality as a means to discriminate against the development of those technologies seen by most as facilitating secure e-commerce.

As we move towards the use of electronic forms of communication and documentation, to trust and confidence as integral constituents of business and commercial transactions must not only be built but must be maintained. Building such trust and confidence is a prerequisite to win over businesses and consumers to electronic commerce. It implies the deployment of secure technologies such as digital signatures, digital certificates and secure electronic payment mechanisms, and have a predictable legal and institutional framework to support these technologies. Secure technologies, such as digital signatures and digital certificates, go some way to meeting these challenges. Digital signatures enable the unambiguous confirmation of the identity of the sender and the authenticity and integrity of electronic documents. Unique to the sender and unique to the message sent, digital signatures are verifiable and non-repudiable.

Similarly, the exchange of Internet certificates through an automatic 'digital handshake' between computers provides assurance that the parties are who they say they are and helps to assess whether the service provided and the goods or services delivered are genuine. Digital signatures will be the driving force behind the development of many new services, which vary from certification (e.g. likely to identify with a public key) to fully-fledged digital notary services (e.g. adding a time stamp to an electronic document, electronic archiving etc). These services are expected to play a dominant role in the Information Society, particularly in electronic commerce. The necessary regulatory and institutional framework supporting technologies ought to be set up and fully operational particularly in areas such as infrastructure, interoperability and mutual recognition across borders.

### 4.15 Digital signatures explained.

Several different methods exist to sign documents electronically. These electronic signatures vary from very simple methods (e.g. inserting a scanned image of handwritten signature in a word processing document) to very advanced methods (e.g. using cryptography). The sub-set of electronic signatures based on public key cryptography, is often called digital signatures. The basic nature of digital signatures is that the author of an electronic document can sign his or her electronic document by using a secret cryptography key. This key must be kept private at all times by the user. The signature can only be verified with the associated public key of the author. This public key is widely known.

The idea behind this form of authentication is the confirmation of identity by proving the possession of a secret key. The author encrypts the message or a part of it with his or her secret key. The recipient of the message can check the identity of the author by decrypting the information with a public key of the presumed author. If the decryption is not successful, the recipient will not validate the message. This process of authentication relies on the public keys of the users that are accessible to all the communication partners and on a trusted relationship between the identity of the users and their public key.

Like the signature used on written documents today, digital signatures are now being used to identify authors of e-mail or other information objects of electronic data. Digital signatures can provide three important functions-

(a) Authentication - to authenticate the identity of the person who signed the data so it is known who participated in the transaction.

(b) Integrity - to protect the integrity of the data so it is possible to know the message read has

(c) Non-repudiation - to allow it to be proved later who participated in a transaction so that it cannot be denied who sent or received the data.

It should be noted that in order to create a signed message, it is not necessary to send the message itself in encrypted form. The digital signature can be appended to the message and can be verified irrespective of the form of the message itself.

Cryptography is a highly important instrument for achieving secure electronic commerce. There are a number of ways that cryptography can work in an electronic environment. The most popular method being used today is where the encoding and decoding of the message is performed using two keys: (i) a public key, which is publicly known, and (ii) a secret key, which is only known by the sender or the recipient or both. This cryptography technique is often known as 'public key encryption'. The public key can be used by anyone to encrypt a message. Only the owner of the secret key can decrypt it. Thus, if two parties want to send information to each other, they exchange their public keys. The public keys could also be retrieved from a database, which is open to the public. When X sends to Y a message, X enciphers the message using the public key of Y. Only Y can decipher the message using his secret key.

The primary advantage of public key cryptography is increased security. The secret keys do not have to be transmitted or revealed to anyone. Another advantage of the system is that the public key and the secret key can both be used for encoding as well as for decoding. Their functions are interchangeable. This means that X can encode a message with his own secret key, which Y can decode by using the public key of X. On first sight, this seems a silly method, because everybody has access to the public key of X and can thus decrypt and read the message.

This is, indeed, true. On the other hand, Y can be sure that the message can only originate from X, since he is the only one who knows the secret key. Without having contacted X before, Y can trust the authenticity of a message. It is on this technology of sharing a public key that digital signatures are based. The key pair can be generated by the user himself by running specific cryptography software. Even the recent versions of the most popular Internet communication software such as MS Internet Explorer and Netscape Communicator, allow the user to create his own key pair.

Temporarily, secret keys are being stored on the hard disc of the user's computer. The user gains access to the secret key by entering a password or pass phrase. This type of storage, however, has the disadvantage of non-mobility. The user always needs his own computer in order to put his digital signature on an electronic file. Therefore, the storage of the secret key on a removable carrier, such as a smart card, is getting more popular. The user simply inserts his smart card into a reader by which he can sign digitally.

Once a person has generated or received his public and private key, it is extremely important to keep the secret key free from access by others. If someone gains access to the secret key, that person will be able to counterfeit the key and, thus, to create digital signatures. Protection of the secret key is, however, for the user a local matter under his control or the control of a responsible site security officer. Every person bears responsibility for his own signature and should protect it from loss, theft or illegal use. Neither should the user forward his secret key to other people such as his secretary or colleague.

The user needs the public key of his partner in order to check the authenticity of his digital signature. His public key can be delivered by the partner himself but can also be retrieved from a database, which is publicly accessible. Normally, the communication software of the user will automatically check the digital signature by retrieving previously stored public keys or accessing the relevant public database.

### 4.16 Certification authorities.

The authentication procedure is based on the presumption that the public key really belongs to the signer. This

key in a public directory under somebody else's name and thus signs electronic messages in the name of somebody else. Furthermore, a public and private key pair has no inherited association with any identity; it is simply a pair of numbers. Therefore, the assurance should exist that the public key really belongs to the claimed identity.

The answer is to rely on third parties to certify public keys. A third party can guarantee the relationship between the identity and the public key. This association is achieved in a certificate that binds the public key to an identity. These third parties are known as 'Certification Authorities' (CAs) and must be accepted by all users as impartial and a 'Trusted Third Party' (TTP). In addition, the process of key certification must be full proof and should be afforded the highest level of security. The act of using a registered digital signature to sign an electronic message becomes very similar to appearing in front of a notary public to manually sign a paper.

The CA can check the identity of the user by for example passing out the certificates after a simple e-mail address check. This type of assurance is minimal, and only good for establishing a consistent presence, not for guaranteeing someone is a real person. Other certificates could be issued after receiving third party proofing of name, address and other personal information provided in the online registration. Usually this would be a check on some consumer databases.

The best identification is, of course, the personal appearance. CAs could require someone to personally take his or her application to a notary, who will check identification before endorsing it. This adds an additional layer of credibility to the certificate.

Digital certificates could contain every type of information necessary to identify the creator of the digital signature. Usually they contain the owner's public key, the owner's name, the expiration date of the certificate, the name of the Certification Authority that issued the digital certificate, a serial number and perhaps some other information. CAs sign information and thereby add credibility to the certificate. People who receive the certificate check the signature and will believe the attribute information/public key binding if they trust that certifying authority. In order to allow an automated checking of the certificates it is important that the certificates are built up in the same form. It is therefore necessary that standards be followed, describing the elements that the certificate should contain.

Many cases could exist where the certificate of somebody should not be used or trusted any more, such as an employee who leaves the company, someone's computer or smart card containing the secret key is stolen. When a certificate becomes compromised, there must be a way to call up the Certification Authority and request that the certificate is disallowed. The most common way of making the revocation public is to put it in a database, called a 'Certificate Revocation List' or CRL. The CRL can be accessed by the public to check if the certificate of a user is still valid. A Certification Authority thus must maintain two databases, a complete list of certificates and a list of revoked certificates.

Why should the user trust the CA of the other party? There is a need for both parties who use different CAs to trust each other's authority. One way to achieve this confidence is by cross-certification. This means that both CAs certify each other's public key. Another solution could be that the two CAs are certified by a third CA, functioning as a top CA. In this hierarchical CA structure each CA only needs to be certified once in order to gain trust. At the moment, most practising CAs however, are certifying themselves by simply signing their own public key and posting the certificate on their own web sites.

This self-certification is possible because the CAs rely on their trust gained from other activities, such as postal services or banking activities. In order to assess the level of trust that may be put into a CA, the CA should also provide a combination of technology (such as security protocols and standards, securing messaging and cryptography), infrastructure (including secure facilities, customer support and redundant systems), and practices - a defined model of trust and legally binding framework for subscriber activities and disputes. In short, a CA

### 4.17 Liability of certification authorities.

Liability in the world of electronic commerce is complex and the need to balance the interests of the various parties who might be involved, either directly or indirectly, in a particular transaction is always pertinent. Applying the principle that policy should be technology neutral, liability in the electronic world should, as far as possible, match that in the traditional world. However, given that there are no direct analogues of cryptography services in the world of pen and paper transactions some special rules might be needed. However, while the apportionment of liability would have to be incorporated in the legislation, the following points stand out-

(a) the purchaser of a licensed service, who would expect the licence to offer some guarantee of quality, e.g. a customer would expect due care to have been taken in generating their signature key pair, and someone buying a confidentiality service would expect the CA to take proper care of their private confidentiality keys if they stored them;

(b) a third party relying on a licensed service, who would have similar expectations, e.g. that what was stated on a Certificate was true and that the Certification Authority would have some liability if it turned out to be false, and had an effective revocation policy;

(c) the service provider, which would need to be able to manage and limit its liability would not apply for a licence if being licensed meant taking on unlimited liability. A cap on liability would constitute an advantage of being licensed by reducing the cost of liability insurance.

The national policy view could initially be reconciled by imposing a limitation onliability but which could not be decreased by contractual terms, on licensed service providers. This would, in effect, encourage CAs to apply for licences and thereby become subject to regulation. Different limits would probably be set for different services. The consumer would be protected by knowing that a licensed provider was taking on a certain level of liability. The provider's interests would also be protected by having a cap on their liability.

### 4.18 Difference between traditional and digital signatures.

The concept signature has a long tradition and is normally easy to describe. It gives basic mechanisms for secure traditional information management. A hand written signature is physically tied to a carrier (the sheet of paper), which gives borderlines and structure to the information in an immediately readable format. This 'lock' for the information, provided by the carrier and the signature representing the issuer's unique patterns of handwriting, gives the reader reasons to believe that the object originates from the individual who is seen to be the originator and the identity tribute is inherent, not given to the signatory.

Digital signatures are not immediately readable and the signature, the carrier and the signed object are not physically related to each other in the same locked and durable form. A manipulation of the data normally leaves no such traces as a manipulation in the traditional environment and portions of a signed information object may be stored on different locations for example a hard disc. The visual aspect of a traditional example is replaced by technical verification of a signed information object, stored in a computer readable format and logically tied to the signature. As the digital attribute making the signature unique for the individual is assigned, not an inherent characteristic of the signatory, the signature process may be performed by any one who has access to the secret and the procedures.

The hand written signature furnishes the information with a physically unique sign of authenticity - it is an original example. Such signed objects may be in a person's possession and can thus be a carrier of authority (e.g. power of attorney) or a certain right (e.g. bills of lading and other negotiable instruments). However, the unique aspect of a digitally signed object has to be related to a pattern of data, which may easily be copied and the duplicate will have exactly the same qualities as the 'template'. Consequently, unique existence of IT material is built upon the storing and transmittal of original contents and certain IT applications such as shipping

The management of traditionally signed objects may in name be replaced by digital equivalents. By making use of security techniques, such as digital signatures, the authenticity of the information can be maintained. The need for protection of such objects is already carefully considered in the traditional environment. An examination of electronic commerce, electronic handling of cases by administrative agencies and similar routines shows the same need for protection in the IT environment. However, the changes relate to the transition from original examples to original context has to be noticed where appropriate. Consequently, current issues are in principle traditional matters of legal protection and security, which give basic mechanisms for the information management. Instead of creating a complete new legal framework, existing achievements should be advised, as far as they are compatible with IT.

**4.19 Conclusion.**

The above discourse clearly brings forth the following legal issues.

(a) The use of electronic signatures arises in a number of areas and as such Uganda has to adapt its national legislation to the new techniques of document management.

(b) The provision of trusted services is a completely new service sector. This sector is still in its infancy, but interested market players are positioning and preparing themselves. From a legal point of view it is important to distinguish clearly between on the one hand the procedures and conditions governing the establishment of a CA and the other hand the conditions imposed on the different services provided by a CA.

(c) The establishment of a controller of certification services is necessary to institutionalise the security structure in Uganda. This may intend to impose specific establishment requirements and authorisation procedures on CAs. Others only require compliance with general provisions in the law concerning the establishment of a company.

(d) In order to ensure reliable use and legal validity, and to combat fraud and misuse, digital signatures require adequate products, key generation, key storage, certificate storage and retrieval, signature generation and verification. At a national level there is need to engender free circulation of these products.

**Recommendations 18.**

(a) Regulation of public key encryption. In order to support the rapid development of the market in terms of user demand and technical innovation, prior authorisation had to be avoided. As a means to gain the confidence of consumers, voluntary accreditation schemes for certification service providers aiming at providing enhanced levels of security should be considered

(b) Ensuring legal recognition, in particular cross borders, of electronic signatures and of certification services should be regarded as the most important issue in the area. This would involve clarifying the essential requirements for certification service providers, including their liability.

(c) The certification service providers must be able to:

  (i) Demonstrate the reliability necessary for offering certification services;

  (ii) Offer a prompt and secure revocation service;

  (iii) Verify by appropriate means the identity and capacity to act of the person to which a qualified certificate is issued;

  (iv) To employ experts in the technical and management processes so that they are adequate and correspond to recognised standards.

(d) Use trustworthy systems and electronic signature products which are adequate for the job and which ensure the technical and cryptographic security of the certification processes supported by the products;

(e) Take measures against forgery of certificates and guarantee confidentiality during the process of generating private cryptographic signature keys if relevant;

(f) Be sufficiently financially secure to provide the services and to bear the legal risk of liability for damages;

(g) Maintain a proper record keeping system for qualified certificates electronically and in particular for legal proceedings;

(h) Not to store or copy private cryptographic signature keys of a person for whom the certification service provides office key management services unless that persons explicitly asks for it;

(i) Inform consumers of the precise terms and conditions for the use of the certificate including any limitations on liability, the existence of voluntary accreditation and the procedures for complaints and dispute settlement for entering into a contractual relationship in writing using readily understandable language and a durable means of communication.The certificates' are digital attestations which link the signature verification device to a person and confirms the identity of that person. Qualified certificates must contain-

(A) The identification of the certification service provider;

(B) The unmistakable name of the holder or an unmistakable pseudonym which shall be identified as such;

(C) A specific attribute of the holder such as the address, the authority to act on behalf of the company, credit worthiness, VAT or other tax registration numbers etc;

(D) A signature verification device which corresponds to a signature creation device under the control of the holder;

(E) Beginning and end of the operational period of the certificate;

(F) A unique identity code of the certificate;

(G) The electronic signature of the certification service provider issuing it;

(H) Limitation on the scope of the use of the certificate, if applicable;

(I) Limitations on the certification service providers' liability and on the value of transactions for which a certificate is valid, if applicable.

The liability of certification providers must be clearly set out. It must include-

(a) The need to promote users' confidence both in the technologies which allow integrity and confidentiality, and in the providers of cryptography services;

(b) The law should, as far as possible, be technology neutral;

(c) The intention that licensed Certification Authorities would be in a position to offer certificates to support electronic signatures reliable enough to be recognised as equivalent to written signatures;

(d) Recognition that clear differences in approach need to be afforded to the development of electronic and digital signature services, and to encryption services;

(e) The need for new powers for law enforcement agencies to gain legal access, under proper authority and on a case by case basis, to encryption keys or other information protecting the secrecy of stored or transmitted information so as to maintain the effectiveness of the existing legislation designed to protect the public from crime and terrorism in response to new technological developments.

**It is recommended that the licencing and regulation of certification authorities should be by Uganda Computer Services because they give rise to complex IT issues.**

As can be seen from above, there are numerous recommendations relating to Electronic Signature legislation. Below is a "checklist" of issues, which should be dealt with when attempting to draft Electronic signature legislation.

| *Category of Issues* | *Examples* |
|---|---|
| *Types of Signatures to be dealt with* | *(a) electronic signatures*<br>*(b) digital signatures*<br>*(c) digital signatures with third-party certification*<br>*(d) digital signature with certificates from licensed certification authorities* |
| *Parties Affected* | *(a) subscriber*<br>*(b) certification authority*<br>*(c) recipient of electronically signed message*<br>*(d) any possible third party* |
| *Acts or Events to be given Legal Effect* | *(a) issuance of certificate;*<br>*(b) revocation of certificate;*<br>*(c) use of an electronic signature;*<br>*(d) verification of an electronically signed message;*<br>*compromise of keys.* |
| *Types of Legal Effect* | *(a) validity;*<br>*(b) obligations;*<br>*(c) remedies;*<br>*(d) liability (include limits of liability);*<br>*(e) evidence* |
| *Drafting Techniques* | *(a) prescription of standards;*<br>*(b) legal effect if standards were met;*<br>*(c) legal effect if standards were not met* |
| *Sphere of Application* | *(a) domestic only;*<br>*(b) international only (provision for cross-certifications)*<br>*(c) international and domestic.* |

# CHAPTER 5

# COMPUTER CRIME.

## 5.1 Background.

It is an inevitable feature of technological development that criminal applications follow legitimate uses as a consequence. The computer is no exception to the rule. Today, computer viruses endlessly threaten the survival of computer networks whilst the most secret information held on computer systems is at the mercy of the computer hacker. In considering the application of the criminal law to instances of computer-related conduct, a variety of issues arise. One of the most critical is whether computer-related conduct should be regarded as requiring technology-specific legislation or whether it might satisfactorily be regulated through the application of more general criminal law provisions.

The attacks on computers can be classified into those suspected to be the work of hackers and those suspected to have been carried out by script kiddies. The distinction primarily lies in the basis of the tools used, the damage (actual and potential) and the methodology. The attacks where sophisticated techniques and methodologies are used have been classified as "hacking " while the others have been classified as "script kiddies" attacks. The term "script kiddies" implies the use of ready made "hacking scripts and codes" by "kids". Thousands of "underground" websites have sprung up that offer free download of hacking tools and utilities that are increasingly being used by youngsters for committing computer crimes. This demonstrates that persons with relatively low knowledge are able to penetrate organizational networks using freely available "hacking tools".

It is important to note that various surveys in different jurisdictions have indicated that most of computer related abuses are perpetrated by disgruntled employees and business rivalries. It is also interesting to note that the percentage of incidents attributable to former employees outnumbers those attributable to business rivals. This makes the nature of computer related crime a very hard nut to crack and peculiar in the sense that it is perpetrated from within.

While computer related crimes are committed every single day, relatively few cases have been brought before the courts and in Uganda no case has come before the courts so far. Such paucity is generally regarded as being due to a range of factors. First, there is failure to report, by victims as commercial organisations avoid adverse publicity. Secondly, there is lack of adequate training within the investigating and prosecuting authorities. Thirdly, the trans-national nature of computer crime and the associated jurisdictional problems contribute to the complexity of investigating and prosecuting offenders. Finally, computers, particularly when networked, create significant forensic challenges to law enforcement agencies when obtaining evidence and subsequently presenting it before the courts.

It is obvious that computers may play a part in the commission of nearly every form of criminal activity- from fraud, terrorism, money laundering, murder to treason. A review of the appropriate Ugandan criminal law focusing on those areas that may give rise to particular problems where computers are involved is made difficult by two reasons. First, the criminal legislation in Uganda and the subsequent amendments was drafted in an era before such technology was envisaged and secondly the statutory drafting has failed to be robust enough to appropriately cope with the rapid developments in computer technology.

## 5.2 Justification for review.

Computers are playing an integral part in the functioning of our society. They are used not only, as the sophisticated repositories of vast amounts of information, but also in operational roles. In performing these roles, computers are relied on to perform functions upon which human life as well as the economic and

industrial functioning of society are dependant. Computers are used, for instance, as instruments in the administering of systems, supporting medical treatment, transport control systems, banking and financial systems, communication systems and national security. The potential danger when computers performing these functions are interfered with is very serious and cannot be overlooked.

As technology advances the risk of computers either becoming the instruments of crime or the targets thereof increases. Consequently computers are becoming particularly vulnerable to crime because of a number of factors-

(a) The storage capacity of computers is increasing rapidly which allows for the centralisation of large amounts of information.

(b) More and more computers are connected to open networks such as the Internet. This can allow the transfer of information between systems spanning the globe.

The potential danger of interference with the functioning of a computer coupled with the increased vulnerability of computers to such interference provides sufficient policy grounds for the criminalisation of the actions by means of which information can be obtained from a computer. There are a multitude of methods by means of which information can be obtained from a computer or its functioning can be interfered with. It is difficult to describe all the elements of each method in order to develop an offence for each. The common denominator among all of these methods is the obtaining of access to a computer without the requisite authority, and this is the basis for the justification of making the act of unauthorised access of a computer a punishable offence.

The unauthorised entering of the personal domain of a person is prohibited in respect of physical concepts such as a premises or a building. This personal domain also includes a person's privacy and an invasion of privacy can lead to criminal liability. In the modern society of information technology, this personal domain ought to be extended to include information which is of personal or economic value and which is stored in electronic format.

The potential danger referred to earlier becomes especially relevant when one considers the unauthorised modification of computer data and software applications. This potential danger provides sufficient justification for the criminalisation of such modification of computer data and software applications. A person's economic interest in his or her tangible property is protected by offences such as theft and malicious injury to property. The demands of our modern society, however, are not catered for when incorporeal property that resides in a computer system is considered. It then becomes important at this point to contexualise computer crime in light of the existing legal framework.

Before one can embark on the review process of computer related crime two options ought to be considered;

(a) Amending the existing law to incorporate the computer related crimes in the existing legal regime; and

(b) Formulating a new technology specific legislation

### 5.3 Data theft .

The Ugandan Penal Code has limitations in regard to controlling theft in the cyber world. First, there are a few things that are considered by the Code as capable of being the subject of theft. Information or data does not qualify as a subject of theft. The relevant section in the above respect is section 244 and the things capable of being stolen are-

(a) every inanimate thing, whatever, which is the property of any person and which is movable is capable of being stolen.

(b) every inanimate thing which is the property of any person and which is capable of being made movable is capable of being stolen when it becomes movable, although it is made movable to steal it.

Computer hardware would certainly qualify as a thing (s) capable of being stolen; but software would not fit the description. The section has connotations of the corporeal as it precludes anything, which is not physical like an idea, an electronic document, a computer program, a computer file or services. This is reinforced by Section 245 of the Penal Code, which defines theft as-

(1) A person who fraudulently and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person other than the general or special owner thereof anything capable of being stolen, is said to steal that thing.

(2) A person who takes or converts anything capable of being stolen, is deemed to do so fraudulently if he does so with any of the following intents, that is to say;

(a) An intent permanently to deprive the general or special owner of the thing of it;

(b) An intent to use the thing as a pledge of security;

(c) An intent to part with it on condition as to its return which the person taking or converting it may be unable to perform;

(d) An intent to deal with it in such a manner that it cannot be returned in the condition in which it was at the time of the conversation;

(e) In the case of money, an intent to use it at the will of the person who takes or converts it, although he may intend afterwards to repay the amount to the owner.

(3) A person shall not deemed to steal a thing unless he moves it or causes it to be moved'.

The initial qualification required of a subject matter of theft, is that it is a thing capable of being stolen, short of which any allegation of theft would have no basis. Data or information stored on a computer, are not therefore "things" capable of being stolen under the Penal Code.

### 5.4 Unauthorised access.

This is essentially the basic ingredient of computer-related crime. The first category includes those cases of unauthorized access where no data is stolen. The methods used for unauthorized access vary from use of malicious code, reverse engineering, exploiting remote dial in vulnerabilities and Internet based attacks. The second category deals with viruses, which are deliberately sent to the particular victim. This Report concerns itself with cases of planned virus attacks targeted towards specific victims. Although, this category reflects only part of the total incidents of virus attacks, it is significant because of the damage potential.

A sustained and targeted virus attack firstly can cause severe damage to the victim's assets and information. Secondly, because the victim also unwittingly sends out copies of the computer virus, it renders the victim liable for the damage resultant there from. The third category simply deals with data alteration and includes incidents relating to unauthorized alteration of vital information like alteration of hospital records, unauthorized changes made to quotations, financial accounts, bank records etc. Although most of these incidents of data alteration involve unauthorized access, there are many instances where persons having authorized access to the data make the unauthorized alteration. In this respect, it is important to analyse the efficacy of the present law in relation to the above-mentioned acts.

## 5.5 Existing legal framework.

Unauthorised access is closely allied to the offence of house breaking and criminal trespass. Housebreaking is provided for in Section 281 of the Penal Code and occurs where one breaks and enters with intent to commit a felony. The elements of the offence are discussed in section 280 of the Penal code and involve "breaking." The element of "breaking" requires the displacement of an obstruction that forms part of the premises. This does not imply that there has to be any physical damage to the obstruction in question. The second element is "entering". Entering takes place if any part of the perpetrator's person or of any instrument, which he or she is using, is inserted into the premises. The entry must be unlawful, which means that the perpetrator is not entitled to enter the premises. The intended offence must not in itself be contained in the breaking and entering. The intent to commit the offence must have been formed when the breaking and entering took place.

The difficulties which one encounters in the application of this offence to the unauthorised accessing of computers relate mainly to the fact that the offence was developed to protect the sanctity of the home against intrusions that involve danger to its inhabitants. The elements of the offence are all developed to function in the physical world. The requirement of the presence of a person in a physical structure excludes the possibility that the offence, in its present form, can be applied to the unauthorised access of a computer.

Even if the gaining of access to a computer can be equated with the element of entering physical premises, there is the other aspect that the access to the computer must be connected to the or be with the intention to commit another offence. This may not always be possible since the majority of the actions, which may follow the accessing of the computer, will not lead to criminal liability.

The second offence is that of criminal trespass which is provided for under Section 286 of the Penal Code. It provides that;

> (1) Any person who —
>
> (a) enters into or upon property in the possession of another with intent to commit an offence or intimidate, insult or annoy any person; or
>
> (b) having lawfully entered into or upon such property, remains there with intent thereby to intimidate, insult or annoy any person or with intent to commit any offence is guilty of the misdemeanour termed criminal trespass and is liable to imprisonment for one year.

The section clearly prescribes two main elements for the offence of trespass: the entering of, or being present on, land or any building or part of a building on the one hand, and the absence of the requisite permission of the lawful occupier, owner or person in charge of the land or building concerned on the other. The element of entering, or being present on, land or any building or part of a building requires the physical presence of a person on fixed property. This excludes the possibility that the offence, in its present form, can be applied to the unauthorised access of a computer. The elements of the offence of trespass do not include the causing of any damage while present on the land or building concerned. This offence can therefore in no way be applied to the alteration of computer data or software applications.

Since trespass is a statutory offence there is no scope for the courts to extend its application to areas that fall outside the ambit of the section. This would clearly be the case if the provisions of the Section 286 of the Penal Code, were to be applied to unauthorised access of a computer. The offence of unauthorised modification can be said to fall under Section 315 of the Penal Code, which provides that any person who wilfully and unlawfully destroys or damages any property is guilty of an offence. The elements of the offence are damage. This is caused where property is destroyed, lost, permanently damaged or damaged to such an extent that it reasonably requires repair or that its use is permanently or temporarily interfered with. The damage must be

the consequence of the actions of the accused. The damaged property must be corporeal. The mere invasion of a person's economic sphere is not sufficient. The element of culpability is satisfied if there is intent to do the relevant act and to cause the resulting damage.

A modification of computer data or software applications causing the alteration or destruction of information stored on a computer would have fallen squarely within the description of malicious injury to property. However it must be borne in mind that the property in question must be corporeal. In effect, the offence cannot be committed under circumstances where damage is caused by means of modification of computer data and software applications. It cannot be expected that the courts can extend the application of the common law offence of malicious injury to property to incorporeal property such as information stored on a computer. For this to happen, court has to extend the concept of "property" in the definition of this offence to include intangibles that have economic value to a person.

Even if such an extension is to take place it will only relate to the intentional damage of information or data stored on a computer. This will leave open the question of whether negligent damage caused by means of the alteration of computer data or software applications should have criminal sanctions. Should any alteration of computer data and software applications, which interferes with the use of a computer or computer network, be regarded as an injury to property? Or will the court require proof that alteration of computer data or software applications necessitated the repair of the affected computer data or software applications or that the use of the affected computer data or software applications has been permanently or temporarily interfered with?

When all these issues are considered in their entirety it becomes clear that the existing legal framework is not appropriate to handle the crimes that are related to the use of computers.

### 5.6 Assessing the options.

The options to be considered for Uganda therefore seem to be a choice between legislative intervention to create certain offences on the one hand, or to leave the matter to the courts to punish such activities by way of extensions to existing common law offences on the other. The extension of the common law offences is unlikely as it is dependant on the level of appreciation of relevant IT issues by the courts. Additionally, there is the capacity of the investigating and prosecuting authorities to prepare a case for prosecution and thereafter be able to convince court to extend the common law offences to a set of circumstances to which it did not apply hitherto. This therefore leaves the option of introducing new offences by way of legislation as preferable.

**Recommendation 19.**

A new Act should be enacted to deal with the new offences of computer misuse that cannot appropriately be dealt with under the Penal Code.

### 5.7 Formulating a legal framework.

Computer crime has an obvious international dimension. It is therefore necessary to ensure that legal protection is harmonised internationally. Over recent years, attempts have been made through international organisations to achieve a harmonised approach to legislating against computer crime and there by prevent the appearance of "computer crime havens".

From 1983 to 1985, an ad hoc committee of the OECD discussed the need for international harmonisation of criminal laws with respect to computer-related economic crime. After further joint work with the Working Party on Information, Computers and Communications Policy (ICCP), a final report was published in 1986.

The Report listed five categories of offences, which it believed would constitute a common approach to computer crime.

The Council of Europe has also considered this field. A select committee of experts, "The European Committee on Crime Problems" was established in December 1985 to consider the legal issues raised by computer crime. The final report was published in September 1989. As part of the Committee's work, it produced guidelines for national legislatures on a 'Minimum List of Offences Necessary for a Uniform Criminal Policy'. These eight offences were seen by all Member States to be the critical areas of computer misuse that required provisions in the criminal law. In addition, the Report put forward an 'optional list' of four offences that failed to achieve a consensus among Members, but were thought to be worthy of consideration. The Report was published with a Council of Ministers Recommendation urging governments to take account of the report when reviewing and initiating legislation in this field.

In view of the above, it is our recommendation that the computer-crime legislation for Uganda ought to conform with the minimum basic standards established by international organisations.

**5.8 Salient offences.**

**(a) Unauthorised access.**

Unauthorised access is the basic 'hacking' or 'cracking' offence. Commission of the offence requires the *actus reus* of causing 'a computer to perform any function'. Some form of interaction with the computer is required, but access does not need to be achieved. This broad formulation means that simply turning on a computer does not constitute the necessary act. The *mens rea* of the offence would comprise of two elements. First, there must be 'intent to secure access to any program or data held in any computer'. Secondly, the person must know at the time he commits the *actus reus* that the access he intends to secure is unauthorised. The intent does not have to be directed at any particular program, data or computer.

**(b) Intent to commit a further offence.**

This offence involves the commission of the offence of unauthorised access together with the intent to commit, or facilitate the commission, of a further offence. The further offence is one for which the sentence is fixed by law, for example, life imprisonment for murder, or where imprisonment may be for a term of five years or more. The access and the further offence do not have to be carried out at the same time. It also does not matter if the further offence was in fact impossible. Different jurisdictions have treated these offences in different ways as exemplified below;

**(i) Australia.**

Australian Crimes Act 1914 (the "Australian Crimes Act") provides for offences relating to computers. Two of the sections contain offences concerning access to computer data. The first of these is unlawful access to data in the Commonwealth. It provides thus:

"A person who with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a commonwealth computer, being data that the person knows or ought reasonably to know relates to: the security, defence or international relations of Australia; the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory; the enforcement of a law of the Commonwealth or of a State or Territory; the protection of public safety; the

personal affairs of any person; trade secrets; records of a financial institution; or commercial information the disclosure of which could cause advantage or disadvantage to any person; is guilty of an offence."

The above provision creates the offence of unauthorised access to computer data that is under government control. The only additional element contained in the section is that a facility operated by the government or a telecommunications service provider is used in order to obtain the unauthorised access. This section, however, does not specify the equipment or the method by means of which the access referred to there is to be obtained.

**(ii) United Kingdom**

In the United Kingdom the Computer Misuse Act 1990 provides for two offences relating to unauthorised access to computers. The first offence is "unauthorised access to computer material":

(1) A person is guilty of an offence if–

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;.

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

This offence is committed when a person causes a computer to perform any function with the intent to secure unauthorised access to a computer program or data held in any computer. The required form of culpability for this offence is intent and the accused ought to have known the intended access is unauthorised. This is seen as a relatively minor offence and carries a penalty of a fine or imprisonment for a maximum of six months.

An important aspect to note about this offence is that the program or data to be accessed need not be located on the computer, which performs the function referred to earlier. The purpose for which access is secured is not qualified. As a consequence the offence can be committed even when the purpose for the access is well meaning. In practice this offence can be committed in a number of ways such as unauthorised use of a person's password, trying to guess a password or installing a program that will obtain a person's password without his or her knowledge. It can even be committed by just switching on a computer, which a person is not authorised to use.

The second offence is "Unauthorised access with the intent to commit a further offence. Section 2 provides thus:

(2) Unauthorised access with intent to commit or facilitate a commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent–

(i) to commit an offence to which this section applies; or

(ii) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

This offence is committed when a person causes a computer to perform any function to secure unauthorised access to a computer with the intent to commit or to facilitate the commission of an offence. The punishment for such an offence is fixed by law or a term of imprisonment for five years can be imposed.

**(iii) Singapore**

In Singapore the Computer Misuse Act (Chapter 50A) ("the Singapore Act") came into being in 1993. This Act corresponds to a large extent with the Computer Misuse Act 1990 of the United Kingdom. The Singapore Act contains an offence of unauthorised access to computer material which , is similar to the offence contained in the Computer Misuse Act 1990:

(c) Unauthorised access to computer material

"Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both."

The Singapore Act also contains an offence of unauthorised access to commit or facilitate a further offence:

> "(1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both."

This offence applies where the further offence, which is intended, involves property, fraud, and dishonesty or can cause bodily harm. Apart from these offences the Singapore Act contains an offence of unauthorised use or interception of a computer service. It provides thus;

(1) Subject to subsection (2), any person who knowingly –

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both."

(d) Comparative analysis

The focus of the Australian Crimes Act is the protection of data stored on computers over which the federal government exercises control. This does not include unauthorised access to the computer equipment itself. It is not advisable for Uganda to follow the Australian law due its inflexibility. On the other hand, the Computer Misuse Act 1990 of United Kingdom creates an offence that is hard to appreciate. The judges and magistrates who have to decide cases relating thereto may easily misconstrue it.

If the underlying danger relating to a particular act is not understood, it may lead to questions such as why it is wrong and how serious is it to be created as an offence. If the scope of an offence is too wide, its application may become unworkable. Additionally, the Act does not contain categories of offences or the distinction of the more serious cases from the less serious ones. Coupled with the complexity of the law, the underlying reasons why computer misuse is criminalized may be obscured.
On the other hand, the Singapore legislation revisits the short falls in the United Kingdom Act and comes with a more concise and adaptive approach that could easily suit the Ugandan situation. It also takes on a new dimension with regard to the punitive measures taking cognisance of the gravity of the offence. It is this

**Recommendation 20.**

Uganda should adapt the Singapore legislation on computer crime as a basis for the proposed legislation as it fits well within the socio- economic circumstances.

**(e) Unauthorised modification**

The other substantive offence under Computer Misuse is that of unauthorised modification of computer material. This offence is principally promoted by the spate of publicity and fear surrounding computer viruses. The concept of damage in the Penal Code is inappropriate to cater for such an offence and as such ' modification of the contents of the computer' cannot be regarded as damage to constitute an offence under the Penal Code, as it does not impair the 'physical condition' of the computer. In the case of the removable data media, such as a computer disk or CD-ROM, deletion of data would only be an offence if the storage medium were in the computer. Once removed, any damage would be subject to the terms of the Penal Code. The offence of unauthorised modification comprises three elements: 'unauthorised modification' of contents, 'requisite intent' and 'requisite knowledge'.

The first element can be further broken down into 'unauthorised' and 'modification'. Whether an act is unauthorised or not is a potentially difficult issue where the person doing the act is the part of the organisation against whom the offence is being committed and has certain 'authorisation' to use the computer system in question. The 'requisite knowledge' element may be defined as knowledge that any modification one intends to cause is unauthorised. It is important at this stage to compare the directions taken by U.K and Singapore in the formulation of the criminalisation of this offence.

**(i) United Kingdom**

The Computer Misuse Act 1990 provides for an offence of unauthorised modification of computer material thus;

(1) A person is guilty of an offence if–

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing–

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised"

The required form of culpability is intent. The intent should be aimed at causing the modification and thereby impair the operation of a computer, prevent access to any program or data or impair the operation of a program or the reliability of data. There are thus two elements to the perpetrator's intent, namely to cause the

any particular computer, any particular data or software application or any particular type of modification. Consequently this formulation can be applied, for example, to a case where a person develops a virus program, which is distributed indiscriminately via e-mail or on the Internet. In a commentary on the Computer Misuse Act 1990 it is pointed out that since intent is expressly required as an element of the offence, it does not cover reckless damage or modification. This contrasts with the corresponding offence of criminal damage of property in English law, which includes reckless acts that cause damage.

Additionally, the description of the offence in Section 3 of the Computer Misuse Act 1990 only refers to "the contents of a computer i.e. data on a computer. This would exclude the modification of data on a removable storage media such as diskettes or CDs. When the data on a storage medium is being accessed by a computer, it can be argued that the data is technically "on that computer" even though it is not stored on the computer. However, once the storage medium is removed from the computer the data it contains can no longer be said to be "the contents of a computer".

**(ii) Singapore.**

The Singapore Act provides for an offence of unauthorised modification of computer material as hereunder:

(a) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

(b) If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

**(f) Comparative analysis.**

The Singapore Act contains a similar provision to the UK Computer Misuse Act 1990, making it clear that the required intent need not be directed at any particular data or computer. However, the Singapore Act does not expressly require intent to be aimed at causing any impairment of a computer or any program or data contained on a computer, nor to be aimed at causing any hindrance of access to any program or data. As far as the state of mind is concerned, Section 5(1) of the Singapore Act only requires that the perpetrator should have the knowledge that his or her actions will cause an unauthorised modification of the contents of a computer. The consequences of the unauthorised modification are irrelevant to this offence.

The standards set in the Singapore Act are very high to suit the Ugandan context. The offence may limit innovation and have a negative impact on electronic transactions in Uganda.

**Recommendation 21.**

The criminalisation of this offence in Uganda should follow the United Kingdom format.

**(g) Child pornography.**

Computer-based pornography is one of the most significant forms of computer crime. The obscenity laws in Uganda on the other hand do not significantly deal with this offence. There is need to protect the exploitation of children sexually and commercially through use of technological advancement.

### 5.8.1 Procedural aspects.

In the majority of cases where offences are committed through the use of computers, there is some evidence of the commission of the offence to be found on a computer. What needs to be considered is whether the procedural laws provide appropriate mechanisms for the detection, investigation and prosecution of such offences? The Criminal Procedure Code and the Magistrates Court Act provide for a general power of the state to search for and seize certain articles. The articles that are liable to be seized can be divided into three categories-

(a) articles which are concerned with the commission of an offence;

(b) articles which may afford evidence of the commission of an offence; and

(c) articles which are intended to be used in the commission of an offence.

No limitation is placed on the nature of the article to be seized, as long as it can be included in one of the above-mentioned categories. The purpose of the power to seize articles is to obtain evidence for the institution of a prosecution and to assist the police in their investigation of a case. As a general rule the search for and seizure of the above-mentioned articles must be authorised under a search warrant. A search warrant authorises a police official to search any person identified in the warrant, or to enter and search any premises identified in the warrant. In certain exceptional cases a search may be undertaken without a search warrant. This is when the person concerned consents to the search for and the seizure of the article in question or where the police official, on reasonable grounds, believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search.

It is clear from the use of words "article" and "premises" that the provisions of the Criminal Procedure Code and the Magistrates Court Act only apply in respect of physical items. This means that the computer itself may be seized under the provisions of the Criminal Procedure Code. It is doubtful that a warrant can be issued for the search and seizure of specific information contained on a computer.

Apart from the application of the Criminal Procedure Code and the Magistrates Court Act, there are other issues in connection with the procedural aspects that require discussion. These issues are unique to the search for and seizure of information stored on computers. Computers are increasingly linked with other computers to form networks. A computer network can span a building, a province, a country and even the globe. The interconnectivity of computers makes it possible to store information on a computer situated in a remote location that need not even be in the same country as the computer used to store the information. This raises issues related to the validity of a search for information stored at a remote location via a network.

Normally a search will be authorised in respect of specific premises where the relevant articles are suspected to be found. In the case of information stored and accessed via a computer network the physical location of the computer containing that information may be difficult to determine. If the computer on which the information is stored is located, it may be in such a location that is not referred to in the search warrant. The question arises, whether that information can legally be searched without obtaining another search warrant? If a new search warrant is required, chances are that the information will have been destroyed or altered or moved to another location by the time the warrant is obtained. Such a requirement places a near-impossible task on investigating authorities to obtain very accurate information of the exact location of the computer on which the relevant information is stored before applying for a search warrant.

The possibility that information may be stored in remote locations also raises issues related to jurisdiction. If the network spans the areas of more than one magisterial district, for instance, it will be very difficult, if not impossible, to decide who has jurisdiction to issue a search warrant in respect of the relevant information. The issue can be further compounded if the information is distributed over a network in such a way that parts of the relevant information are located in one jurisdiction and other parts of it are located in another. If the information

searched for is stored via a global network on a computer located outside Uganda, issues of international cooperation will come into play.

It may be that the country in which the computer containing the relevant information is located relies strongly on the existence of Treaties or Conventions as a basis for providing assistance to foreign investigating authorities. It is also possible that the system for the provision of assistance in the foreign country is based on onerous formalities. The delays and difficulties encountered in the area of mutual legal cooperation may provide an opportunity for the relevant information to be destroyed or altered or moved to another location.

It is also probable that when the information searched for is located, it will be found to be protected by security systems such as passwords and encryption. The question arises whether the authority of the investigating officer to do the search is wide enough to entitle him or her to proceed in attempting to get past any obstacle aimed at preventing access to the relevant information. Apart from this there is the practical question of the methods that may be used to overcome such security measures. One of the main functions of a computer is to store information. This may include information of a private nature or information in respect of which an obligation of confidentiality or secrecy exists. The ability to store information in remote locations compounds this issue as the gaining of access to such a computer may infringe on the privacy of other persons not associated with the offence under investigation. Issues of civil liberties, privacy and confidentiality ought to be considered in respect of the search for and seizure of information stored on a computer. These issues need to be balanced with the need for the effective administration of justice.

Since a computer is capable of storing a vast amount of information, it is likely that the information of interest to the investigation officer co-exists with other information that is of no interest to him or her. The collateral information found on the computer may be necessary for the day-to-day functioning of a business. This problem is further aggravated if the required information is located on a network file server, which is crucial to the functioning of a whole

### 5.9 Admissibility of evidence.

Where an offence is committed by means of a computer or where the computer itself has been the target of illegal activity (such as where unauthorised access has been gained obtained to a computer) the evidence needed to prove the offence will be found on the computer in question unless steps were taken to destroy that evidence. This means that in order to prove the relevant offence, either the computer itself or a printout of the information stored on the computer has to be produced in court. The general rule of admissibility of evidence is that evidence is admissible if it is relevant to a matter before court.

Relevant evidence is evidence tendered to prove or disprove a fact in issue. To this general rule there are a number of exceptions where evidence is inadmissible in spite of its relevance, such as the rule against hearsay evidence. Apart from the general rules as to admissibility of evidence there are a number of rules prescribing how evidence should be tendered. Normally, rule evidence is produced by calling a witness to give a viva voce testimony under oath in an open court. Evidence can also be tendered in the form of real evidence or documentary evidence. Real evidence refers to objects produced for inspection by the court so that the court may draw some conclusion in respect of a fact in issue. The object itself is therefore evidence. Documentary evidence is evidence of a statement in writing, contained in a document that is intended to prove the truth of its contents. The contents of the document are therefore evidence, as opposed to the document itself.

The issues of admissibility of evidence will generally involve a chain of evidence. While this term has no standard legal definition, it is generally accepted as referring to the factual matrix that proves or disproves a particular assertion and the evidence, which supports that factual matrix. The various pieces of evidence, which make up the chain, are literally strung together into a sequence of events or pieces of a puzzle. A weakness in any particular link in the chain will normally mean that the chain will not support the case or defence.

The chain of evidence consists of the interpretive process in which it is necessary to draw proper conclusions from the available evidence as well as the integrity of the physical evidence which includes ensuring that the evidence presented in court is that which was collected from the scene or an accurate representation thereof (i.e. no tampering with or degradation of the evidence). Retaining the chain of evidence helps to rebut the allegations of evidence tampering because a print out can be re-traced to its originating computer file. Therefore, the question that arises, is whether the handling of computer generated evidence should be provided for specifically to avoid breaking the complex chain of evidence in the circumstances?

## 5.10 Analysis of the implications of procedural issues.

In the following example, we present a scenario to illustrate the practical difficulties that may be encountered in investigating a computer related offence. We shall assume that obtaining unauthorised access to a computer constitutes an offence prescribed under the law. It is further assumed that an investigating officer has received information that a certain computer located at a specific address was used to commit this offence. The investigating officer has the authority to search the computer under a search warrant issued for that purpose. As a result of the search the investigating officer locates the computer in question. However, the owner of the computer objects to the searching of the computer's storage disk for information that is not included in the search as it is not an "article" and the computer's storage space cannot be described as premises. The only option open to the investigating officer is to seize the computer itself and to remove it from the premises. The computer equipment, may however belong to a legitimate business and it may contain information that is crucial to the operation of the business and which is totally unrelated to the information which the investigating officer is searching for.

Another problem that may arise in this regard is that the computer on which the relevant information is located may be a file server connected to a huge network which is used for totally lawful purposes, and without which the network cannot function. The computer that is the target of the search may also be shared by a number of users. In such a case the computer will contain collateral information, which is not associated with the search. Additionally, the removal of the computer will deprive the users of their legitimate use of the computer. If the investigating officer has the authority to search the storage area of the computer, for instance with the consent of the owner, he or she may find that the information in question is encrypted.

The owner of the computer can also object to attempts by the investigating officer to de-encrypt the information, as this is not included in the authority to locate that information. Another possibility could be that the information is protected by software that will cause the information to be destroyed if it is not accessed in a specific manner. Again the owner of the computer may object to attempts to circumvent this software, as this is not included in the authority to locate that information.

The owner may also object to such attempts because the investigating officer's actions may alter some information or the functioning of some software on the computer. Further, even if it were to be assumed that the search of a computer's storage area is authorised under a search warrant, and that the investigating officer has located the computer in question, it may transpire that the computer is linked to other computers via a network.

In such a case the perpetrator will have made use of the connectivity of the computer to store the relevant information on another computer at a different location, which is connected to the same network. The investigating officer would then be faced with the problem that the computer, which he or she is authorised to search, does not contain all the relevant information, which is however, on another computer that he or she is not authorised to search. By the time a new search warrant is obtained the perpetrator may have moved the information again or altered or destroyed it. The other possibility may be, that the investigating officer is unable to determine the location of the computer where the perpetrator has stored the relevant information. This means that the investigating officer is not allowed to search for the relevant information in terms of the search warrant which authorises a search of the computer in question, although it is practically possible to

Similarly, the information may be stored via a network on a computer located outside Uganda. The investigating officer would then have to seek for mutual legal cooperation with another country in order to get authority to search for the relevant information. By the time all the formalities associated with mutual legal cooperation are complied with, the perpetrator may have moved the information to another location, or he or she may have altered or destroyed that information.

The computer, which is the target of the search, may also contain privileged information, which does not relate to the search. The owner of the computer can object to the investigating officer obtaining access to such information in the course of his or her search. It is, however, impossible to locate the relevant information on the storage area of the computer and to sift this from the other information on the computer without accessing all the information on the computer.

If the investigating officer succeeds in obtaining the relevant information in the course of an authorised search that information ought to be produced as evidence in court. At this stage the accused may object to the admissibility of the evidence on the basis that the correct procedure for its presentation to the court was not followed or that it constitutes hearsay evidence. If the accused accepts the admissibility of the evidence, he or she may attack the value of the evidence because the information was obtained from the computer in suspicious circumstances.

The above example therefore, shows the complexity of procedural issues that may be encountered in investigating computer related crime. It is recommended that proposed computer misuse legislation should be able to comprehensively cover all the above loopholes and provide a framework that facilitates electronic transactions rather than stifle the technological innovations.

### 5.11 General remarks.

The perception of computer crime in the image of the "hacker" attacking computers of big brother organisations contrasts sharply with reality. The reality of computer crime is in activities that encompass a broad range of perpetrators: the traditional criminal exploiting the power of a new technology, the disgruntled employees utilising their insider knowledge, the curious and thrill-seekers treating the medium as a challenge and those engaged in industrial espionage and information warfare. States have reacted to the phenomena of computer crime by updating their criminal law through the amendment of existing statutes or the adoption of *sui generis* offences.

Policy makers have had to shift their focus from the defining offences to providing for the needs of law enforcement agencies in a networked environment. From a commercial perspective, computer misuse has such a substantial impact that often affects the systems upon which organisations rely on thereby consuming considerable management time and effort and generating adverse publicity. Perpetrators of computer crime usually exploit weaknesses in the systems either being used or attacked. Inadequate security procedures both physical and organisational continue to be a central feature in the vast majority of examples of computer crime. The growth of the Internet, and the timeless connectivity of "always on" computers presents new and enhanced security threats to individuals and society as a whole.

**Recommendation 22.**

The computer misuse legislation should make provision for the new challenges to the law enforcement agencies regarding the investigation and prosecution of computer misuse crime. Such legislation should cover the following areas-

(a) Searches and seizures

(b) Evidence

(c) Jurisdiction

# CHAPTER 6

# ASSESSING THE OPTIONS OF THE FUTURE.

## 6.1 Taxation of electronic products: a challenge to Uganda's tax law.

As e-commerce changes the traditional ways of doing business, new electronic products and delivery systems come into play. Certain products may be delivered electronically rather than in physical form: examples include computer software, music, video clips, photographs and a whole range of written texts or books. As a result, e-commerce gives rise to the characterisation of income under tax laws. Taxation rules distinguish between the sale of goods and the provision of services and the use of intangibles. Where double taxation agreements are followed, the question of how taxing rights are allocated have to be resolved. For example, many double taxation agreements allow the source country to tax royalty payments, payments for the lease of property and, in some cases, payments for certain types of services.

There is a legitimate concern that the development of the Internet may have the effect of shrinking the tax base and hence reducing fiscal revenue. There are concerns on the difficulty in defining jurisdiction in the cyber world coupled with the problem of administration and enforcement. In addressing these problems and in recommending a taxation framework, it is important to ensure that the taxation system is fair, predictable and does not distort the conduct of business. The challenge for Uganda is to develop a taxation policy that is not isolated from its e-commerce partners.

Taxation of electronic transactions raises a number of issues and questions that are both real and imaginary. This Chapter explores, whether there are any problems, and if so, how can they be solved, and whether Uganda has attained the capacity to pursue a solution to these problems. This paper poses issues, which can guide a detailed study of taxation in the electronic environment. The issues in question are hereunder-

(a) Whether the existing tax laws can adequately cater for electronic commerce in Uganda

(b) Whether electronic commerce should be taxed considering the problems involved in the process

### 6.1.1 Tax system in Uganda.

As part of the Economic Recovery Programme, which was launched in 1987, government embarked upon major reforms of the taxation system with the following medium and long-term objectives.

(a) To increase domestic revenue.

(b) To widen the tax base and to gradually lower tax rates in order to enhance equity, improve on taxpayer compliance and minimise tax evasion.

(c) To increase the share of domestic consumption taxes through the introduction of value added tax.

(d) To minimise taxes and tariffs which inhibit export competitiveness and have a direct bearing on production or out put decisions.

(e) To limit the application of excise duty to a few goods such as petroleum, alcohol, beverages and tobacco. The excise duty would not discriminate between imported and locally produced goods.

(f) To simplify the system of tax administration by reducing the number of rate bands while at the same time allowing for flexibility in the implementation of tax policy.

(g) To use import tariff for protective purposes while the sales or consumption tax would be used for revenue generating purposes.

(h) To improve tax administration by offering attractive remuneration to personnel.

(i) To avoid meaningless and uncoordinated adjustments in order to allow for a period of stabilisation

Progress towards achieving these goals can easily be discerned from the various Finance Decrees, Statutes and Acts from 1986 like The Uganda Revenue Statute, The Value Added Tax Statute and the Income Tax Act. A brief review for purposes of emphasis will suffice and is hereunder:

**(i) Value added tax .**

In order to widen the tax base and increase the revenue share of consumption taxes, the government introduced VAT in 1996 replacing sales tax and commercial transactions levy (CTL).

VAT is a consumption tax imposed at each stage of the distribution chain on the value added component of the good or service and is borne by the final consumer. It is normally charged on the manufacturing, importation, wholesale, retail and finally the consumer. It is broad based and capable of raising considerable sums of revenue by comparatively small increases in tax rates and consequently consumer prices. It also rises automatically with inflation and the growth of consumer expenditure. It is neutral and does not depend on a variety of tax rates nor does it discriminate between imports and domestic supplies or different sectors. The major disadvantage of VAT is the cost involved in record keeping, auditing and filing returns that are required on a monthly basis.

**(ii) Income tax.**

The Income Tax Act of 1997 primarily governs this tax. It is basically assessed on business income, employment income and property income. Business income includes gains or losses on disposal of assets, consideration for business restraint, sale of trading stock, gifts received in business connections, interest, rent and any other income. On the other hand, employment income deals with compensation, insurance premium, consideration for variation of employment terms and shares. Property income includes any dividends, interest, annuity, natural resource payments, rents, royalties and any other payment derived by a person from the provision, use or exploitation of property. It also includes the value of any gifts derived by any person in connection with the provision, use or exploitation of property. Property income is also the total amount of any contributions made to a retirement fund during a year of income by a tax exempt employer and any other income derived by a person.

**iii) Other indirect taxes.**

These are the most likely to be affected by electronic commerce. These include; customs duties and excise duty. It should be noted that the tariff regime of Uganda has passed through a reform process aimed at simplifying it. These reforms have has also been in line with the COMESA initiatives and the obligations under EAC Treaty especially relating to the formation of a customs union. Under the COMESA Agreement, Uganda has obligations under Articles 63, 64 and 69 to intensify cooperation in customs management including the simplification and harmonisation of customs formalities and trade documents, the adoption of uniform tariff classification and establishment of a standard system of customs valuation.

Uganda has attempted to fulfil these obligations through replacing the national customs tariff system based on the Customs Cooperation Council Nomenclature (CCCN) with the harmonised commodity description coding system (HS) with 53000 tariff lines at the six digital level with all the tariffs based on the *ad valorem* basis. In 1997 all excise surcharges were harmonised at 19%. On the international plane, the government introduced the GATT valuation system, which is based on the transactions value paid by an importer for imported goods.

Uganda has thus, in the area of trade policy instruments continued to adjust trade taxes. It has minimised tax bands for administrative convenience and replaced quantitative restrictions. In this respect therefore, any legal regime that will attempt to regulate the taxation of electronic commerce will have to seriously put into consideration all these factors and policies.

### 6.1.2 International perspective on taxation.

International organisations and governments have highlighted principles that should guide the work of governments in the field of taxation of electronic commodities. These include the Organisation for Economic Cooperation and Development (OECD), the U.S. government and the World Trade Organisation (WTO).

### 6.1.3 OECD perspective.

The principles-based approach adopted by the OECD culminated in an agreement that the following widely accepted general tax principles should apply to the taxation of e-commerce:

(a) Neutrality. Taxation should seek to be neutral and equitable between forms of e-commerce and between conventional and electronic forms of commerce. Business decisions should be motivated by economic rather than tax considerations. Taxpayers in similar situations carrying out similar transactions should be subject to similar levels of taxation. In other words there is no need for a special new tax such as a "flat rate" or a "bit" tax.

(b) Efficiency. Compliance costs for taxpayers and administrative costs for the tax authorities should be minimized as far as possible.

(c) Certainty and Simplicity: The tax rules should be clear and simple to understand so that taxpayers can anticipate the tax consequences in advance of a transaction, including knowing when, where and how the tax is to be accounted.

(d) Effectiveness and Fairness: Taxation should produce the right amount of tax at the right time. The potential for evasion and avoidance should be minimized and counter-acting measures should be proportionate to the risks involved; and

(e) Flexibility: The systems for taxation should be flexible and dynamic to ensure that they keep pace with the technological and commercial developments.

The above principles are in line with Uganda's general taxation principles. Nevertheless, care should be taken to ensure that the existing Ugandan tax-base is not eroded by international decisions favouring nations with sophisticated and developed economies.

### 6.1.4 The US treasury perspective.

It identifies the following points-

(a) New technologies, such as the Internet, have effectively eliminated national borders on the information highway. As a result, cross-border transactions may run the risk that countries will claim inconsistent taxing jurisdictions, and that taxpayers will be subject to quixotic taxation.

(b) In order to ensure that these new technologies are not impeded, the development of substantive tax policy and administration in this area should be guided by the principle of neutrality.

(c) Transactions in cyberspace will likely accelerate the current trend to de-emphasize traditional concepts of source-based taxation, increasing the importance of residence-based taxation.

In October 1998, the Internet Tax Freedom Act was signed in the USA. This Act places a moratorium on any new taxes on Internet access and created a commission to study and make recommendations about domestic and foreign policies toward the taxation of e-commerce. This commission completed its work with a number of proposals, including an extension of the moratorium on new taxes on Internet access and support for the extension of the WTO moratorium on tariffs and duties on electronic transmissions.

### 6.1.5 E-commerce and taxation challenges.

**(a) Characterization of income.**

**(i) Residence versus source.**

Uganda uses the residence based taxation system. Residence or non-residence for that matter is used to determine whether a taxpayer is to be taxed on his or her worldwide income or on income from Uganda. The tension between residence-based and source-based taxation lies at the heart of the e-commerce taxation debate. Most first-world countries follow the principle of taxing worldwide income of residents of the country and income sourced in that country belonging to non-residents. Where a double tax agreement (DTA) exists, income sourced in that country is only taxed in the case of non-residents where certain types of income are involved or a permanent establishment as defined by the DTA is present. Double taxation is avoided through DTAs, which make the residence country responsible for giving credit relief or exemption for foreign income taxed at source. The applicability of these issues would require a more detailed study.

**(ii) Residence of companies.**

In the world of e-commerce, a company may for all practical purposes only exist in cyberspace. Business can be conducted electronically with directors meeting by way of video-conferencing. In this kind of setting, determining whether an e-company is effectively managed in a particular country could prove problematic.

**(iii) Residence of a trust .**

Ordinarily, if the executors, administrators or trustees are resident in Uganda and if the estate or trust fund is administered from Uganda, the estate or trust is resident in Uganda. However, electronic commerce may change all this. Therefore, each instance ought to be decided on its own merits, but the place where the assets of the estate or trust are managed or controlled may well be crucial. The residence of a trust, being a person other than a natural person, is the same as that of a company.

**(iv) Residence of a Partnership.**

A partnership in Uganda is not a separate legal person distinct from the persons who constitute the partnership, and under the Income Tax Act it is a mere pass through entity. However, a partnership operating electronically may obscure all these time-honoured ideals.

**(b) Place of consumption.**

It is thought that one way of managing electronic taxation is by making sure that Indirect taxes apply where consumption takes place. However, there is need to seek for an international consensus on the identification of the place of consumption. Consensus is essential to avoid double taxation or unintentional non-taxation, particularly as double taxation treaties do not apply to indirect taxes. The main difficulties that arise here are, that the supplier may not be able to determine the location of the customer and may also be outside the fiscal jurisdiction of the authorities in the country where the consumption takes place.

**(c) Electronic products.**

The supply of electronic products should not be treated as a supply of goods. Many Revenue Authorities have already reached this conclusion, which means that under most VAT systems; the supply of electronic products would be treated as a supply of services. This treatment would prevent the problems that could otherwise arise in relation to taxes on importation and the application of place-of-supply rules.

**(d) "Reverse charge" mechanism.**

The use of the "reverse charge" mechanism or similar mechanisms should be considered for the taxation of businesses that acquire services and intangible property from suppliers outside the country. In relation to VAT systems, the "reverse charge" mechanism requires the customer to account for output VAT on imported services, but it also gives a right to an input tax deduction.

**(e) Private consumers.**

The collection of indirect taxes from private consumers represents the major area of concern in relation to the application of indirect taxes to e-commerce. Three main options should be considered:

(a) Requiring the supplier to account for taxation in the country of consumption.

(b) Requiring the customer to account for the tax. This is the position in Uganda where goods are not required to be entered through customs and excise or where a service is rendered.

(c) Requiring the payment intermediary (such as the bank or credit card company dealing with the payment) to account for the tax.

Each of these three alternatives is potentially unsatisfactory and it has been suggested that the best approach may be to require the supplier to account for the tax but to simplify greatly the existing registration procedures.

**(f) Telecommunication issues.**

It is very apparent that electronic commerce thrives on an efficient and vibrant telecommunications sector. Therefore, the mode of taxing the telecommunications sector must equally be addressed.

**6.1.6 Tax administration and compliance issues.**

**(a) Identification.**

The accurate identification of the party responsible for paying a particular tax is a fundamental requirement of any taxation system. Tracing the physical owner of a website, can be a time-consuming process often with reliance being placed upon a third party. Conventional businesses are easier to keep track of as they operate from a physical and geographical location that can be visited. In addition, all conventional correspondence of Companies, Corporations and Trusts in Uganda require the relevant registration certificates to be displayed. As there is a blurring between advertising and the actual trading capabilities of an enterprise through a website, there is need to establish a minimum standard in respect of identification requirements.

**(b) Information.**

The ability to access reliable and verifiable taxpayer information is essential for any tax administration to be able to do its job effectively and efficiently.

**(c) Evidence.**

The tax laws described above provide a framework for the collection and retention of commercial documents by taxpayers. Currently, the law is based on physical businesses conducting business using traditional methods to record their transactions. This legal framework is also dependent on established rules of evidence that are applied in court to test the probity of facts and documents. A foundation ought to be laid to ensure the admissibility and probative value of computer evidence in litigation.

**(d) Collection.**

Some of the most efficient collection mechanisms are those, which make use of a leverage point. A common example is PAYE where a limited number of employers collect the taxes on behalf of the Uganda Revenue Authority from a significant number of taxpayers. Collection activities are concentrated, in other words, as e-commerce tends to eliminate the "middleman", so too could tax collection efficiency be reduced. All collection proposals, in essence, require a greater degree of international cooperation in revenue collection than currently exists.

### 6.1.7 Conclusion.

Uganda needs a comprehensive review of all the taxation issues that arise from electronic commerce. Such a study is beyond the scope of the Consultant's TOR.

**Recommendation 23.**

The issue of electronic taxation is a policy issue. However, there are few areas in Uganda, which need urgent review especially the residence basis of taxation, electronic money and identification of website owners.

## 6.2 Intellectual property issues.

Intellectual property rights are legal means to protect and balance the interests of an individual against those of the public. This is done in terms of disclosure, dissemination, alteration, use and abuse of ideas, with an exclusive right to control and profit from invention and/or authorship of such intangible goods, services and ideas. The World Intellectual Property Organisation (WIPO) classifies intellectual property into two categories, namely, industrial property, such as inventions, trademarks, industrial designs and appellations of origin and copyright literature that refers to items such as musical, artistic, photographic and audio-visual works.

It has become relatively easier to infringe intellectual property through the use of electronic technologies. Therefore there is an urgent need to formulate a system of laws that define and protect intellectual property as a response to technological changes, particularly the emerging circumvention technologies that are constantly defying copyrights on electronic systems. In this context, it becomes increasingly difficult to ensure that intellectual property rights and related neighbouring rights are applied to the electronic environment in a manner that is promoting e-commerce.

### 6.2.1 Challenges around the protection of intellectual property rights

Some of the problems around the adaptation, protection and enforcement of intellectual property rights in an electronic environment are-

(a) Existence of excessive regulations limiting or discouraging the generation, use and sharing of ideas.

(b) Difficulty in distinguishing between the original owner of intellectual property and the host or custodian of such property in an electronic environment.

(c) The availability of free, unsolicited, and cheap electronic goods and services online.

(d) Availability of inexpensive (sometimes free) sophisticated and innovative methods for reproduction and distribution often referred to as circumventing technologies including duplicating devices of intellectual property.

(e) Absence of adequate legislation relating to the protection of indigenous intellectual property.

(f) Limited presence of adequate capacity, instruments and mechanisms to monitor and protect intellectual property rights.

(g) The ever-changing technological innovations relating to the use of Internet for commercial transactions.

(h) The dominance of developed countries in the creation of Intellectual Property

(i) The global nature of e-commerce, the Internet transcending borders, juxtaposed to traditionally local or territorial nature of intellectual property laws.

(j) Inadequate legal framework to regulate rights and responsibilities for and on behalf of Internet Service Providers in terms of liability

### 6.2.2 Local context.

The Ugandan intellectual property law is not fully equipped to deal with the implications of the Internet, convergence, multimedia, digital technology or generally electronic transactions. The advent of the Internet has changed the underlying assumptions of the original copyright laws under the Copyright Act. The Trade Marks Act provides for instances under which trademarks cannot be infringed, yet domain naming has created a loop-hole in the Act, i.e. Trademarks Vs domain names.

The application of traditional copyright law to open, public and global networks such as the Internet is hindered by the fact that traditional protection of intellectual property rights has always specifically referred to the protection of information contained in tangible media such as books. Therefore convergence of traditional forms of communication into a single electronic environment presents challenges in the attempt to amend the Act and accommodate this new environment. It is however, crucial to keep the intellectual property law in Uganda abreast of the technological developments with a legislation that conforms to innovation.

### 6.2.3 International context.

Debates relating to intellectual property rights are ongoing in the international fora such as the World Intellectual Property Organisation, the World Trade Organisation and the European Union. There are currently no international agreements that sufficiently address the various issues fundamental to the protection of intellectual property rights in the electronic environment. In effect, multilateral and bilateral treaties may prove to be the most feasible way to deal with trans-border intellectual property related issues.
Traditionally, intellectual property rights are limited by territorial boundaries. The scope of the rights established in each country is determined by that country and the effect of those rights, as well as their protection, are, in principle, confined to the territory of the country. However, the transnational nature of e-commerce suggests that several national laws could apply to a single act of transgression. This can create legal uncertainty that may unduly hamper the progress and the growth of e-commerce and the general flow of information.

The TRIPS Agreement (The Agreement on Trade-Related Aspects of Intellectual Property) was adopted in 1994 to provide rules concerning trade-related intellectual property rights, basic principles of previous intellectual property conventions, standards regarding availability, scope, and use of intellectual property rights. Appropriate enforcement, multilateral dispute settlement procedures and transitional arrangements for countries are also included in the agreement. Administered by the WTO, the TRIPS Agreement is enforced through WTO consultative panels and dispute resolution mechanisms. TRIPS basically covers copyrights and related rights such as the rights of broadcasters, performers, producers of sound recording and broadcasting organisations; industrial designs and patents including the protection of layout and design of integrated designs; undisclosed information including trade secrets and test data; trademarks and service marks.

It also outlines the main elements and standards of protection to be provided by each member, the nature of the subject matter to be protected, and the rights to be conferred and permissible exceptions to those rights, as well as the duration of protection. It further outlines enforcement mechanisms on behalf of the standards and their protection. These include provision of civil and administrative procedures, criminal procedures, , remedies for such an environment and other dispute resolution mechanisms. TRIPS further allows developing member countries with a grace period and autonomy to implement compliant and necessary changes as recommended in the agreement.

The contribution of the Internet in the creation, production, and use of literary and artistic works, performances and phonograms, including its potential to undermine the basic tenets of copyright and related rights, compelled the WIPO to lead the adoption of two treaties in December 1996, namely, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). These treaties are commonly referred

to as the "Internet treaties". These treaties address issues of the definition and scope of rights in the electronic environment, and some of the challenges of online enforcement and licensing.

To give impetus to the efforts to reach a global consensus on the protection of intellectual property, WIPO developed a "digital agenda" that included the following-

(a) Broadening the participation of developing countries through the use of WIPONET and other means for access to intellectual property information, participation in global policy formulation and opportunities to use their intellectual property assets in e-commerce.

(b) Promoting the adjustment of the international legislative framework to facilitate e-commerce through the extension of the principles of the WPPT to audiovisual performances, the adaptation of broadcasters' rights to the digital era and progress toward a possible international instrument on the protection of databases.

(c) Implementing the recommendations of the Report of the WIPO Domain Name Process and pursue the achievement of compatibility between identifiers in the real and virtual worlds through the establishment of rules for mutual respect and the elimination of contradictions between the domain name system and intellectual property rights.

(d) Developing appropriate principles with the aim of establishing, at the appropriate time at the international level, rules for determining the circumstances of intellectual property liability of Online Service Providers (OSPs), which are compatible and workable within a framework of general liability rules for OSPs.

(e) Promoting adjustment of the institutional framework for facilitating the exploitation of intellectual property in the public interest in a global economy.

(f) Introducing and developing online procedures for the filing and administration of international applications for the PCT, the Madrid System and the Hague Agreement at the earliest possible date.

(g) Studying and, where appropriate, responding in a timely and effective manner to the need for practical measures designed to improve the management of cultural and other digital assets at international level.

(h) Studying any other emerging intellectual property issues related to electronic commerce and, where appropriate, develop norms in relation to such issues.

(i) Co-ordinating with other international organisations in the formulation of appropriate international positions on horizontal issues affecting Intellectual Protection, in particular the validity of electronic contracts and jurisdiction.

(j) Copyright

(k) Copyrights are referred to as the rights to ensure protection of information from duplication and distribution. Computers are changing the way copyrighted goods can be illegally copied and distributed. Violation of copyrights is difficult to monitor in the electronic environment, since content exists not physically but in electronic form and can be instantaneously distributed without even being copied. All of this occurs cheaply and easily. This creates new challenges for copyright owners and law enforcement agencies in that the distinction originally drawn between copying and distribution is blurred. In this regard, a number of issues need to be addressed: -

(l) The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted there under, fully apply in the digital environment, in particular to the use of works

in digital form. The issues include whether electronic reproduction is "reproduction" in terms of the Ugandan copyright law, whether temporary storage is "reproduction", whether the copyrights owner can and should prohibit/authorise the digitisation of his/her copyright work and whether technology devices/measures to reproduce and or prevent unauthorised reproduction should be protected.

Therefore, a more detailed study would be required to establish the following-

(a) Determining liability in copyright infringements given the intangibility of information in transit

(b) Potential liability of end-users "reproducing" infringing copies (transient copies) of copyrighted works by the mere act of viewing them on their computers

(c) Balancing the enforcement and monitoring of intellectual property rights with the need to promote the use of e-commerce and cyberspace publishing.

(d) Implementing the expenses, efforts, duration and technical evidence demands for enforcing copyright protection in court.

### 6.2.4 Patents.

The process of patenting entails the registration and protection by law of new and innovative ideas that have industrial or commercial value. An invention can be defined to be a novel idea, which permits in practice the solution of a specific problem in the field of technology. More formally WIPO defines a patent to be a document, issued by a government office, which describes the invention and creates a legal situation in which the patented invention can only be exploited (altered, used or sold) by, or with the authorisation of the patentee.

Lack of material objects is not the only problem for intellectual property rights owners, posed by the digitalisation of information. Information in digital form is much more easily manipulated and adapted than traditional forms of information and the changes are much harder to detect. Again historically patents are technical and territorial in nature. There is an increasing need to protect software, business practices, formulae, recipes etc. The scope of the definition and the criterion in rendering a patent need to be widened with emphasis on protection, monitoring and enforcement measures. This should apply on a local and a legally compatible and interoperable global basis. There is a need to implement a global integrated mechanism for the administration and issuing of patents to synchronise the global growth of the knowledge based society.

### 6.2.5 Trademarks.

A trademark is a sign, or a combination of signs, capable of distinguishing goods and services of one undertaking to those of other undertakings. The sign may consist of one or more distinctive words, letters, numbers, drawings, pictures, emblems, colours or combination of colours. The emergence of a truly global electronic market place has created an increase in demand for brand-named consumer goods and, unfortunately a concomitant rise in illegal copying and reproduction of these goods.

Trademarks laws, the world over are important tools of protecting the public from fraud and brand confusion, promoting the goodwill of business and facilitating product distinction and integrity in society. The Trademarks Act presently provides for instances where trademark rights are infringed, which generally revolves around the prevention of registration of already registered trademarks. The framework regarding the unauthorised use of trademarks in relation to goods and services in the traditional environment should hold for the virtual environment as well.

Trademarks are territorial in nature i.e. their registration applies to a particular country or jurisdiction. There is a general discrepancy between the national scope of trademark laws and the international nature of electronic commerce, particularly since e-commerce is borderless and instantaneous in nature. For example, different parties can register a trademark in different jurisdictions at almost the same time.

The fundamental issue arising from trademarks or "well-known marks" relates to domain names. Domain names are essentially addresses allocated to websites through which traders, vendors and virtual locations can be identified and located on the Internet. Currently there are no definite linkages between trademarks and domain names. This means that one can register a trademark as a domain name irrespective of whether the trademark belongs to one or not. Naturally this does not appeal to the original owner of the trademark, and unfortunately the Act does not provide any guidelines. However this still constitutes an infringement in that the uniqueness of the mark will no longer hold.

It is very difficult to resolve these issues and as such the WIPO Dispute Resolution rules were adopted by ICANN. Further, Uganda may encourage the litigants jointly or unilaterally, to submit a dispute to WIPO Dispute Resolution Panel. It is uncertain to what extent the Trademarks Act would or should apply to domain names. The Act protects the proprietor of a registered trade mark from the unauthorised use, in the course of trade, in relation to goods or services for which the mark is registered, of an identical mark or a mark so nearly resembling it as to be likely to deceive or cause confusion. It also deals with "dilution" of a trade mark, that unauthorised use of a registered mark which is identical or similar to a mark which is also well-known in Uganda would amount to infringement, if such use is likely to take unfair advantage of, or be unfairly prejudicial to its distinctive character or repute (it is not necessary to prove deception or confusion). The same principle applies to the dilution of well-known "foreign marks", even if the foreign mark is not registered in Uganda. Under the Business Names Registration Act, the Registrar of Companies has the power to prohibit the use of certain forms of business names to the extent that A Person shall not carry on any business under any name, title or description which includes the words "government" or any other words, or any abbreviation. The electronic advancements in effect, require a more in depth analysis of the following issues-

(a) Determining the rights of a trademark registered in different jurisdictions by different parties almost at the same time.

(b) Determining whether there should be a linkage of administration between the trademark registry and the domain name registry to prevent cyber squatting.

(c) Appraising the implications of the international treaties for Uganda in terms of its capacity for monitoring and enforcing violations of the intellectual property rights protected by these treaties.

### 6.3 Privacy.

The critical benchmark to Uganda's success in facilitating e-commerce is to ensure that the enabling environment is conducive to investment. A UNDP study (supra) conducted for Uganda emphasized that among the most significant barriers to e-business development in Uganda is the lack of a sufficient legal framework that values and protects property. That study noted that because e-commerce involves a global market and relies on the movement of data across international boundaries, there is an unprecedented need for laws that meet international standards and requirements. In addition, like other jurisdictions seeking to maximize the benefits of ICTs, significant gaps in law related to electronic communication and transactions must be filled. Essentially, these include laws governing electronic communications and privacy or 'data protection.'

To realise some of the benefits from e-commerce in Uganda, there is a need to develop tailor made legislation for Uganda that is harmonized with international trade obligations or standards of legal protection already in place in Europe and North America. For example, the EU, Canada and the United States are major potential

markets for Uganda's e-services like data processing and call centres. Each jurisdiction has established laws based on the OECD Guidelines on the Protection of Privacy and Trans-border Flow of Personal Data.

The importance of legislative harmonization in this area for Uganda cannot be overstated. For example, the EU Directive on Data Protection requires good data management practices on the part of entities that process personal data through a series of legal obligations. These obligations include the requirement that the use of personal data be only for specified reasons, involving explicit and legitimate purposes, along with obligations to guarantee security of data against unauthorized or accidental access, as well as the subject's consent for collection and use.

The EU Directive sets rules requiring among other things that data can only be transferred to countries outside the EU when its protection is guaranteed. The movement of data for processing in Uganda from a call centre or other form of data entry may only occur if Uganda has high standards of protection recognized by the EU. Limited transfers of data may be permissible under explicit contractual mechanisms set out by the EU, but contractual mechanisms are not optimal as the EU has the power to block all data flows to a country if it perceives it as a risk.

The most desirable path for Uganda would be to have a data protection law providing equivalent protection. To date only a few countries such as Canada, the US, Hungary and Switzerland have had their laws recognized. The first African jurisdiction to gain such recognition would have substantial advantages in global e-commerce. In designing this law there are other guidelines that ought to be followed and these include:

(a) The United Nations Economic and Social Council guidelines concerning computerised personal data files of 20th February 1990.

(b) OECD Declaration on Trans-border Data Flows adopted in April 1985.

(c) 1981 Convention for the Protection of individuals with Regard to the Automatic processing of Personal Data of the Council of Europe.

(d) The EU Data Protection Directive of 24th October 1998.

(e) The EU Telecom Directive adopted in December 1997.

The list is by no means exhaustive. It would also be important to consider national legislation like The UK Data Protection Act of 1998 and The South African Electronic Communications and Transactions Act of 2002. In considering protection of the right to privacy, the regime governing the whole environment of protection will have to be evaluated. The institution that will control the use of and processing of data will be paramount. This may be the Data Protection Registrar/Commissioner that can be a department in the office of the Registrar General in Uganda. On the other hand, it may be worthwhile to consider a Data Protection Authority that would result in the establishment of a new infrastructure for data protection.

In considering the above factors, the main areas for scrutiny should be the modes of obtaining data, storage, processing, use of data and data security. Consequently, any legislation on privacy will have to be harmonized with the above, in order for Ugandan businesses including government enterprises to be able receive or process data provided by businesses or individuals located in the EU, Canada or the United States.

**Recommandation 24.**

There is need to urgently put in place a legal framework for privacy and data protection. With such legislation in place, and in harmony with the international standards or benchmarks for privacy and data protection, Uganda is strategically positioned to fully exploit the benefits of electronic transactions.

## GLOSSARY OF TERMS.

(a) Armored virus-An armored virus is one that uses special tricks to make the tracing, disassembling and understanding of its code more difficult.

(b) Chain of evidence- The factual matrix that proves or disproves a particular assertion and the evidence, which supports that factual matrix. The various pieces of evidence, which make up the chain, are literally strung together into a sequence of events or pieces of a puzzle. A weakness in any particular link in the chain will normally mean that the chain will not support the case or defence being pleaded. The chain of evidence consists of the interpretive process in which it is necessary to draw proper conclusions from the available evidence as well as the integrity of the physical evidence which includes ensuring that the evidence presented in court is that which was collected from the scene or an accurate representation thereof (i.e. no tampering with or degradation of the evidence).

(c) Companion virus- A companion virus is one that, instead of modifying an existing file, creates a new program, which (unknown to the user) gets executed by the command-line interpreter instead of the intended program. (On exit, the new program executes the original program so things will appear normal.) Creating an infected .COM file with the same name as an existing .EXE file does this. Note that this type of malicious code is not always considered to be a virus, since it does not modify existing files.

(d) Computer contaminant -Computer contaminant means any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, or by any means to usurp the normal operation of the computer, computer system, or computer network.

(e) Computer source code- A computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

(f) Computer virus - Computer virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource

(g) Cookie Poisoning- Cookie poisoning is a technique mainly used for achieving impersonation and breach of privacy through manipulation of session cookies, which are primarily used to maintain the identity of the user.

(h) Copy- In relation to the term document, this means anything onto which information recorded in the document has been copied by whatever means whether directly or indirectly.

(i) Denial of service attack- This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.

(j) Direct evidence- Evidence given by the witness of a fact, which he actually perceived with his own senses.

(k) Discovery- A process in which each party to an action is required to disclose to the other party all documents in its possession, custody or power which relate to the matters which will come before the court

(l) Email spoofing- A spoofed email is one that appears to originate from one source but actually has been sent from another source.

(m) Extrinsic evidence-This is evidence, which is usually given in connection with the document. Normally, this applies to evidence given in court by the maker of a written witness statement who is called to give oral evidence to substantiate what he has said in documentary form.

(n) Hearsay evidence- This is evidence which is not direct evidence and which is not presented by the maker of the statement in question but by another person or a document.

(o) Macro virus- Many applications allow you to create macros. A macro is a series of commands to perform an application-specific task. Those commands can be stored as a series of keystrokes, or in a special macro language. A macro virus is a virus that propagates through only one type of program, usually either Microsoft Word or Microsoft Excel. It can do this because these types of programs contain auto open macros, which automatically run when you open a document or a spreadsheet. Along with infecting auto open macros, the macro virus infects the global macro template, which is executed anytime you run the program. Thus, once your global macro template is infected, any file you open after that becomes infected and the virus spreads.

(p) Oral evidence -Evidence, which is given by a witness making statement in court.

(q) Polymorphic virus - A polymorphic virus is one that produces varied (yet fully operational) copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus.

(r) Primary evidence -The original evidence or a duplicate copy

(s) Real evidence- Evidence, which is taken from, or consists of, material objects or the result of automatic or natural processes

(t) Secondary evidence - Evidence, which is neither original nor the best evidence available.

(u) Social engineering- This refers to exploitation of personal relations with a person to obtain confidential information under his / her control.

(v) SQL Injection - Refers to attacks on websites which allow users to input data. A user can exploit weak coding on the website to input malicious code, which then runs on the server or on the computers of other users. An effective counter-measure is script validation wherein all data input by the user is sanitized. This ensures that the user can only send expected values, and not malicious script.

(w) Stealth virus-This is one that hides the modifications it has made in the file or boot record, usually by monitoring the system functions used by programs to read files or physical blocks from storage media, and forging the results of such system functions so that programs which try to read these areas see the original uninfected form of the file instead of the actual infected form. Thus the viral modifications go undetected by anti-viral programs. However, in order to do this, the virus must be resident in memory when the anti-viral program is executed.

(x) Web-defacement - Web Defacement occurs when the attacker spoils the appearance of the website of the victim organization. In most cases the perpetrator leaves obscene messages on the website

(y) XSS attack -An XSS attack (sometimes called cross scripting) occurs when an attacker uses a Web application to send malicious code, usually JavaScript, to a different end user.

## REFERENCES

Arkiran (1999), Quality Customer Service Demands human Contact. The International Journal of Bank Marketing Volume 17, issue NO.2.
Bank Uganda (2000), A Revolution in Delivery of financial services

Bridging the Gender Digital Divide through Strategic Partnerships- Africa Launch of the Digital Diaspora Initiative and Global Advisory Committee meeting Kampala, Uganda (May 5-6, 2003)

Christine Sgaulatta Chong and David S. Byer, 'The Electronic Paper Trail. Evidentiary Obstacles to Discover and Admission of Electronic Evidence.' Boston University Journal of Science and Technology, spring 1993.
Contract Amendment, Final Report April 2002

El-Nawawy, Mohammed and Magdamismail: Overcoming Deterrents and Impediments to Electronic Commerce in Light of Globalisation; The Case of Egypt,

Experiences from the use of a CD-ROM, by rural women in Uganda, 31/October/2002

Gates, Arland: Canada Law on Jurisdiction in Cyberspace,

Geoffrey Bakunda (2001), An introduction to business strategy.

Gillian Marcelle: From Conceptual Ambiguity to Transformation

Global Conference on the Development Agenda for Small States

Harris, G. Jeanne: Managing the Digital Economy, Do You Have What it Takes?
Hartmany, Amir: Not Ready: Strategies for Success in the E-Economy (can be accessed on www.amazon.com under books e-commerce)
http://www.bakerinfo.com/toronto. (15-03-2002)
http://www.comesaec.org (16-03-2002)
http://www.comesaec.org (16-03-2002)
http://www.comesaec.org (16-03-2002)
http://www.comsaec.org (15-03-2002)
Ian Lloyd- Information technology law 2nd edition-Butterworths publications. U.K, 2001- http://www.butterworths.co.uk/ac.

Ignatius Kakembo-Ntambi, Vincent K. Musubire: E-READINESS & E-NEEDS ASSESSMENT STUDY July 2002

Imparato, Nicolas: Public Policy and the Internet; Privacy, taxes and contract, Hoover Institution Press Publications, U.K, 1998

Incorporating Gender Equality and Women's Empowerment in the ICT arena, 02/December/2002

Justin Semuyaba, Legal frame work for E-Commerce in Uganda.

Kaijage Johnson (2002), The Legal Perspectives of Internet Based Contracts, Makerere University
Lewis Barbara (2000), Service failure and Recovery in Retail Banking.

Livermore J. Etal, Electronic Bill of Lading and Functional Equivalence, 1998 the journal of Information Law and Technology

London, February 17-18,2000.

Miller Esselaar and Associates: A Country ICT Survey for Tanzania, Final Report, November 2001.

Miltonlouw, Josemurta and Dobekpater: The Policy Contexts Surrounding Electronic Commerce in a Region Report on Southern Africa

Munene (2000), Coping with technological changes in the 21st Century publication of Minutes from that Seminar.

Musubire, Vincent: Status of Internet Commerce in Uganda,.

PERWIT INTERNATIONAL:Strategic Partnership for E-Business in Uganda:

Peter F. Drucker: Managing in the Next Society

Phillip Kottler (1988), Service Marketing.

Reynolds, Janice and Mofazali: The Complete E-Commerce Book, Design, Build and Maintain a successful Web Based Business, Oxford Publishers, UK, 1997

Rita Mijumbi: ICTs as a tool of economic empowerment of women.

Robert Schware and Paul Kimberley: Exploiting Information Technologies for Electronic Commerce and Better Public Sector Management.

Semuyaba, Justin: The Legal Aspects of International Electronic Commerce.

Shaun Lake: E-Commerce in Least Developed Countries.

Stephen Musubire (2002) A Ugandan Perspective of the Legal Challenges of Internet based sale of Goods.

Submission on the Business Sector June 2000.

Vincent K. Musubire : Information Infrastructure Agenda for Uganda.

Zethaml et al (1985), Serqual is an internationally acclaimed method of assessing the quality of a service.

## ANNEX 1

# THE COMPUTER MISUSE BILL, 2004
## Arrangement of Clauses

PART 1 - PRELIMINARY

**Clause**



PART II – GENERAL PROVISIONS



PART III – COMPUTER MISUSE OFFENCES



PART IV - MISCELLANEOUS.

# THE COMPUTER MISUSE BILL, 2004

## A BILL for an Act

## ENTITLED

## THE COMPUTER MISUSE ACT, 2004

**An Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transaction in a trustworthy electronic environment and to provide for other related matters**.

### PART I – PRELIMINARY

1. **Interpretation.**

In this Act, unless the context otherwise requires-

"access" in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not;

"application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function, and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;

"child" means a person under the age of eighteen years;

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, other than-

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may by notification in the Gazette, prescribe;

"computer output" or "output" means a statement or representation, whether in written, printed, pictorial, graphical or other form, purporting to be a statement or representation of fact-

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"currency point" means the value of one currency point specified in the Schedule;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that-

(a) causes loss aggregating at least one million shillings in value, or such other amount as the Minister may, by notification in the Gazette prescribe, except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;
(c) causes or threatens physical injury or death to any person; or
(d) threatens public health or public safety;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"data message" for purposes of this Act, means data generated, sent, received or stored by electronic means and includes-

(a) Voice, where the voice is used in an automated transaction; and
(b) a stored record;

"electronic", "acoustic", "mechanical" or other "device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;
"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;
"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;
"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;
"information system services" includes a provision of connections, operation facilities, for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;
"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport of such function;
"program or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

## PART II – GENERAL PROVISIONS

**2. Securing access.**

A person secures access to any program or data held in a computer if by causing a computer to perform any function, such person-

(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

**3. Using a program.**

A person uses a program if the function he or she causes the computer to perform-

(a) causes the program to be executed; or
(b) is itself a function of the program.

**4. Authorised access.**

Access by A person to any program or data held in a computer is authorised if-

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access such program or data from A person who is charged with giving such consent.

**5. References.**

(1) Reference to program or data held in a computer includes a reference to any program or data held in any removable storage medium and a computer may be regarded as containing any program or data held in any such medium.

(2) Reference to a program includes a reference to part of a program.

**6. Modification of contents.**

A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer-

(a) a program or data held in the computer concerned is altered or erased; or

(b) a program or data is added to its contents; and any act which contributes towards causing such a modification shall be regarded as causing it.

**7. Unauthorised modification.**

Modification is unauthorised if-

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from A person who is so entitled.

PART III – COMPUTER MISUSE OFFENCES.

**8. Unauthorised access.**

(1) A person who intentionally accesses or intercepts any data without authority or permission to do so commits an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a manner that causes such data to be modified destroyed or otherwise rendered ineffective commits an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section commits an offence.

(4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access to such data commits an offence.

(5) A person who commits any act specified under this section with intent to interfere with access to any information system so as to constitute a denial including a partial denial, of service to legitimate users commits an offence.

(6) The intent of a person to commit an offence under this section need not be directed at-

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(7) A person who commits an offence under this section is liable on conviction to imprisonment not exceeding six months or to a fine not exceeding twelve currency points or both.

**9. Access with intent to commit or facilitate commission of further offence.**

(1) A person commits an offence under this section if he or she commits an offence under section 9 above with intent to facilitate the commission of such offence whether by himself or by any other person.

(2) It is immaterial for the purposes of this section that the offence under this section committed on the same occasion as the offence under section 10 or on any future occasion.

(3) A person may commit an offence under this section even though the facts are such that the commission of the offence under this section is impossible.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding seventy-two currency points or to imprisonment not exceeding 3 years or both.

**10. Unauthorised modification of computer material.**

(1) A person commits an offence if-

(a) he or she does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he or she does the act, he or she has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer, and by so doing-

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent under subsection (1)(b) need not be directed at-

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification he or she intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind specified in subsection (2) is, or is intended to be permanent or temporary.

(6) A person who commits of an offence under this section is liable on conviction, to imprisonment not exceeding five years or to a fine not exceeding one hundred and twenty currency points or both.

**11. Unauthorised use or interception of computer service.**

(1) Subject to subsection (2), A person who knowingly-

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence and is liable on conviction to a fine not exceeding seventy two currency points or to imprisonment not exceeding 3 years or both; and in the case of a subsequent conviction, to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding 5 years or both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred and sixty eight currency points or to imprisonment not exceeding 7 years or both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at-

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

**12. Unauthorised obstruction of use of computer.**

(1) A person who, knowingly and without authority or lawful excuse-

(a) interferes with, or interrupts or obstructs the lawful use of, a computer;

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer, commits an offence and is liable on conviction to a fine not exceeding seventy two currency points or to imprisonment not exceeding 3 years or both and; in the case of a subsequent conviction, to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding 5 years or both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred sixty eight currency points or to imprisonment not exceeding 7 years or both.

**13. Unauthorised disclosure of access code.**

(1) A person who knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer commits an offence if he or she does so-

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding seventy two currency points or to imprisonment not exceeding 3 years or both and; in the case of a second or subsequent conviction, to a fine not exceeding one hundred twenty currency points or to imprisonment not exceeding 5 years or both.

**14. Breach of the confidentiality obligation.**

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has access to any electronic data, record, book, register, correspondence, information, document or any other material shall disclose to any other person or use for any other purpose other than that for which he or she obtained access, the contents of such electronic data, record, book, register, correspondence, information, document, or such

(2) A person who contravenes subsection (1) commits an offence and shall be liable on conviction to a fine not exceeding seventy-two currency points or to imprisonment for a term not exceeding three years or to both.

**15. Enhanced punishment for offences involving protected computers.**

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 9, 11, 12 or 13, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding 10 years or both.

(2) For the purposes of subsection (1), a computer is treated as a "protected computer" if the person committing the offence knows, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for-

(a) the security, defence or international relations of Uganda;
(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or
(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning conspicuously exhibited stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

**16. Abatements and attempts.**

(1) A person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act that offence and is liable on conviction to the punishment prescribed for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

**17. Child pornography.**

(1) A person commits an offence if he or she-

(a) produces child pornography for purposes of its distribution through a computer system;
(b) offers or makes available child pornography through a computer system;
(c) distributes or transmits child pornography through a computer system;
(d) procures child pornography through a computer system for oneself or another person;
(e) possesses child pornography on a computer system or on a computer-data storage medium.

(2) For purposes of this section "child pornography" includes pornographic material that visually depicts-

(a) a child engaged in sexually suggestive and explicit conduct;
(b) a person appearing to be child engaged in sexually suggestive and explicit conduct; or
(c) realistic images representing children engaged in sexually suggestive and explicit conduct.

(3) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding 5 years or both.

PART IV – MISCELLANEOUS

**18. Searches and Seizure.**

(1) Any authorised officer may seize any computer system or take any samples or copies of applications or data-
- (a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;
- (b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or
- (c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(2) Subject to subsection (5), a computer system referred to in subsection (1) may be seized, or samples or copies of applications or data may be taken, only by virtue of a search warrant.

(3) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (2)

(4) An investigating officer executing a search warrant referred to in subsection (2), may-
- (a) at any time search for, have access to, and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant; and
- (b) require A person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant.

(5) An investigating officer may, without a search warrant referred to in subsection (2), seize any computer system or take any samples or copies of applications or data or perform any of the actions referred to in subsection (4)-
- (a) if the person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data consents to such seizure; or
- (b) if that official on reasonable grounds believes-
  - (i) that a search warrant shall be issued under subsection (2) if he or she applies for such a warrant; and
  - (ii) that the delay in obtaining such a warrant would defeat the object of the search.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (4), whether by virtue of a search warrant or in terms of subsection (5), an investigating officer shall have due regard to the rights and interests of A person affected by such seizure to carry on his or her normal activities.

(7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers in terms of this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

(8) Any computer system seized, or samples or copies of applications or data taken by the investigating officer shall be returned within 72 hours unless the investigating has applied for and obtained an order in an inter party application for extension of such time.

**19. Evidence.**

(1) Notwithstanding the provisions of any law, information in any medium, including but not confined to data or computer output, shall be admissible as evidence of any fact stated in such information in any criminal proceedings in terms of this Act, if it is shown that a standard or best procedure, acceptable to the court, has been followed in obtaining the information concerned.

(2) In the event of any departure from procedure under subsection (1) which, in the opinion of the court, is not gravely prejudicial to the accused, such information shall still be admissible as evidence, but the court may attach correspondingly less weight to such evidence.

**20. Territorial jurisdiction.**

(1) Subject to subsection (2) the provisions of this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship, outside as well as within Uganda.

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

(3) For the purposes of this Act, this section applies if, for the offence in question-
(a) the accused was in Uganda at the material time; or
(b) the computer, program or data was in Uganda at the material time.

**21. Jurisdiction of Courts.**

A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.

SCHEDULE

**Currency point**

One currency point is equivalent to twenty thousand Uganda shillings.

## ANNEX 2

# THE ELECTRONIC SIGNATURES BILL, 2004

## Arrangement of Clauses.

PART - I - PRELIMINARY.

**Clause**



PART - II – ELECTRONIC SIGNATURES.



PART – III – SECURE DIGITAL SIGNATURES.



PART -IV - PUBLIC KEY INFRASTRUCTURE.

PART – IV- MISCELLANEOUS

# THE ELECTRONIC SIGNATURES BILL, 2004.

## A BILL for an Act

## ENTITLED

## THE ELECTRONIC SIGNATURES ACT, 2004.

**An Act to make provision for and to regulate the use of electronic signatures and to provide for other related matters.**

### 1. Interpretation.

In this Act, unless the context otherwise requires-

"accept a certificate" means-

(a) to manifest approval of a certificate, while knowing or having notice of its contents; or

(b) to apply to a certification authority for a certificate, without revoking the application by delivering notice of the revocation to the licensed certification authority, and obtaining a signed, written receipt from the certification authority, if the certification authority subsequently issues a certificate based on the application;

"advanced electronic signature" means an electronic signature, which is uniquely linked to the signatory; is reliably capable of identifying the signatory; is created using secure signature creation device that the signatory can maintain under his sole control; and is linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable.

"asymmetric cryptosystem" means an algorithm or series of algorithms, which provide a secure key pair;

"certificate" means a computer-based record which-

(a) identifies the certification authority issuing it;

(b) names or identifies its subscriber;

(c) contains the subscriber's public key; and

(d) is digitally signed by the certification authority issuing it;

"certification authority" means a person who issues a certificate;

"certification authority disclosure record" means an on-line and publicly accessible record that concerns a licensed certification authority, which is kept by the controller under subsection 21(5);

"certification practice statement" means a declaration of the practices, which a certification authority employs in issuing certificates generally, or employed in issuing a particular certificate;

"certify" means to declare with reference to a certificate, with ample opportunity to reflect, and with a duty to apprise oneself of all material facts;

"confirm" means to ascertain through diligent inquiry and investigation;

"controller" means the controller of certification authorities appointed under section 21;

"correspond", with reference to keys, means to belong to the same key pair;

"digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine-

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) whether the message has been altered since the transformation was made;

"electronic signature" means data in electronic form in, affixed thereto, 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;
"electronic signature product" means configured hardware or software, or relevant components thereof, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures;
"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator, an addressee in an electronic communication;
"forge a digital signature" means-

(a) to create a digital signature without the authorisation of the rightful holder of the private key; or

(b) to create a digital signature verifiable by a certificate listing as subscriber a person who either does not exist or does not hold the private key corresponding to the public key listed in the certificate;

"hash function" means a mathematical process, based on an algorithm which creates a digital representation, or compressed form of the message often referred to as a "message digest" or "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it . Any change to the message invariably produces a different hash result when the same hash function is used.
"hold a private key" means to be able to utilise a private key;
"incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated;
"issue a certificate" means the act of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate;
"key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates;
"licensed certification authority" means a certification authority to whom a licence has been issued by the controller and whose licence is in effect;
"message" means a digital representation of information;
"notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person;
"person" means a natural person or a body of persons, corporate or unincorporated, capable of signing a document, either legally or as a matter of fact;
"prescribed" means prescribed by or under this Act or any regulations made under this Act;
"private key" means the key of a key pair used to create a digital signature;
"public key" means the key of a key pair used to verify a digital signature and listed in the digital signature certificate;
"publish" means to record or file in a repository;
"qualified certification authority" means a certification authority that satisfies the requirements under section 23;
"recipient" means a person who receives or has a digital signature and is in a position to rely on it;
"recognised date/time stamp service" means a date/time stamp service recognised by the controller under section 79;
"recognised repository" means a repository recognised by the controller under section 77
"recommended reliance limit" means the monetary amount recommended for reliance on a certificate under section 75;

"repository" means a system for storing and retrieving certificates and other information relevant to digital signatures;
"revoke a certificate" means to make a certificate ineffective permanently from a specified time forward;
"rightfully hold a private key" means to be able to utilise a private key-

(a) which the holder or the holder's agents have not disclosed to any person in contravention of this act; and
(b) which the holder has not obtained through theft, deceit, eavesdropping or other unlawful means;

"security procedure" means a procedure for the purpose of----;

(a) verifying that an electronic record is that of a specific person; or
(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgement procedures, or similar security devices;

"secure signature creation device" means a signature creation device which meets the requirements laid down in section 4;
"signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents
"signature creation device" means configured software or hardware, used by the signatory to create an electronic signature;
"signature verification data" means unique data such as codes or public cryptographic keys, used for the purpose of verifying an electronic signature;
"signature verification device" means configured software or hardware, used for the purpose of verifying an electronic signature;
"signed" or "signature" and its grammatical variations includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;
"subscriber" means a person who-

(a) is the subject listed in a certificate;
(b) accepts the certificate; and
(c) holds a private key which corresponds to a public key listed in that certificate;

"suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward;
"this Act" includes any regulations made under this Act;
"time-stamp" means-

(a) to append or attach to a message, digital signature or certificate a digitally signed notation indicating at least the date, time and identity of the person appending or attaching the notation; or
(b) the notation so appended or attached;

"transactional certificate" means a certificate, incorporating by reference one or more digital signatures, issued and valid for a specific transaction;
"trustworthy system" means computer hardware and software which-

(a) are reasonably secure from intrusion and misuse;
(b) provide a reasonable level of availability, reliability and correct operation; and
(c) are reasonably suited to performing their intended functions;

"valid certificate" means a certificate which-

(a) a licensed certification authority has issued;
(b) has been accepted by the subscriber listed in it;

(c) has not been revoked or suspended; and
(d) has not expired:
Provided that a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference;

"verify a digital signature" means, in relation to a given digital signature, message and public key, to determine accurately that-

(a) the digital signature was created by the private key corresponding to the public key; and
(b) the message has not been altered since its digital signature was created;

"writing" or "written" includes any handwriting, typewriting, printing, electronic storage or transmission, or any other method of recording information or fixing information in a form capable of being preserved.

(2) For the purposes of this Act, a certificate shall be revoked by making a notation to that effect on the certificate or by including the certificate in a set of revoked certificates.

(3) The revocation of a certificate does not mean that it is destroyed or made illegible.

**2. Equal treatment of signature technologies.**

Nothing in this Act shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements for a signature in this Act or otherwise meets with the requirements of any other applicable law.

PART 11- ELECTRONIC SIGNATURES.

**3. Compliance with a requirement for a signature.**

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:
(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) where a purpose of legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph(3) does not limit the liability of any person-
(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph(1),the reliability of an electronic signature; or
(b) to adduce evidence of the non-reliability of an electronic signature.

**4. Conduct of the signatory.**

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) exercise reasonable care to avoid unauthorised use of its signature creation data;

(b) without undue delay, notify A person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

**5. Variation by agreement.**

The provisions of this Act may be derogated from or their effect may be varied by agreement unless that agreement would not be valid or effective under applicable law.

**6. Conduct of the relying party.**

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and

(ii) observe any limitation with respect to the certificate

**7. Trustworthiness.**

When determining whether or to what extent any systems procedures and human resources utilised by a certification service provider are trustworthy, regard may be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the state, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor;

**8. Conduct of the certification service provider**

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the certification service provider;
(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:
(i) the method used to identify the signatory;
(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) that the signature creation data are valid and have not been compromised;
(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;
(v) whether means exist for the signatory to give notice pursuant to section 5(1)
(vi) whether a timely revocation service is offered;

(e) where services under subsection (d) (v) are offered, provide a means for a signatory to give notice pursuant to section 5(1)(b) and, where services under subsection d(vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of subsection (1).

**9. Advanced signatures.**

(1) An advanced electronic signature, verified with qualified certificate, is equal to an autographic signature in relation to data in electronic form, and has therefore equal legal effectiveness and admissibility as evidence.

(2) The advanced signature verification process shall ensure that;
(a) the data used for verifying the electronic signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of the verification and identity of the certificate holder is correctly displayed to the verifier;
(c) the verifier can reliably establish the contents of the signed data:
(d) the authenticity and validity of the certificate required at the time of signature verification are verified;
(e) the use of a pseudonym is clearly indicated;
(f) any security-relevant changes can be detected.

**10. Secure electronic signature.**

If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, an electronic signature is executed in a trustworthy manner, reasonably and in good faith is relied upon by the relying party, such signature shall be treated as a secure electronic signature at the time of verification to the extent that it can be verified that said electronic signature satisfied, at the time it was made, the following criteria:
(a) the signature creation data used for signature creation is unique and its secrecy is reasonably assured;
(b) it was capable of being used to objectively identify such person;

(c) it was created in a manner or using a means under the sole control of the person using it, that cannot be readily duplicated or compromised;

(d) it is linked to the electronic record to which it relates in a manner such that if the record was changed to electronic signature would be invalidated.

(e) the signatory can reliably protect his signature creation data from unauthorised access

**11. Presumptions relating to secure and advanced electronic signatures.**

(1) In any civil proceedings involving a secure electronic record, it shall be presumed, unless the contrary is proved, that the secure or advanced electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any civil proceedings involving a secure or advanced electronic signature, the following shall be presumed unless the contrary is proved:

(i) the secure or advanced electronic signature is the signature of the person to whom it correlates: and

(ii) the secure or advanced electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(3) In the absence of a secure or advanced electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(4) The effect of presumptions provided in this section is to place on the party challenging the genuineness of a secure or advanced electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the court of fact that the non-existence of the presumed fact is more.

## PART III - SECURE DIGITAL SIGNATURES.

**12. Secure digital signatures.**

When any portion of an electronic record is signed with a digital signature the digital signature shall be treated as a secure electronic signature in respect to such portion of the record, if-

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to a public key listed in such certificate; and

(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because—

(i) the certificate was issued by a certification authority operating in compliance with regulations made under this Act

(ii) the certificate was issued by a Certification Authority outside Uganda recognised for this purpose by the controller pursuant to regulations made under this Act;

(iii) the certificate was issued by a department or ministry of the Government, an organ of state of statutory corporation approved by the minister to act as a certification Authority on such conditions as the regulations may specify; or

(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

**13. Satisfaction of signature requirements.**

(1) Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where-

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
(b) that digital signature was affixed by the signer with the intention of signing the message; and
(c) the recipient has no knowledge or notice that the signer-
  (i) has breached a duty as a subscriber; or
  (ii) does not rightfully hold the private key used to affix the digital signature.

(2) Notwithstanding any written law to the contrary-
(a) a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumbprint or any other mark; and
(b) a digital signature created in accordance with this Act shall be deemed to be a legally binding signature.

(3) Nothing in this Act shall preclude any symbol from being valid as a signature under any other applicable law.

**14. Unreliable digital signatures**.

(1) Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.

(2) Where the recipient determines not to rely on a digital signature under this section, the recipient shall promptly notify the signer of its determination not to rely on a digital signature and the grounds for that determination.

**15. Digitally signed document deemed to be written document.**

(1) A message shall be as valid, enforceable and effective as if it had been written on paper if-
(a) it bears in its entirety a digital signature; and
(b) that digital signature is verified by the public key listed in a certificate which-
  (i) was issued by a licensed Certification Authority; and
  (ii) was valid at the time the digital signature was created.

(2) Nothing in this Act shall preclude any message, document or record from being considered written or in writing under any other applicable law.

**16. Digitally signed document deemed to be original document.**

A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

**17. Authentication of digital signatures**.

A certificate issued by a licensed Certification Authority shall be an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgement appear with the digital signature and regardless of whether the signer physically appeared

(a) Verifiable by that certificate; and
(b) affixed when that certificate was valid.

**18. Presumptions in adjudicating disputes**.

In adjudicating a dispute involving a digital signature, a court shall presume-

(a) that a certificate digitally signed by a licensed certification authority and-
  (i) published in a recognised repository; or
  (ii) made available by the issuing licensed certification authority or by the subscriber listed in the certificate, is issued by the licensed certification authority which digitally signed it and is accepted by the subscriber listed in it;
(b) that the information listed in a valid certificate and confirmed by a licensed certification authority issuing the certificate is accurate;
(c) that where the public key verifies a digital signature listed in a valid certificate issued by a licensed certification authority-
  (i) that digital signature is the digital signature of the subscriber listed in that certificate;
  (ii) that digital signature was affixed by that subscriber with the intention of signing the message; and
  (iii) the recipient of that digital signature has no knowledge or notice that the signer-
    (A) has breached a duty as a subscriber; or
    (B) does not rightfully hold the private key used to affix the digital signature; and
(d) that a digital signature was created before it was time-stamped by a recognised date/time stamp service utilising a trustworthy system.

PART IV - PUBLIC KEY INFRASTRUCTURE (PKI).

**19. Sphere of Application.**

This part shall specifically apply to digital signatures or such signatures that are able to use the Public Key Infrastructure (PKI).

**20. Appointment of Controller.**

(1) The Minister shall appoint a Controller of Certification Authorities for the purposes of this Act, in particular for the purpose of monitoring and overseeing the activities of certification authorities.

(2) The Controller shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act.

(3) The minister is to be consulted on the appointment of officers and staff, as the Controller considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act.

(4) The Controller and all officers and servants appointed by the Controller under subsection (3) shall exercise their powers under this Act subject to such directions as to general policy guidelines as may be given by the Minister.

(5) The Controller shall maintain a publicly accessible database containing a Certification Authority disclosure record for each Certification Authority, which shall contain all the particulars required under the regulations made under this Act.

(6) The Controller shall publish the contents of the database in at least one recognised repository.

**21. Certification authorities to be licensed.**

(1) No person shall carry on or operate, or hold himself out as carrying on or operating, as a certification authority unless that person holds a valid licence issued under this Act.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding fifty thousand shillings for each day the offence continues to be committed.

(3) The Minister may, on an application in writing being made in accordance with this Act, exempt a person operating as a Certification Authority within an organisation where certificates and key pairs are issued to members of the organisation for internal use only and the minister shall not delegate this power to the controller.

(4) The liability limits specified in Chapter 8 of Part V shall not apply to an exempted Certification Authority and Part VI shall not apply in relation to a digital signature verified by a certificate issued by an exempted Certification Authority.

**22. Qualifications of certification authorities.**

(1) The Minister shall, by regulations made under this Act, prescribe the qualification requirements for certification authorities.

(2) The Minister may at any time vary or amend the qualification requirements prescribed under subsection (1) provided that any such variation or amendment shall not be applied to a Certification Authority holding a valid licence under this Act until the expiry of that licence.

**23. Functions of licensed certification authorities.**

(1) The function of a Certification Authority shall be to issue a certificate to a subscriber upon application and upon satisfaction of the Certification Authority's requirements as to the identity of the subscriber to be listed in the certificate and upon payment of the prescribed fees and charges.

(2) The Certification Authority shall, before issuing any certificate under this Act, take all reasonable measures to check for proper identification of the subscriber to be listed in the certificate.

**24. Application for licence**.

(1) An application for the grant of a licence under this Act shall be made in writing to the Controller in such form as may be prescribed.

(2) Every application under subsection (1) shall be accompanied by such documents or information as may be prescribed and the Controller may, at any time after receiving the application and before it is determined, require the applicant to provide such additional documents or information as may be considered necessary by the Controller for the purposes of determining the suitability of the applicant for the licence.

(3) Where any additional document or information required under subsection (2) is not provided by the applicant within the time specified in the requirement or any extension thereof granted by the Controller, the application shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

**25. Grant or refusal of licence**.

(1) The Controller shall, on an application having been duly made in accordance with Section 10 and

after being provided with all such documents and information as he may require, consider the application, and where he is satisfied that the applicant is a qualified Certification Authority and a suitable licensee, and upon payment of the prescribed fee, grant the licence with or without conditions, or refuse to grant a licence.

(2) Every licence granted under subsection (1) shall set out the duration of the licence and the licence number.

(3) The terms and conditions imposed under the licence may at any time be varied or amended by the Controller provided that the licensee is given a reasonable opportunity of being heard.

(4) The Controller shall notify the applicant in writing of his decision to grant or refusal to grant a licence within 30 days of receiving the application.

**26. Revocation of licence.**

(1) The Controller may revoke a licence granted under section 8 if he is satisfied that-

(a) the Certification Authority has failed to comply with any obligation imposed upon it by or under this Act;

(b) the Certification Authority has contravened any condition imposed under the licence, any provision of this Act or any other written law;

(c) the Certification Authority has, either in connection with the application for the licence or at any time after the grant of the licence, provided the Controller with false, misleading or inaccurate information or a document or declaration made by or on behalf of the Certification Authority or by or on behalf of A person who is or is to be a director, controller or manager of the licensed certification authority which is false, misleading or inaccurate;

(d) the Certification Authority is carrying on its business in a manner which is prejudicial to the interest of the public or to the national economy;

(e) the licensed Certification Authority has insufficient assets to meet its liabilities;

(f) a winding up order has been made against the licensed certification authority or a resolution for its voluntary winding-up has been passed;

(g) the Certification Authority or its director, controller or manager has been convicted of any offence under this Act in his capacity as ; or

(h) the Certification Authority has ceased to be a qualified certification authority.

(2) Before revoking a licence, the Controller shall give the licensed Certification Authority a notice in writing of his intention to do so and require the licensed Certification Authority to show cause within thirty days as to why the licence should not be revoked.

(3) Where the Controller decides to revoke the licence, he shall notify the certification authority concerned of his decision by a notice in writing within 48 hours of making such a decision.

(4) The revocation of a licence shall take effect where there is no appeal against such revocation, on the expiration of thirty days from the date on which the notice of revocation is served on the licensed Certification Authority.

(5) Where an appeal has been made against the revocation of a licence, the certification authority whose licence has been so revoked shall not issue any certificates until the appeal has been disposed of and the revocation has been set aside by the Minister but nothing in this subsection shall prevent the Certification Authority from fulfilling its other obligations to its subscribers during such period.

(6) A person who contravenes subsection (5) commits an offence and shall, on conviction, be liable to a fine not seventy two currency points or to imprisonment for a term not exceeding three years or to both

(7) Where the revocation of a licence has taken effect, the Controller shall, as soon as practicable, cause such revocation to be published in the Certification Authority disclosure record he maintains for the certification authority concerned and advertised in at least two English language national daily newspapers for at least three consecutive days.

**27. Appeal**.

(1) A person who is aggrieved by-

(a) the refusal of the Controller to license any certification authority under Section 11 or to renew any such licence under section 20; or

(b) the revocation of any licence under section 12,

may appeal in writing to the Minister within thirty days from the date on which the notice of refusal or revocation is served on that person.

(2) The decision of the Minister under this section shall be final and conclusive.

**28. Surrender of licence.**

(1) A Certification Authority may surrender its licence by forwarding it to the Controller with a written notice of its surrender.

(2) The surrender shall take effect on the date the Controller receives the licence and the notice under subsection (1), or where a later date is specified in the notice, on that date.

(3) The licensed Certification Authority shall, not later than fourteen days after the date referred to in sub-section (2), cause such surrender to be published in the Certification Authority disclosure record of the certification authority concerned and advertised in at least two English language national daily newspapers for at least three days consecutive.

**29. Effect of revocation, surrender or expiry of licence.**

(1) Where the revocation of a licence under section 12 or its surrender under section 11 has taken effect, or where the licence has expired, the licensed Certification Authority shall immediately cease to carry on or operate any business in respect of which the licence was granted.

(2) Notwithstanding subsection (1), the Minister may, on the recommendation of the Controller, authorise the licensed Certification Authority in writing to carry on its business for such duration as the Minister may specify in the authorisation for the purpose of winding up its affairs.

(3) Notwithstanding subsection (1), a licensed Certification Authority whose licence has expired shall be entitled to carry on its business as if its licence had not expired upon proof being submitted to the Controller that the licensed Certification Authority has applied for a renewal of the licence and that such application is pending determination.

(4) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding Seventy two currency points or to imprisonment for a term not exceeding three years or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five currency points for each day the offence continues to be committed.

(5) Without prejudice to the Controller's powers under Section 36, the revocation of a licence under Section 9 or its surrender under Section 14 or its expiry shall not affect the validity or effect of any certificate issued by the Certification Authority concerned before such revocation, surrender or expiry.

(6) For the purposes of subsection (5), the Controller shall appoint another licensed Certification Authority to take over the certificates issued by the Certification Authority whose licence has been revoked or surrendered or has expired and such certificates shall, to the extent that they comply with the

requirements of the appointed licensed Certification Authority, be deemed to have been issued by that licensed Certification Authority.

(7) Nothing in subsection (6) shall preclude the appointed licensed Certification Authority from requiring the subscriber to comply with its requirements in relation to the issuance of certificates or from issuing a new certificate to the subscriber for the unexpired period of the original certificate provided that any additional fees or charges to be imposed shall only be imposed with the prior written approval of the Controller.

**30. Effect of lack of licence.**

(1) The liability limits specified in chapter 8 of Part V shall not apply to unlicensed Certification Authorities.

(2) Part VI shall not apply in relation to an electronic signature, which cannot be verified by a certificate issued by a licensed certification authority.

(3) In any other case, unless the parties expressly provide otherwise by contract between themselves, the licensing requirements under this Act shall not affect the effectiveness, enforceability or validity of any digital signature.

**31. Return of licence**.

(1) Where the revocation of a licence under Section 12 has taken effect, or where the licence has expired and no application for its renewal has been submitted within the period specified or where an application for renewal has been refused under Section 20, the licensed certification authority shall within fourteen days return the licence to the Controller.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding forty eight currency points or to imprisonment for a term not exceeding two years or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two and half currency points for each day the offence continues to be committed, and the court shall retain the licence and forward it to the controller.

**32. Restricted licence**.

(1) The Controller may classify licences according to specified limitations including-
- (a) maximum number of outstanding certificates;
- (b) cumulative maximum of recommended reliance limits in certificates issued by the licensed certification authority; and
- (c) issuance only within a single firm or organisation.

(2) The Controller may issue licences restricted according to the limits of each classification.

(3) A licensed Certification Authority that issues a certificate exceeding the restrictions of its licence commits an offence.

(4) Where a licensed certification authority issues a certificate exceeding the restrictions of its licence, the liability limits specified in chapter 8 of Part V shall not apply to the licensed certification authority in relation to that certificate.

(5) Nothing in subsection (3) or (4) shall affect the validity or effect of the issued certificate.

**33. Restriction on use of expression "certification authority".**

(1) Except with the written consent of the controller, no person, not being a licensed certification authority, shall assume or use the expressions "certification authority" or "licensed certification authority", as the

case may be, or any derivative of these expressions in any language, or any other words in any language capable of being construed as indicating the carrying on or operation of such business, in relation to the business or any part of the business carried on by such person, or make any representation to such effect in any bill head, letter, paper, notice, advertisement or in any other manner.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding ninety six currency points or to imprisonment for a term not exceeding four years or to both.

**34. Renewal of licence**.

(1) Every licensed certification authority shall submit an application to the controller in such form as may be prescribed for the renewal of its licence at least thirty days before the date of expiry of the licence and such application shall be accompanied by such documents and information as may be required by the controller.

(2) The prescribed fee shall be payable upon approval of the application.

(3) If any licensed certification authority has no intention of renewing its licence, the licensed certification authority shall, at least thirty days before the expiry of the licence, publish such intention in the certification authority disclosure record of the certification authority concerned and advertise such intention in at least two English language national daily newspapers for at least three consecutive days.

(4) Without prejudice to any other grounds, the controller may refuse to renew a licence where the requirements of subsection (1) have not been complied with.

**35. Lost license.**

(1) Where a certification authority has lost its license, it shall immediately notify the controller in writing of the loss.

(2) The certification authority shall, as soon as practicable, submit an application for a replacement license accompanied by all such information and documents as may be required by the controller together with the prescribed fee.

**36. Recognition of other licenses.**

(1) The controller may recognise, by order published in the Gazette, certification authorities licensed or otherwise authorised by entities outside Uganda that satisfy the prescribed requirements.

(2) Where a license or other authorisation of an entity is recognised under subsection (1)-

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority licensed or otherwise authorized by such an entity shall have effect in the same manner as a recommended reliance limit specified in a certificate issued by a certification authority of Uganda; and

(b) Part V shall apply to the certificates issued by the certification authority licensed or otherwise authorized by such entity in the same manner as it applies to a certificate issued by a certification authority of Uganda.

**37. Performance audit.**

(1) The operations of a certification authority shall be audited a least once a year to evaluate its compliance with this Act.

(2) The audit shall be carried out by an internationally recognised computer security professional or a certified public accountant having expertise in this field.

(3) The qualifications of the auditors and the procedure for an audit shall be as may be prescribed by regulations made under this Act.

(4) The controller shall maintain and publish, the date and result of the audit in the certification authority disclosure record he maintains for the certification authority concerned.

**38. Activities of certification authorities.**

(1) A certification authority shall only carry on such activities as may be specified in its license.

(2) A certification Authority shall carry on its activities in accordance with this Act and any regulations made under this Act.

**39. Requirement to display license.**

A certification authority shall at all times display its license in a conspicuous place at its place of business and on its website.

**40. Requirement to submit information on business operations**.

(1) A licensed certification authority shall submit to the controller such information and particulars including financial statements, audited balance sheets and profit and loss accounts relating to its entire business operations as may be required by the controller within such time as he may determine.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding twelve currency points or to imprisonment for a term not exceeding six months or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding one currency point thousand shillings for each day the offence continues to be committed.

**41. Notification of change of information.**

(1) Every certification authority shall, before making any amendment or alteration to any of its constituent documents, or before any change in its director or chief executive officer, furnish the controller particulars in writing of any such proposed amendment, alteration or change.

(2) Every licensed certification authority shall immediately notify the controller of any amendment or alteration to any information or document which has been furnished to the controller in connection with the licence.

**42. Use of trustworthy systems.**

(1) A certification authority shall only use a trustworthy system -

(a) to issue, suspend or revoke a certificate;

(b) to publish or give notice of the issuance, suspension or revocation of a certificate; and

(c) to create a private key, whether for itself or for a subscriber.

(2) A subscriber shall only use a trustworthy system to create a private key.

**43. Disclosures on inquiry.**

(1) A certification authority shall, on an inquiry being made to it under this Act, disclose any material certification practice statement and any fact material to either the reliability of a certificate, which it has issued, or its ability to perform its services.

(2) A certification authority may require a signed, written and reasonably specific inquiry from an identified person, and payment of the prescribed fee, as conditions precedent to affecting a disclosure required under subsection (1).

**44. Prerequisites to issuance of certificate to subscriber.**

(1) A certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(a) the certification authority has received a request for issuance signed by the prospective subscriber; and

(b) the certification authority has confirmed that-

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber has duly authorised the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(2) The requirements of subsection (1) shall not be waived or disclaimed by the certification authority, the subscriber, or both.

**45. Publication of issued and accepted certificate**.

(1) Where the subscriber accepts the issued certificate, the certification authority shall publish a signed copy of the certificate in a recognised repository, as the certification authority and the subscriber named in the certificate may agree, unless a contract between the certification authority and the subscriber provides otherwise.

(2) Where the subscriber does not accept the certificate, a certification authority shall not publish it, or shall cancel its publication if the certificate has already been published.

**46. Adoption of more rigorous requirements permitted.**

Nothing in sections 30 and 31 shall preclude a certification authority from conforming to standards, certification practice statements, security plans or contractual requirements more rigorous than, but nevertheless consistent with, this Act.

**47. Suspension or revocation of certificate for faulty issuance.**

(1) Where after issuing a certificate a certification authority confirms that it was not issued in accordance with sections 30 and 31, the certification authority shall immediately revoke it.

(2) A certification authority may suspend a certificate which it has issued for a reasonable period not exceeding forty-eight hours as may be necessary for an investigation to be carried out to confirm the grounds for a revocation under subsection (1).

(3) The certification authority shall immediately notify the subscriber of a revocation or suspension under this section.

**48. Suspension or revocation of certificate by order.**

(1) The controller may order the certification authority to suspend or revoke a certificate issued by it

where the controller determines that-

(a) the certificate was issued without compliance with sections 30 and 31; and

(b) the non-compliance poses a significant risk to persons reasonably relying on the certificate.

(2) Before making a determination under subsection (1), the controller shall give the licensed certification authority and the subscriber a reasonable opportunity of being heard.

(3) Notwithstanding subsections (1) and (2), where in the opinion of the controller there exists an emergency that requires an immediate remedy, the controller may, after consultation with the Minister, suspend a certificate for a period not exceeding forty-eight hours.

**49. Warranties to subscriber**.

(1) By issuing a certificate, a Certification Authority warrants to the subscriber named in the certificate that-

(a) the certificate contains no information known to the Certification Authority to be false;

(b) the certificate satisfies all the requirements of this Act; and

the Certification Authority has not exceeded any limits of its licence in issuing the certificate.

(2) A Certification Authority shall not disclaim or limit the warranties under subsection (1).

**50. Continuing obligations to subscriber.**

Unless the subscriber and Certification Authority otherwise agree, a Certification Authority, by issuing a certificate, promises to the subscriber-

(a) to act promptly to suspend or revoke a certificate in accordance with chapters 5 or 6; and

(b) to notify the subscriber within a reasonable time of any facts known to the licensed certification authority, which significantly affect the validity, or reliability of the certificate once it is issued.

**51. Representations upon issuance**.

By issuing a certificate, a Certification Authority certifies to all who reasonably rely on the information contained in the certificate that-

(a) the information in the certificate and listed as confirmed by the licensed certification authority is accurate;

(b) all information foreseeable material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) the subscriber has accepted the certificate; and

(d) the Certification Authority has complied with all applicable laws governing the issuance of the certificate.

**52. Representations upon publication.**

By publishing a certificate, a Certification Authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the licensed certification authority has issued the certificate to the subscriber.

**53. Implied representations by subscriber.**

By accepting a certificate issued by a Certification Authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that-

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;
(b) all representations made by the subscriber to the Certification Authority and material to information listed in the certificate are true; and
(c) all material representations made by the subscriber to a Certification Authority or made in the certificate and not confirmed by the Certification Authority in issuing the certificate are true.

**54. Representations by agent of subscriber.**

By requesting on behalf of a principal the issuance of a certificate naming the principal as subscriber, the requesting person certifies in that person's own right to all who reasonably rely on the information contained in the certificate that the requesting person-

(a) holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and
(b) has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

**55. Disclaimer or indemnity limited.**

A Person shall not disclaim or contractually limit the application of this chapter, nor obtain indemnity for its effects, if the disclaimer, limitation or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

**56. Indemnification of certification authority by subscriber.**

(1) By accepting a certificate, a subscriber undertakes to indemnify the issuing licensed certification authority for any loss or damage caused by issuance or publication of the certificate in reliance on-
(a) a false and material representation of fact by the subscriber; or
(b) the failure by the subscriber to disclose a material fact, if the representation or failure to disclose was made either with intent to deceive the Certification Authority or a person relying on the certificate, or with negligence.

(2) Where the Certification Authority issued the certificate at the request of one or more agents of the subscriber, the agent or agents personally undertake to indemnify the Certification Authority under this section, as if they were accepting subscribers in their own right.

(3) The indemnity provided in this section shall not be disclaimed or contractually limited in scope.

**57. Certification of accuracy of information given**.

In obtaining information of the subscriber material to the issuance of a certificate, the Certification Authority may require the subscriber to certify the accuracy of relevant information under oath or affirmation.

**58. Duty of subscriber to keep private key secure.**

By accepting a certificate issued by a Certification Authority, the subscriber named in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorised to create the subscriber's digital signature.

**59. Property in private key.**

A private key is the personal property of the subscriber who rightfully holds it.

**60. Fiduciary duty of a certification authority.**

Where a Certification Authority holds the private key corresponding to a public key listed in a certificate which it has issued, the Certification Authority shall hold the private key as a fiduciary of the subscriber named in the certificate, and may use that private key only with the subscriber's prior written approval, unless the subscriber expressly and in writing grants the private key to the licensed certification authority and expressly and in writing permits the licensed certification authority to hold the private key according to other terms.

**61. Suspension of certificate by certification authority.**

(1) Unless the Certification Authority and the subscriber agree otherwise, the licensed Certification Authority, which issued a certificate, which is not a transactional certificate, shall suspend the certificate for a period not exceeding forty-eight hours-

(a) upon request by a person identifying himself as the subscriber named in the certificate, or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee or member of the immediate family of the subscriber; or

(b) by order of the Controller under section 34.

(2) The Certification Authority shall take reasonable measures to check the identity or agency of the person requesting suspension.

**62. Suspension of certificate by controller**.

(1) Unless the certificate provides otherwise or the certificate is a transactional certificate, the Controller may suspend a certificate issued by a Certification Authority for a period of forty-eight hours, if-

(a) a person identifying himself as the subscriber named in the certificate or as an agent, business associate, employee or member of the immediate family of the subscriber requests suspension; and

(b) the requester represents that the Certification Authority, which issued the certificate, is unavailable.

(2) The Controller may require the person requesting suspension to provide evidence, including a statement under oath or affirmation regarding his identity and authorisation, and the unavailability of the issuing licensed certification authority, and may decline to suspend the certificate in his or its discretion.

(3) The Controller or other law enforcement agency may investigate suspensions by the Controller for possible wrongdoing by persons requesting suspension.

**63. Notice of suspension**.

(1) Immediately upon suspension of a certificate by a Certification Authority, the Certification Authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the Certification Authority shall publish signed notices of the suspension in all such repositories.

(3) Where any repository specified no longer exists or refuses to accept publication, or if no such repository is recognised under section 68 the Certification Authority shall also publish the notice in a recognised repository.

(4) Where a certificate is suspended by the Controller, the Controller shall give notice as required in this section for a Certification Authority provided that the person requesting suspension pays in advance any prescribed fee required by a repository for publication of the notice of suspension.

**64. Termination of suspension initiated by request.**

A Certification Authority shall terminate a suspension initiated by request-

(a) where the subscriber named in the suspended certificate requests termination of the suspension, only if the Certification Authority has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorised to terminate the suspension; or

(b) where the licensed Certification Authority discovers and confirms that the request for the suspension was made without authorization by the subscriber.

**65. Alternate contractual procedures.**

(1) The contract between a subscriber and a licensed Certification Authority may limit or preclude requested suspension by the Certification Authority or may provide otherwise for termination of a requested suspension.

(2) Where the contract limits or precludes suspension by the Controller when the issuing licensed certification authority is unavailable, the limitation or preclusion shall be effective only if notice of it is published in the certificate.

**66. Effect of suspension of certificate.**

Nothing in this Chapter shall release the subscriber from the duty under Section 46 to keep the private key secure while a certificate is suspended.

**67. Revocation on request.**

(1) A licensed certification authority shall revoke a certificate, which it issued but which is not a transactional certificate, -

(a) upon receiving a request for revocation by the subscriber named in the certificate; and

(b) upon confirming that the person requesting revocation is that subscriber or is an agent of that subscriber with authority to request the revocation.

(2) A Certification Authority shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity of the person requesting the revocation or of the agent.

**68. Revocation on subscriber's demise.**

A licensed certification authority shall revoke a certificate which it issued-

(a) upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead; or

(b) upon presentation of documents effecting a dissolution of the subscriber or upon confirming

**69. Revocation of unreliable certificates.**

(1) A licensed certification authority may revoke one or more certificates, which it issued if the certificates are or become unreliable regardless of whether the subscriber consents to the revocation and notwithstanding any provision to the contrary in a contract between the subscriber and the licensed Certification Authority.

(2) Nothing in subsection (1) shall prevent the subscriber from seeking damages or other relief against the licensed Certification Authority in the event of wrongful revocation.

**70. Notice of revocation.**

(1) Immediately upon revocation of a certificate by a licensed Certification Authority, the licensed certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

(2) Where one or more repositories are specified, the licensed Certification Authority shall publish signed notices of the revocation in all such repositories.

(3) Where any repository specified no longer exists or refuses to accept publication, or if no such repository is recognised under section 68, the licensed certification authority shall also publish the notice in a recognised repository.

**71. Effect of revocation request on subscriber.**

Where a subscriber has requested for the revocation of a certificate, the subscriber ceases to certify as provided in Chapter 3 and has no further duty to keep the private key secure as required under section 44 -

(a) when notice of the revocation is published as required under section 56; or

(b) when 48 hours have lapsed after the subscriber requests for the revocation in writing, supplies to the issuing licensed certification authority information reasonably sufficient to confirm the request, and pays any prescribed fee, whichever occurs first.

**72. Effect of notification on certification authority.**

Upon notification as required under section 56, a Certification Authority shall be discharged of its warranties based on issuance of the revoked certificate and ceases to certify as provided in sections 36 and 37 in relation to the revoked certificate.

**73. Expiration of certificate.**

(1) The date of expiry of a certificate shall be specified in the certificate.

(2) A certificate may be issued for any period not exceeding three years from the date of issuance.

(3) When a certificate expires, the subscriber and licensed Certification Authority shall cease to certify as provided under this Act and the licensed Certification Authority shall be discharged of its duties based on issuance in relation to the expired certificate.

(4) The expiry of a certificate shall not affect the duties and obligations of the subscriber and licensed Certification Authority incurred under and in relation to the expired certificate.

**74. Reliance limit.**

(1) A licensed certification authority shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed Certification Authority may specify different limits in different certificates as it considers fit.

**75. Liability limits for certification authorities.**

Unless a licensed certification authority waives the application of this section, a licensed Certification Authority-

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed Certification Authority complied with the requirements of this Act;

(b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either-

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed Certification Authority is required to confirm; or

(ii) failure to comply with sections 30 and 31 in issuing the certificate.

**76. Recognition of repositories.**

(1) The Controller may recognise one or more repositories, after determining that a repository to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognition of repositories shall be as may be prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised repositories in such form and manner as he may determine.

**77. Liability of repositories.**

(1) Notwithstanding any disclaimer by the repository or any contract to the contrary between the repository and a licensed certification authority or a subscriber, a repository shall be liable for a loss incurred by a person reasonably relying on an electronic signature verified by the public key listed in a suspended or revoked certificate, if loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation, and the repository had failed to publish the notice when the person relied on the digital signature.

(2) Unless waived, a recognised repository or the owner or operator of a recognised repository-

(a) shall not be liable for failure to record publication of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(b) shall not be liable under subsection (1) in excess of the amount specified in the certificate as the recommended reliance limit;

(c) shall not be liable for misrepresentation in a certificate published by a certification authority;

(d) shall not be liable for accurately recording or reporting information which a licensed certification authority, a court or the Controller has published as required or permitted under this Act, including information about the suspension or revocation of a certificate; and

(e) shall not be liable for reporting information about a certification authority, a certificate or a subscriber, if such information is published as required or permitted under this Act or is published by order of the Controller in the performance of his licensing and regulatory duties under this Act.

**78. Recognition of date/time stamp services.**

(1) The Controller may recognise one or more date/time stamp services, after determining that a service to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognition of date/time stamp services shall be as may be prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised date/time stamp services in such form and manner as he may determine.

## PART IV - MISCELLANEOUS.

### 79. Prohibition against dangerous activities.

(1) No certification authority, whether licensed or not, shall conduct its business in a manner that creates an unreasonable risk of loss to the subscribers of the certification authority, to persons relying on certificates issued by the certification authority or to a repository.

(2) The Controller may publish in one or more recognised repositories brief statements advising subscribers, persons relying on digital signatures and repositories about any activities of a certification authority, whether licensed or not, which create a risk prohibited under Subsection (1).

(3) The certification authority named in a statement as creating or causing a risk may protest the publication of the statement by filing a brief written defence.

(4) On receipt of a protest made under subsection (3), the Controller shall publish the written defence together with the Controller's statement, and shall immediately give the protesting certification authority notice and a reasonable opportunity of being heard.

(5) Where, after a hearing, the Controller determines that the publication of the advisory statement was unwarranted, the Controller shall revoke the advisory statement.

(6) Where, after a hearing, the Controller determines that the advisory statement is no longer warranted, the Controller shall revoke the advisory statement.

(7) Where, after a hearing, the Controller determines that the advisory statement remains warranted, the Controller may continue or amend the advisory statement and may take further legal action to eliminate or reduce the risk prohibited under subsection (1).

(8) The Controller shall publish his decision under subsection (5), (6) or (7), as the case may be, in one or more recognised repositories.

### 80. Obligation of confidentiality.

(1) Except for the purpose of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under this Act, obtained access to any electronic record, book, register, correspondence, information, document or other material to any other person.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding forty-eight currency points or to imprisonment for a term not exceeding two years or to both.

### 81. False information.

A person who makes, orally or in writing, signs or furnishes any declaration, return, certificate or other document or information required under this Act which is untrue, inaccurate or misleading in any particular way commits

an offence and shall, on conviction, be liable to a fine not exceeding one hundred and twenty currency points or to imprisonment for a term not exceeding five years or to both.

**82. Offences by body corporate.**

(1) Where a body corporate commits an offence under this Act, A person who at the time of the commission of the offence was a director, manager, secretary or other similar officer of the body corporate or was purporting to act in any such capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management-

(a) may be charged severally or jointly in the same proceedings with the body corporate; and

(b) where the body corporate is convicted of the offence, such a person shall be deemed to have committed an offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves-

(i) that the offence was committed without his knowledge, consent or connivance; and

(ii) that he took all reasonable precautions and had exercised due diligence to prevent the commission of the offence.

(2) Where A person would be liable under this Act to any punishment or penalty for any act, omission, neglect or default, he shall be liable to the same punishment or penalty for every such act, omission, neglect or default of any employee or agent of his, or of the employee of such agent, if such act, omission, neglect or default was committed-

(a) by his employee in the course of his employment;

(b) by the agent when acting on his behalf; or

(c) by the employee of such agent in the course of his employment by such agent or otherwise on behalf of the agent.

**83. Authorised officer.**

(1) The Minister may in writing authorise any public officer or officer of the Controller to exercise the powers of enforcement under this Act.

(2) Any such officer shall be deemed to be a public servant within the meaning of the Criminal Procedure Code.

(3) In exercising any of the powers of enforcement under this Act, an authorised officer shall on demand produce to the person against whom he is acting, the authority issued to him by the Minister.

**84. Power to investigate.**

(1) The Controller may investigate the activities of a certification authority material to its compliance with this Act.

(2) For the purposes of subsection (1), the Controller may issue orders to a certification authority to further its investigation and secure compliance with this Act.

(3) Further, in any case relating to the commission of an offence under this Act, any authorized officer carrying on an investigation may exercise all or any of the special powers in relation to police investigation in sizeable cases given by the Criminal Procedure Code.

**85. Search by warrant.**

(1) If it appears to a Magistrate, upon written information on oath and after such inquiry as he considers necessary, that there is reasonable cause to believe that an offence under this Act is being or has been committed on any premises, the Magistrate may issue a warrant authorizing any police officer not below the rank of Inspector, or any authorized officer named therein, to enter the premises at any

reasonable time by day or by night, with or without assistance and if need be by force, to search for and seize-

(a) copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed;

(b) any signboard, card, letter, pamphlet, leaflet, notice or other device representing or implying that the person is a licensed certification authority; and

(c) any other document, article or item that is reasonably believed to furnish evidence of the commission of such offence.

(2) A police officer or an authorised officer conducting a search under subsection (1) may, if in his opinion it is reasonably necessary to do so for the purpose of investigating into the offence, search A person who is in or on such premises.

(3) A police officer or an authorised officer making a search of a person under subsection (2) may seize, detain or take possession of any book, accounts, document, computerised data, card, letter, pamphlet, leaflet, notice, device, article or item found on such person for the purpose of the investigation being carried out by such officer.

(4) No female person shall be searched under this section except by another female person.

(5) Where, by reason of its nature, size or amount, it is not practicable to remove any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item seized under this section, the seizing officer shall, by any means, seal such book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item in the premises or container in which it is found.

(6) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (5) or removes any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item under seal or attempts to do so commits an offence.

**86. Search and seizure without warrant.**

If a police officer not below the rank of Inspector in any of the circumstances referred to in Section 77 has reasonable cause to believe that by reason of delay in obtaining a search warrant under that section the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, such officer may enter such premises and exercise in, upon and in respect of the premises all the powers referred to in Section 77 in as full and ample a manner as if he were authorized to do so by a warrant issued under that section.

**87. Access to computerised data.**

(1) A police officer conducting a search under section 77 or 75 or an authorised officer conducting a search under section 74 shall be given access to computerised data whether stored in a computer or otherwise.

(2) For the purposes of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data.

**88. List of things seized.**

(1) Except as provided in subsection (2), where any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item is seized under section 77 or 78, the seizing officer shall prepare a list of the things seized and immediately deliver a copy of the list

signed by him to the occupier of the premises which have been searched, or to his agent or servant, at those premises.

(2) Where the premises are unoccupied, the seizing officer shall whenever possible post a list of the things seized conspicuously on the premises.

**89.** Obstruction of authorised officer

A person who obstructs, impedes, assaults or interferes with any authorized officer in the performance of his functions under this Act commits an offence.

**90. Additional powers**.

An authorised officer shall, for the purposes of the execution of this Act, have power to do all or any of the following:

(a) to require the production of records, accounts, computerised data and documents kept by a licensed certification authority and to inspect, examine and copy any of them;

(b) to require the production of any identification document from A person in relation to any case or offence under this Act;

(c) to make such inquiry as may be necessary to ascertain whether the provisions of this Act have been complied with.

**91. General penalty.**

(1) A person who commits an offence under this bill for which no penalty is expressly provided shall, on conviction, be liable to a fine not exceeding seventy two currency points or to imprisonment for a term not exceeding three years or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two currency points for each day the offence continues to be committed.

(2) For the purposes of this section, "this Act" does not include the regulations made under this Act.

**92. Institution and conduct of prosecution.**

(1) No prosecution for or in relation to any offence under this Act shall be instituted without the written consent of the Director of Public Prosecutions.

(2) Any officer of the Controller duly authorised in writing by the Director of Public Prosecutions may conduct the prosecution for any offence under this Act.

**93. Jurisdiction to try offences.**

Notwithstanding any written law to the contrary, Magistrate a Grade 1 shall have jurisdiction to try any offence under this Act and to impose the full punishment for any such offence.

**94. Protection of officers.**

No action or prosecution shall be brought, instituted or maintained in any court against -

(a) the Controller or any officer duly authorised under this Act for or on account of or in respect of any act ordered or done for the purpose of carrying into effect this Act; and

(b) any other person for or on account of or in respect of any act done or purported to be done by him under the order, direction or instruction of the Controller or any officer duly

authorised under this Act if the act was done in good faith and in a reasonable belief that it was necessary for the purpose intended to be served thereby.

**95. Limitation on disclaiming or limiting application of Act.**

Unless it is expressly provided for under this Act, A Person shall not disclaim or contractually limit the application of this Act.

**96. Regulations**.

(1) The Controller may make regulations for all or any of the following purposes:

(a) prescribing the qualification requirements for Certification Authorities;
(b) prescribing the manner of applying for licences and certificates under this Act the particulars to be supplied by an applicant, the manner of licensing and certification, the fees payable there for, the conditions or restrictions to be imposed and the form of licences and certificates;
(c) regulating the operations of licensed certification authorities;
(d) prescribing the requirements for the content, form and sources of information in certification authority disclosure records, the updating and timeliness of such information and other practices and policies relating to certification authority disclosure records;
(e) prescribing the form of certification practice statements;
(f) prescribing the qualification requirements for auditors and the procedure for audits;
(g) prescribing the requirements for repositories and the procedure for recognition of repositories;
(h) prescribing the requirements for date/time stamp services and the procedure for recognition of date/time stamp services;
(i) prescribing the procedure for the review of software for use in creating digital signatures and of the applicable standards in relation to digital signatures and certification practice and for the publication of reports on such software and standards;
(j) prescribing the forms for the purposes of this Act;
(k) prescribing the fees and charges payable under this Act and the manner for collecting and disbursing such fees and charges;
(l) providing for such other matters as are contemplated by, or necessary for giving full effect to, the provisions of this Act and for their due administration.

(2) Regulations made under subsection (1) may prescribe any act in contravention of the regulations to be an offence and may prescribe penalties of a fine not exceeding twenty four currency points or imprisonment for a term not exceeding one year or both.

**97. Savings and transitional.**

(1) A certification authority that has been carrying on or operating as a certification authority before the commencement of this Act shall, not later than three months from such commencement, obtain a licence under this Act.

(2) Where a certification authority referred to in subsection (1) fails to obtain a licence after the period prescribed in subsection (1), it shall be deemed to be an unlicensed certification authority and the provisions of this Act shall apply to it and the certificates issued by it accordingly.

(3) Where a Certification Authority referred to in subsection (1) has obtained a licence in accordance with this Act within the period prescribed in subsection (1), all certificates issued by such Certification Authority before the commencement of this Act, to the extent that they are not inconsistent with this Act, shall be deemed to have been issued under this Act and shall have effect accordingly.

## ANNEX 3

## THE ELECTRONIC TRANSACTIONS BILL, 2004

### Arrangement of Clauses.

PART I - PRELIMINARY.

**Clause**

# THE ELECTRONIC TRANSACTIONS BILL, 2004

## A BILL for an Act

## ENTITLED

## THE ELECTRONIC TRANSACTIONS ACT, 2004.

**An Act to provide for the use, security, facilitation and regulation of electronic communications and transactions; and to encourage the use of e-government services and to provide for matters connected therewith.**

## PART 1 - PRELIMINARY

### 1. Interpretation.

In this Act, unless the context otherwise requires-

"addressee", in respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment;

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"data" means electronic representations of information in any form;

"data message" for purposes of this Act, means data generated, sent, received or stored by electronic means and includes-

(a) Voice, where the voice is used in an automated transaction; and

(b) a stored record;

"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

"e-government services" means any public service provided by electronic means by any public body in Uganda;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of data messages;

"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.
"information" includes data, text, images, sound, codes, computer programs, software, databases and the like.
"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;
"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;
"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;
"Minister" means the Minister responsible for Communications;
"originator" means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;
"person" includes a public body;
"public body" includes the Government, any department, services or undertaking of the Government, Cabinet , Parliament, any 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;
"third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;
"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;

**2. Application.**

(1) This Act does not apply to:
- (a) wills and their codicils;
- (b) trusts created by wills or by codicils to wills;
- (c) powers of attorney;
- (d) documents that create or transfer interests in property and require registration to be effective against third parties; and
- (e) negotiable instruments, including negotiable documents of title.

(2) Nothing in this Act limits the operation of any provision of any law that expressly authorises, prohibits or regulates the use of electronic documents.

(3) This Act shall be construed consistently with what is commercially reasonable under the circumstances

as to achieve business sense.

(4) The Minister may, by statutory instrument, amend subsection (2).

## PART II-FACILITATING ELECTRONIC TRANSACTIONS.

### 4. Legal requirements for data messages.

(1) For the avoidance of doubt, it is declared that Information shall not be denied legal effect, validity or enforcement solely on the ground that it is wholly or partly in the form of a data message.

(2) Information incorporated into a contract and that is not in the public domain is regarded as having been incorporated into a data message if such information is-

(a) Referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and

(b) Accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

(3) The following requirements imposed under the law, can be met in electronic form:

(a) a requirement for an act to be in writing;
(b) a requirement for a signature;
(c) a requirement to produce a document;
(d) a requirement to record information; and
(e) a requirement to retain a document.

### 5. Writing.

A requirement in law that a document or information must be in writing is met if the document or information is-

(a) In the form of a data message; and
(b) Accessible in a manner usable for subsequent reference.

### 6. Signature.

Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, that requirement in relation to a data message is met if an electronic signature is used.

### 7. Original.

(1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-

(a) The integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) That information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity shall be assessed-

(a) By considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) In the light of the purpose for which the information was generated; and

(c) Having regard to all other relevant circumstances.

(1) (a) This section does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

(b) A court may have regard to evidence adduced under this section in applying any common law or statutory rule relating to the admissibility of records.

(2) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(3) The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(4) In any legal proceeding, Subject to Subsection (3), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(5) In assessing the evidential weight of a data message or electronic record, regard shall be had to-

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

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(6) In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding;

(a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(7) For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in any legal proceeding in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, having regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

**9. Retention.**

(1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; and

(d) the consent of the department or ministry of the Government, organ of State or the statutory corporation, which has supervision over the requirement for the retention of such records, has been obtained.

(2) An obligation to retain documents, records or information in accordance with subsection (1)(c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.

(4) Nothing in this section shall –

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records.

(b) preclude any department or ministry of the Government, organ of State or a statutory corporation from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department or ministry of the Government, organ of State or statutory corporation.

**10. Production of document or information.**

(1) Where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if-

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for-

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display.

**11. Notarisation, acknowledgement and certification.**

(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced or secure electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a printout certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced

electronic signature.

**12. Other requirements.**

(1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if- the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to a service provider authorised by the relevant regulatory authority, is registered by the said service provider and sent by that service provider to the electronic address provided by the sender.

**13. Automated transactions.**

In an automated transaction-

(a) a contract may be formed where an electronic agent performs an action required by law for agreement formation;

(b) a contract may be formed where all parties to a transaction or either one of them uses an electronic agent:

(c) a party using an electronic agent to form a contract shall subject to paragraph (d), be presumed to be bound by the terms of that contract irrespective of whether that person reviewed the actions of the electronic agent or the terms of the contract;

(d) a party interacting with an electronic agent to form a contract is not bound by the terms of the contract unless those terms were capable of being reviewed by a natural person representing that party prior to contract formation.

(e) no contract is formed where a natural person interacts directly with the electronic agent of- another person and has made a material error during the creation of a data message and-

(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;

(ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;

(f) that person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(g) that person has not used or received any material benefit or value from any performance received from the other person.

**14. Variation by agreement between parties.**

As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, any provisions contained in sections 15,16, 17,18 and 19 may be varied by agreement.

**15. Formation and validity of agreements.**

(1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

(2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror.

**16. Time and place of communications, dispatch and receipt.**

**Time of dispatch.**

(1) Unless otherwise agreed to between the originator and the addressee of a data message, if a data message enters a single information system outside the control of the originator or the person who sent the message on behalf of the originator, the dispatch of the data message occurs when it enters that information system.

(2) If a data message enters successively two or more information systems outside the control of the originator, then unless otherwise agreed between the originator and the addressee of the data message, the dispatch of the data message occurs when it enters the first of those information systems.

**Time of receipt.**

(3) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows;

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs-

(b) at the time when the data message enters the designated information system; or

(c) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is received by the addressee; or

(d) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(4) Subsection (3) shall apply notwithstanding the place where the information system is located may be different from the place where the data message is deemed to be received under subsection (5).

**Place of dispatch and receipt.**

(5) Unless otherwise agreed between the originator and addressee, a data message is deemed to be dispatched at the place where the originator has it's place of business, and is deemed to be received at the place where the addressee has it's place of business.

(6) For purposes of application of subsection (5) to a data message;

(a) if the originator or addressee has more than one place of business, and one of those places has a closer relation to the underlying transaction-it is to be assumed that the place of business is the originator's or addressee's only place of business; and

(b) if the originator or addressee has more than one place of business, but paragraph (a) doesn't apply – it is to be assumed that the originator's or addressee's principal place of business is the originator's or addressee's only place of business; and

(c) if the originator or addressee doesn't have a place of business-it is to be assumed the originator's or addressee's place of business is the place where the originator or addressee ordinarily resides.

(7) This section shall not apply in such circumstances as the minister may by regulations prescribe.

**17. Expression of intent or other statement.**

As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that-

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred.

**18. Attribution of data messages to originator.**

(1) A data message is that of the originator if it was sent by-

(a) the originator personally;

(b) a person who had authority to act on behalf of the originator in respect of that data message; or

(c) an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

(2) As between the originator and addressee, an addressee is entitled to regard a data message as being that of the originator and to act on that assumption if-

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person gain access to a method used by the originator to identify electronic records as it's own.

(3) Subsection (2) shall not apply-

(a) from the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly;

(b) in a case within subsection (2)(b), at anytime when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator ;or

(c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the data message as that of the originator or to act on that assumption.

(4) Nothing in this section shall affect the law of agency or the law on formation of contracts.

**19. Acknowledgement of receipt of data message.**

(1) An acknowledgement of receipt of a data message is not necessary to give legal effect to that message.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by-

(a) any communication by the addressee, automated or otherwise;

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it had never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of acknowledgement,

agreed or, if no time has been specified or agreed within a reasonable time, the originator-

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a) above, may, upon notice to the addressee, treat the data message as though it has never been sent or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed, unless evidence to the contrary is adduced, that the addressee received the related data message, but that the presumption does not imply that the content of the electronic record corresponds to the content of the record received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(7) Except in so far as it relates to sending or receipt of the data message, this section is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

## PART III- E-GOVERNMENT SERVICES.

### 20. Acceptance of electronic filing and issuing of documents.

Any public body that, pursuant to any law-

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for a manner of payment, may, notwithstanding anything to the contrary in such law-

(i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;

(ii) issue such permit, licence or approval in the form of a data message; or

(iii) make or receive payment in electronic form or by electronic means.

### 21. Requirements may be specified.

(1) In any case where a public body performs any of the functions referred to in section 21, such body may specify by notice in the Gazette-

(a) the manner and format in which the data messages must be filed, created, retained or issued;

(b) in cases where the data message has to be signed, the type of electronic signature required;

(c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;

(d) the identity of or criteria that shall be met by any authentication service provider used by the person filing the data message or that such authentication service provider shall be a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

(2) For the purposes of subsection (1)(d) a relevant generic service provider shall be a preferred

authentication service provider.

## PART IV – CONSUMER PROTECTION.

**22. Scope of application.**

(1) This part applies only to electronic transactions.

(2) This part does not apply to a regulatory authority established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions.

**23. Information to be provided.**

(1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered:

(a) its full name and legal status;
(b) its physical address and telephone number;
(c) its web site address and e-mail address;
(d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;
(e) any code of conduct to which that supplier subscribes and how the consumer may access that code of conduct electronically;
(f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;
(g) the physical address where that supplier will receive legal service of documents;
(h) a sufficient description of the main characteristics of the goods or services offered by that supplier 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 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 can access and maintain a full record of the transaction;
(n) the return, exchange and refund policy of that supplier;
(o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;
(p) the security procedures and privacy policy of that supplier 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 supply of products or services to be performed on an ongoing basis or recurrently;

(2) The supplier shall provide a consumer with an opportunity-

(a) to review the entire electronic transaction;
(b) to correct any mistakes; and
(c) to withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the

transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3)-
- (a) the consumer shall return the performance of the supplier or, where applicable, cease using the services performed; and
- (b) the supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

(5) The supplier shall utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

(7) This section does not apply to an electronic transaction-
- (a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
- (b) by way of an auction;
- (c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption 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 23(1);
- (e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;
- (f) where the goods
  - (i) are made to the consumer's specifications;
  - (ii) are clearly personalised;
  - (iii) by reason of their nature cannot be returned; or
    - (a) are likely to deteriorate or expire rapidly;
    - (b) where audio or video recordings or computer software were unsealed by the consumer;
    - (c) for the sale of newspapers, periodicals, magazines and books;
    - (d) for the provision of gaming and lottery services; or
    - (e) 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.

**24. Cooling-off period.**

(1) Subject to sub section (2) hereof, a consumer may cancel an electronic transaction and any related credit agreement for the supply-
- (a) of goods within seven days after the date of the receipt of the goods; or
- (b) of services within seven days after the date of the conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (I), the consumer is entitled to a full refund of' such payment, which refund shall be made within 30 days of the date of cancellation.

(4) This section shall not be construed as prejudicing the rights of a consumer provided for in any other law.

**25. Unsolicited goods, services or communications.**

(1) A person who sends unsolicited commercial communications to consumers, shall provide the consumer-
(a) with the option to cancel his or her subscription to the mailing list of that person; and

(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) A person who fails to comply with or contravenes sub-section (1) commits an offence and shall be liable, on conviction to a fine not exceeding seventy two currency points or to imprisonment for a term not exceeding three years or both.

(3) A person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, commits an offence and liable, on conviction, to the to a fine not exceeding seventy two currency points or to imprisonment for a term not exceeding three years or both.

**26. Performance**.

(1) The supplier shall execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise.

(2) Where a supplier has failed to execute the order within 30 days or within the agreed period, the consumer may cancel the agreement with seven days' written notice.

(3) If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

**27. Applicability of foreign law.**

The protection provided to consumers in this part, applies irrespective of the legal system applicable to the agreement in question.

**28. Non-exclusion.**

Any provision in an agreement, which excludes any rights provided for in this part, is null and void.

PART V- LIMITATION OF LIABLITY OF SERVICE PROVIDERS.

**29. Liability of service providers.**

(1) A service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on –

(a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or

(b) the infringement of any rights subsisting in or in relation to such material.

(2) Nothing in this section shall affect –

(a) any obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law; or

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) For the purposes of this section -

"Provides access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-

**30. Information location tools.**

A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer or hyperlink, where the service provider-

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

**31. Notification of unlawful activity.**

(1) For the purposes of this Part, a notification of unlawful activity by the complainant shall be in writing and addressed to the service provider or its designated agent and shall include-

(a) the full names and address of the complainant;
(b) the written or electronic signature of the complainant;
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the service provider in respect of the complaint;
(f) telephonic and electronic contact details, if any, of the complainant;
(g) a statement that the complainant is acting in good faith; and
(h) a statement by the complainant that the information in the notification is to his or her knowledge true and correct.

(2) A person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable to the service provider for the loss and or damage occasioned.

**32. No general obligation to monitor.**

(1) When providing the services contemplated in this Part there is no general obligation on a service provider to-

(a) monitor the data which it transmits or stores; or
(b) actively seek for facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to article 41 of the Constitution, prescribe procedures for service providers to-

(a) inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service; and
(b) communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

**33. Regulations.**

The Minister may make regulations regarding any matter that may be prescribed in terms of this Act or any matter, which it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

## SCHEDULE

One currency point is equivalent to twenty thousand shillings.

# ANNEX 4

## PUBLICATIONS OF THE UGANDA LAW REFORM COMMISSION

| No. | Publication. |
|---|---|
| 1. | A study report on rape, refilement and other sexual offences. |
| 2. | A study report on the reform of the raw of domestic relations. |
| 3. | The sixth revised edition of the laws of Uganda, 2000. |
| 4. | A field study report on voices of the people on trial procedures, sentencing and decriminalisation of petty offences. |
| 5. | A study report on company law. |
| 6. | A study report on competition law. |
| 7. | A study report on contracts law. |
| 8. | A study report on cooperatives law. |
| 9. | A study report on copyright and neighbouring rights law. |
| 10. | A study report on electronic transactions law. |
| 11. | A study report on geographical indications law. |
| 12. | A study report on industrial property law (patents, industrial designs technovations and utility models) |
| 13. | A study report on insolvency law. |
| 14. | A study report on intellectual property - traditional medicine practice. |
| 15. | A study report on intellectual property rights - trademarks and service marks law. |
| 16. | A study report on intellectual property rights -trade secrets law. |
| 17. | A study report on law relating to trial procedure law. |
| 18. | A study report on plant variety protection law. |
| 19. | A study report on quadhi's courts law. |
| 20. | A study report on reform of the laws relating to chattel securities. |
| 21. | A study report on reform of the laws relating to hire purchase. |
| 22. | A study report on reform of the laws relating to mortgage transactions. |
| 23. | A study report on sentencing guidelines. |
| 24. | A study report on the law for establishment of special economic zones. |
| 25. | A study report on the proposals for the reform of the Accountants Act, Cap 266. |
| 26. | A study report on the reform of rusiness associations -partnerships law |
| 27. | A study report on the reform of selected trade laws - consumerprotection law. |
| 28. | A study report on the reform of selected trade laws - sale of goods and services law. |
| 29. | A study report on the reform of selected trade laws - trade licensing law. |
| 30. | Handbook on making ordinances and bye-laws in Uganda. |
| 31. | How our laws are made. |
| 32. | Study report on the implementation of the World Trade Organisation Agreements. |
| 33. | Report on the law relating to publishing horrific pictures and pictures of the dead in the press and pornography. |