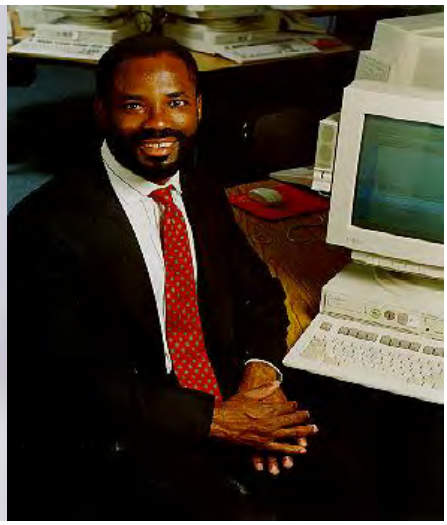
Maitlamo

Botswana's National ICT Policy





LEGISLATIVE FRAMEWORK & CHANGE REPORT

Final Report
December 2004

Maitlamo

TABLE OF CONTENTS

LEGISLATIVE FRAMEWORK AND CHANGE REPORT

LEGISLATIVE FRAMEWORK FOR MAITLAMO

1.0 Background

1.1 The Government of Botswana has committed to developing a National Information and Communications Technology (ICT) Policy that will build upon recent government initiatives and assist in achieving Vision 2016. In keeping with Vision 2016, it is envisioned that the National ICT Policy will position Botswana for sustained growth in the digital age by serving as a key catalyst in achieving social, economic, political and cultural transformation within the country.

1.2 The Government realises that in order to have an effective Policy, a legislative framework must be put in place to identify and support the initiatives to be undertaken. This report serves to review the existing legislative framework in Botswana in regard to ICT and identify key areas that will need addressed or amended in order for the Policy to be implemented effectively.

2.0 Main Findings of Benchmarking and Best Practices Study

2.1 The objectives of the ICT Benchmarking and Best Practices Report, produced during the development of the National ICT Policy, were to identify Botswana's relative level of ICT development and to present examples of ICT usage that are producing positive effects in other parts of the world. The Report, completed in May 2004, was intended to give the reader a better understanding of Botswana's place in the electronic world, its strengths and weaknesses as a connected country, and the methods that may be adopted in order to promote greater ICT usage. Benchmarking, which is a continuous process of measuring organisational performance against relevant and common comparators, allows for the design of initiatives that are tailored to Botswana's specific needs and focuses effort on the areas that need it most. It further identifies a starting point against which progress can be measured.

2.2 The Botswana Benchmarking and Best Practices Report examined seven key areas that collectively represent a nation's connectivity environment. These areas include:

- ICTs in Homes and Communities
- ICTs in Healthcare
- ICTs in Learning
- ICTs in the Marketplace and ICT Sector
- ICTs in Government
- ICT-enabling Infrastructure

- ICT-enabling Legislation

2.3 Seven countries were selected as relevant ICT benchmarks for Botswana: Estonia (similar population and GDP); Malaysia (middle-income export-based economy dominated by ICT growth); Mauritius (shift from agricultural to diversified economy); Namibia (heavily dependent on mineral exports); South Africa (closely linked to the Botswana economy); Trinidad and Tobago (large mineral exports and strong destination for ICT investment); and Canada (shift from rural to highly skilled labour base and economy resembling that of the United States).

2.4 A variety of common and respected international data sources were used, such as the United Nations, the World Bank and the World Economic Forum. Common data for each country were charted and compared against one another. The data was analysed for insights, correlations or implied causation. The results reveal each country's level of ICT development in each category relative to the selected comparator countries.

The ICT Benchmarking and Best Practices Report found that Botswana is a country where information and communication technology has yet to provide society-wide benefits. A national ICT programme for Botswana must address the following observations:

- ICT usage in homes and communities has been sporadic to date. Whether this is due to other social and economic challenges facing the government is not clear. Various other countries around the world, however, have proved that development can be a product of investment in ICT and not a prerequisite to investment.

- The state of health care in Botswana is dominated by the AIDS/HIV crisis. Technology alone cannot solve this problem. Improved communications associated with a national ICT programme can nonetheless provide an opportunity to extend the reach of AIDS/HIV awareness and allow citizens to readily find assistance and information.

- Public education is a high priority in Botswana, based on spending levels. The country, however, is still significantly constrained by low levels of literacy and enrolment in tertiary education. Basic education is a prerequisite to participate fully in the information economy. At present, too many people lack these basic and necessary skills.

- A survey of the ICT market was finalised in November 2004 to support the National e-Readiness Assessment completed in July 2004. The

survey indicated that annual ICT expenditure in Botswana might be approaching 1Billion Pula. This is very encouraging and demonstrates the significant domestic demand for ICT products and services – however, much of this revenue goes directly abroad and not to local IT companies. Based on this impressive internal demand for ICT products and services, the survey stressed the urgency for development of more domestic specialised ICT skills such as Oracle and SAP certification, and the need for on-the-job training etc. to ensure that young graduates have a career path in Botswana's emerging ICT sector, and that these significant revenues remain within the country.

- Despite the Botswana Government's commitment to promoting ICT as a priority, e-Government information and services are still at a very early stage. It is imperative that Botswana address the gap between the e-Government messages and the reality that constituents experience every day.

- In some respects, Botswana is performing at or above global averages in terms of ICT infrastructure. For example, waiting time for phones is acceptable. Internet access is reasonably affordable, ranking in the middle tier of countries worldwide.

- In other areas, infrastructure is inadequate. Telecommunications investment is very low and declining. The availability of telephone mainlines is poor. The country has the fewest Internet hosts per capita of any of the eight nations examined.

- Relative to other countries, Botswana boasts a very advanced legal and legislative system that is generally conducive to the proliferation of ICT and ICT-related industries. Botswana's highly developed legal system is an asset that can be used to assist with the orderly transition to an information-based economy.

2.5 The Best Practices Conclusions showed that countries in all parts of the world have introduced innovative ICT applications that can significantly contribute to social, economic and cultural development. There are many examples of ICT programmes, projects and applications that Botswana can examine to provide learning and guidance to the Maitlamo initiative. If these Best Practices are studied closely, adapted to meet Botswana's needs, and implemented wisely, Botswana can not only make rapid progress in terms of ICT diffusion, but also may leapfrog over many countries that began their ICT initiatives years ahead of the Maitlamo programme.

3.0 Main Findings of e-Readiness Study

3.1 The Benchmarking and Best Practices Study examined how Botswana compares in connectivity and ICT applications to seven other countries using common and internationally accepted comparators. The e-Readiness Study was undertaken to provide a more detailed "snapshot" of Botswana today. Rather than looking to see how Botswana compares to other selected countries (as in the Benchmarking exercise), the e-Readiness assessment examined the degree to which Botswana is prepared to participate in the Networked World. It is gauged by assessing the relative advancement in areas most critical for ICT adoption and the most important applications of ICT. The assessment looks at Access, Learning, Health, Society, Economy, and Legislation and Policy. The questions that were developed under these headings were answered through working with the various Task Forces, who in turn consulted with knowledgeable government officials and members of the private sector.

3.2 The e-Readiness Assessment completed in June 2004, showed that Botswana's level of e-readiness was a contrast of extremes. The World Economic Forum (WEF) Global IT Report 2003-2004 currently ranks Botswana 55th in the world in terms of overall national connectivity, demonstrating that the country is already an active participant in the global information society. The country has invested heavily in infrastructure and telecommunications and has a high penetration of fibre connectivity running to the urban areas. It has a sophisticated Government Data Network (GDN) and Police Private Network delivering connectivity to all government departments and agencies via high-speed Internet and satellite links. Mobile telephone usage continues to soar. In March 2004, a BTA study indicated that 31% of the population (556,000) are using mobile phones.

3.3 Botswana has the distinct advantage of a world-renowned legal system, acknowledged for the integrity of its legal practices and its respect for the Rule of Law. It has a modern Telecommunications Act and a well-established regime of legal institutions. Many of the essentials for accelerating Botswana into the digital economy appear to be in place; however, there are also a number of major constraints that add substantial complexities and challenges.

3.4 In Botswana today, there is considerable disparity between rural and urban access to information and services – a "domestic information divide." The majority of urban centres are relatively well supplied with radio, television, telephone and Internet access. The picture is significantly different in remote and rural areas, where even access to

basic information such as radio, telephones and newspapers is problematic. According to 2001 CSO Census data, and further supported by the e-Readiness community visits, approximately 37 percent of Botswana households use electricity for lighting. Census data also shows that this number further falls, to only 8 percent, in rural and remote settlements. The 2001 Census and the 2004 World Economic Forum Global IT Report both indicate computer ownership and Internet usage levels to be low (between 3-5 percent). This is thought to be primarily due to prohibitive cost and limited access. This disparity in access to information or "connectivity" is of great concern to a large percentage of the population. Many remote communities feel marginalised and not part of mainstream Botswana. The majority of Batswana are aware of the benefits arising from technology and the Internet. However, in most cases, especially in rural areas, basic needs such as electricity, roads and access to healthcare are much more pressing. Rural telephone and electrification programmes are continuing, but not at a pace that is adequate to satisfy demand, let alone the aggressive requirements of the Maitlamo project.

3.5 While technical infrastructure and Internet access are important parts of the ICT puzzle, the most important piece is human capital and a workforce that is capable of maximising the benefits of the ICT infrastructure for social, economic and cultural benefits. Botswana will need to focus many of its ICT efforts, and budget, on learning and the development of technologically literate children if it is to create a vibrant future in the networked world. It is widely accepted that education and skills development lie at the centre of any sustained ICT solution. The 2001 Census survey reported that approximately 67 percent of residents in rural areas attended school, compared with 79 percent in urban villages and 89 percent in cities and towns. These numbers will need to be continually strengthened if Botswana is to maximise ICT benefits for all of its citizens, and avoid regional disparities. Similarly, with the 2004 World Economic Forum Global IT Report suggesting that only 5 percent of the population are entering tertiary levels of education, Botswana must identify and develop programmes to ensure that far greater numbers of the population improve their overall level of education. More students must move into university and excel in fields such as Computer Science, Engineering, Physics, Mathematics, and Business Studies if the country is to achieve its long-term development goals. In the medium-term, it will be necessary for Botswana to attract top-class external specialists and have local professionals work alongside them to acquire new skills.

3.6 Botswana must look at introducing ICT into the formal education system as soon as possible, both as a subject and as an educational tool.

Countries that do well at ICT-driven innovation tend to introduce ICT education as early as kindergarten. There is no ICT education - or computers - in the vast majority of primary schools in Botswana and only limited numbers of computers at the junior and secondary levels. Where there are computers, the student to computer ratio is too high to have any significant benefit. Teachers will have to be trained, and school access to electricity remains a critical challenge that must be addressed as a matter of priority.

3.7 Improving access to healthcare information and services through the effective use of ICT is particularly important in Botswana. Overall, there is a high degree of awareness of the importance of e-Health and there are a few initiatives underway. Lack of integration is a key issue and close coordination between the public and private health systems is essential. One of the concerns identified during community visits was the lack of availability to basic healthcare information, particularly in relation to HIV/AIDS. This information could be incorporated into an e-Government portal. ICT training for health professionals, including administrative and support staff, will be particularly important as ICT offers considerable benefits in terms of healthcare management and administration.

3.8 The November 2004 ICT Sector Survey suggests that Botswana's government and private sector generate approximately 1Billion Pula in annual IT sales. This is impressive and highlights the fact that organisations see great value in ICT. However, there is still significant potential for Botswana's private sector to make better use of ICT as a productivity and efficiency tool. Some of the traditional and more sophisticated sectors, such as mining and financial services, make greater use of ICTs and electronic business transactions than the smaller industries, however, as frequently voiced throughout the e-Readiness and policy development process, there is often a complaint that telecommunications service quality is inadequate and a barrier to additional business opportunities. Currently there are insufficient opportunities in the private sector for IT professionals, and as a result many graduates struggle to find employment and gradually move into other fields. Generally, the marketplace is some way from the National ICT goals of developing a globally competitive ICT sector. Achieving this will require substantial financial investment, significant upgrades in infrastructure, changes in legislation and a development of a suitably trained workforce.

3.9 Government has an important role to play in stimulating ICT take-up in all elements of society. It has a modern technical infrastructure that is capable of providing valuable information and services to citizens and

businesses in all parts of the country. Current initiatives must be coordinated and tightly managed and integrated if maximum service and cost benefits are to be achieved. Botswana needs to develop a formal e-Government strategy as a matter of priority. Websites being introduced by Ministries are not designed around the needs of clients and have no common standards or "look and feel". Without an overarching e-Government strategy (designed in the context of a broader public sector reform programme), there is a danger of creating "cyber stovepipes", wasting money, increasing costs and missing opportunities for service improvements through Electronic Service Delivery. Many communities would benefit significantly from on-line access to basic government information and services. Information on health, jobs and education can be provided easily and have significant impact. Similarly, simple on-line transactions, such as licence, registration and permit applications, would improve customer service standards and reduce costs for citizens and government.

3.10 Public policy can be a help or hindrance in the development of a mature networked economy. The favourable climate that can be encouraged by an appropriate legislative and regulatory regime encourages communities, organisations and individuals to invest in and use ICTs. Important areas, such as Internet availability, the use of ICTs in schools and health facilities, and the growth of e-commerce are all influenced by public policy and the legal framework developed in Botswana. To fully implement the programmes that will be needed to fulfil the goals of Maitlamo and Vision 2016, it will be necessary for Botswana to have in place an evolving, responsive legal and policy infrastructure that is just as important as the physical infrastructure in supporting investment and economic development.

4.0 Legislative Gap Analysis: The Legal Framework Needed to Foster an ICT Strategy

4.1 In general, countries wishing to participate actively in the modern connected world must have in place policies, rules or legislation dealing with a number of areas. Legal certainty must be assured for electronic commercial transactions that can be enforced. Electronic documents and signatures must be capable of being authenticated. Citizens must be able to trust the electronic environment because issues of transactional security, privacy and data integrity have been addressed. The potential for fraud, obfuscation, cross-border and domestic transmission of objectionable content, as well as new criminal behaviour (e.g., the introduction of viruses into a network or intentional and

malicious manipulation of data) must be addressed. In an inter-connected world, co-operative enforcement arrangements must be established, as well as new expertise in the investigation and prosecution of computer-related crimes.

4.2 The exact mix of legislation, self-regulation, voluntary or mandatory industry codes of conduct, market-based incentives and other approaches will depend on both the issue and the priorities of citizens the Government of Botswana. It is imperative, however, that the resulting policy regime address the needs of Government, businesses, foreign investors and individual citizens in their various roles as consumers, students, health providers, clients, educators and so on.

4.3 The importance of the legal framework to successful implementation of an ICT Policy means that existing legal traditions and credibility will play an important role in determining the ability of a country to respond to gaps in its e-Readiness framework. Botswana is fortunate in having a solid and credible legal structure. An analysis of the gaps in legislation and policy required to implement the ICT policy show that there is a mix of relatively advanced legislation and policy existing alongside areas where new policies and legislation must be developed to fill the gaps.

4.4 A number of legislative and legal policy gaps were identified in the Analysis. It should be noted, however, that in some cases policy work is underway to deal with issues that were identified, e.g., the lack of an independent Competition Authority and legislation dealing specifically with competition and abuse of dominant position. Among the gaps or issues that must be addressed through more intensive policy work are:

- Adequacy of the Botswana Telecommunications Authority's powers to deal with anti-competitive conduct;

- Additional liberalisation of the telecommunications regime, including dealing with the potential privatisation of the Botswana Telecommunications Corporation; establishing a regulatory regime to deal with a mix of competitive and monopoly activities (e.g., developing costing methodologies); more vigorous promotion of Universal Service (e.g., establishing a Universal Service Fund or defining contribution methodologies); dealing with convergence; establishing a transparent system (including alternative methods) of allocating

spectrum; and reviewing the policy of banning the use of Voice Over IP;

- Lack of specific legislation and an independent organisation to deal with competition issues; rationalisation of powers and authority of proposed Competition Authority with powers and authority of the Botswana Telecommunications Authority to deal with anti-competitive conduct in the telecommunications industry;

- Lack of comprehensive legislation to deal with data crimes, such as interception, modifications of data, data theft or trafficking in digital signatures or domain names. Current legislation dealing with pornography or undesirable content may not be adequate to cover such matters as "exporting" child pornography through the Internet. "Lawful access" provisions dealing with how law enforcement and security authorities deal with access to information in the course of investigations may be required to provide assurances of a fair process that international investors and users would expect;

- Lack of legislation to deal with e-commerce by providing the same protective legal infrastructure that exists for paper-based transactions. Electronic signatures are an integral part of an authentication scheme and legislation dealing with electronic signatures, as well as the institutional capacity to deal with the recognition and approval of Certificate Authorities, will be required;

- The Botswana *Consumer Protection Act* does not explicitly deal with electronic commerce. As well, there are no programmes or policies in place to educate consumers about e-commerce or increase business and consumer awareness of a consumer protection framework for on-line activities. An additional element is the capacity to co-ordinate enforcement and investigation activities with other jurisdictions dealing with cross-border frauds or other illegal transactions;

- Lack of comprehensive legislation to deal with the protection of personal privacy and personal data. In particular, a legal regime that will satisfy the requirements of the European Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* will be required if Botswana is to become a financial services centre or other base where data is imported in the course of doing business.

- Lack of comprehensive legislation to deal with access to government information by citizens, which is the other side of the right to privacy. Among the major objectives identified for the Botswana ICT

Strategy are improving communication, empowering citizens, and encouraging democratic participation. Citizens in community visits conducted by the Maitlamo Project Team expressed a desire to learn more about government.

- The *Copyright and Neighbouring Rights Act* recognises intellectual property rights in computer software, electronic documents and other forms of data. Concerns were expressed, however, about the adequacy of remedies and enforcement. There is also no legislative protection against cyber-squatting on a website and no dispute resolution system in place to deal with domain name protection. There is also no appropriate legislated limitation on the liability of Internet Service Providers.

- Transparency of the legal system and legal decision-making can be improved by making more information, including the legislation of Botswana and judicial and administrative decisions, available on the Internet. These elements of transparency are related to e-Government. As well, there is considerable scope for the adoption of ICT technologies in the legal system, including case management of the courts and training of legal and judicial officials in the use of new information technologies.

4.5 The Legal and Policy e-Readiness Report and Gap Analysis identified four immediate priorities for legislative and legal policy development. These priorities were developed taking into account reports of other Task Forces and took into consideration that the Legal and Policy Task Force had been charged with identifying changes that are required to enable the development of an ICT Strategy for Botswana. In addition to the policy development that is underway regarding telecommunications liberalisation (which may include spectrum allocation and convergence—information was not available to confirm this) and competition policy, the short-term priorities are:

- Media-neutral legislation to deal with electronic documents (e-commerce legislation).

- Amendments to specific legislation including the *Criminal Procedure and Evidence Act*, the *Authentication of Documents Act*, the *Foreign Documents Evidence Act* and possibly selected other legislation (e.g., the *Botswana Stock Exchange Act*) to allow for the use and enforcement of electronic documents.

- Development of a policy and possibly legislation to deal with electronic signatures.

- Development of a policy and possibly a combination of legislation and industry codes of conduct to deal with the protection of personal privacy, particularly in the context of cross-border data flow, health care, and financial services.

4.6 Other legal issues will require examination in the medium to longer term. For example, a review of the *Penal Code* and other regulatory legislation will determine whether Botswana is prepared to deal with new cyber-crimes. Tax policies and mutual taxation agreements may require review and negotiation to ensure that Botswana receives its fair share of taxation revenues from e-commerce. The desire to have more access to Government information that was expressed in community visits indicates that access to information legislation should be explored to provide a framework for access (and its flip-side, protection of personal and commercial privacy) for citizens.

4.7 More information about proposed future action can be found in the Action Plans developed for the recommendations of the Legal and Policy Task Force, as well as for the other Task Forces.

5.0 Proposals

5.1 The study on Legal e-Readiness and the Legal Gap Analysis indicate that a number of legislative and policy changes will be required to provide the legal and policy infrastructure needed to support Maitlamo. The responsibility for these changes is shared among a number of Ministries and several Parastatal organisations. Co-ordination and priority setting across Government will be required to achieve the necessary results within an acceptable time period.

5.2 Given the number of issues that must be resolved, the various interests and parties that must be consulted, and the co-ordination that must be achieved, it is critical that both political and administrative will at the highest levels of all relevant Government Ministries, Local Authorities and Parastatal Organisations be harnessed to drive the legislative and legal policy initiatives of Maitlamo. It is also critical that a mechanism be created to co-ordinate these initiatives and to ensure that accountability is maintained for the delivery of these inter-related, yet separate, initiatives within the target time periods.

5.3 To assure that high level support is provided to these initiatives and to co-ordinate and ensure accountability for the development and delivery of legislative initiatives and programmes, an Inter-ministerial Legal

Reform Taskforce should be established as a co-ordinating body to set priorities and provide oversight of progress in dealing with the legal and policy issues identified further in Annex I and, in particular, the items outlined in the accompanying Action Plan.

5.4 The Inter-ministerial Legal Reform Taskforce, composed of both senior level public officials and influential members of the private sector ("opinion makers"), will report to Cabinet at six-month intervals on the progress being made in legal and legislative policy development.

5.5 The Minister of Communications, Science and Technology will provide the co-ordinating secretariat to the Inter-ministerial Legal Reform Taskforce with respect to those matters.

ANNEX ONE

REPORT OF THE MAITLAMO LEGAL TASK FORCE ADVISOR

1.0 Introduction

1.1 Public policy and legislation can be a help or hindrance in the development of a mature networked economy. The favourable climate that can be created by an appropriate legislative and regulatory regime encourages communities, organisations and individuals to invest in and use Information and Communication Technologies. Important areas, such as Internet availability, the use of ICT in schools and health facilities, and growth of e-commerce, are all influenced by public policy and the legal framework developed by Botswana regarding ICT.

1.2 In general, any country wishing to participate actively in the modern connected world should have in place ICT-related policies, legislation or other rules dealing with a number of areas. Legal certainty must be ensured for electronic commercial transactions, which can be enforced and electronic documents and signatures can be authenticated. Citizens must be able to trust the electronic environment because issues of transactional security, privacy, and data integrity have been addressed. The potential for fraud, obfuscation and cross-border transmission of objectionable content, as well as new criminal behaviour (e.g., the introduction of viruses into the network) must be addressed and co-operative enforcement arrangements established. The exact mix of legislation, self-regulation, voluntary or mandatory industry codes of conduct, market-based incentives and other approaches will depend on both the issue and priorities of the citizens of Botswana, but the resulting policy regime should address the needs of government, businesses and individual citizens in their various roles as consumers, students, health providers, clients, educators and so on.

1.3 This Annex is a report of the Maitlamo Legal Task Force Advisor and addresses a number of issues that the Task Force believed required priority attention. These include: e-commerce legislation; protection of the e-commerce consumer; digital signatures; protection of personal privacy; security of information systems and networks; and cyber-crime and “inappropriate content” and lawful access.

2.0 E-Commerce Legislation

2.1.1 Objective:

- Ensuring that Botswana has legislation and policies that provide for the acceptance of electronic documents in commerce and for personal use, and provide for the enforceability of electronic contracts. In addition, the Government of Botswana should have the legislative mandate and policies necessary to fully implement an e-Government programme.

2.2 Issues:

- The scope of e-legislation: should it cover only commercial relationships or other types of communications as well?
- Should specific legislation be amended to provide for media-neutral language or should an electronic documents bill be enacted that provides overall authority and guidelines? Alternatively, should some combination of the two techniques be used?
- What is the best technique to ensure that Government Ministries and parastatals are positioned to deal with electronic documents and to protect their networks and infrastructure?
- What kinds of documents, if any, should be excluded from provisions allowing for electronic documents? Wills? Domestic contracts? Adoption papers? Sale of land?
- What adjustments should be made, if any, to Botswana contract law to accommodate electronic contracts? For example, does "clicking" or downloading constitute acceptance? What default rules should apply to the timing of an offer and acceptance?
- How should rules of evidence be modified, if at all, to accommodate the functional equivalency of electronic documents to paper-based documents?

2.3 Discussion:

2.3.1 One of the most exciting and far-reaching uses of the Internet and new ICT technology is e-commerce. Consumers now have a world of products available to them and businesses have new opportunities to reach customers, sell products, and develop niche markets. Both consumers and business can thrive through innovation and e-commerce competition. To develop the potential of e-commerce, however, trust must be established through information and mechanisms to protect both parties. Standards, rules and legislation must be established that provide the same protective infrastructure that exists for paper-based consumer transactions. Different countries have met the challenge in different ways, but there are common approaches dealing with provision of

information, enforcement of contracts, and recourse where agreements are not kept.

2.3.2 An important area to be dealt with in developing legislation to create an enabling and nurturing environment for e-commerce is to make both legislation and transactions "media neutral." The world has long had a series of rules and protocols, found in national and international law and custom, to deal with commercial and personal transactions in an oral and paper-based environment. An electronic environment, however, creates some differences that have to be resolved through rules, which may be found in legislation, standards or other forms of rules (e.g., industry codes of conduct). A media neutral legal regime is intended to be neutral with respect to the medium used to communicate, with a few exceptions. E-commerce legislation is intended to remove obstacles and uncertainties about the use of electronic documents and electronic communication.

2.3.3 E-commerce legislation, however, should not force individuals or persons to use electronic documents or communication. It should be viewed as enabling legislation. The objective is to offer greater choice and efficiencies for Batswana and persons doing business in or with Botswana.

2.3.4 Although individuals and even businesses regularly carry out transactions orally, modern business practice has developed in a paper-based society. Existing legislation and business requirements are likely to contain language that reflects the paper-driven environment in which they are created. This language can relate to obligations that govern relationships with government (e.g., filing of taxation documents or the creation of a corporation) or can establish rules that govern the private sector in its business and personal relationships (e.g., buying and selling property or testamentary provisions). Legislative language that suggests a bias toward a paper or non-electronic environment includes

- "in writing" or "written"
- "prescribed form" or "form"
- "notarised"
- "witnessed"
- "signed" or "signature"
- "sworn" or "made under oath"
- "affidavit"
- "sealed" or "stamped"
- "record"
- "certified"
- "authorised"

- language referring to a number of copies to be filed, delivered, registered or record retention requirements
- language referring to "original" documents or "copies."

2.3.5 Generally, governments have taken the route of searching statutes, regulations and other subordinate legislation or rules having the force of law to identify paper-biased language. While it is possible to create piecemeal amendments to legislation to "neutralise" the language, the general approach has been to create a new statute or statutes (e.g., an "E-Commerce Act", an "Electronic Transactions Act" or an "Electronic Documents Act") to create "equivalencies" of language. Thus, the new "Electronic Documents Act" might state something like:

> A legal requirement that a person provide information or a document in writing to another person is satisfied by the provision of the information or document in electronic form that is, (a) accessible by the other person so as to be usable for subsequent reference; and (b) capable of being retained by the other person.[1]

Or

> Where an enactment requires any information or record to be in writing, that requirement shall be satisfied by an electronic record, where the information contained therein is accessible so as to be usable for subsequent reference.[2]

2.3.6 A number of countries have now established legislation to deal with electronic documents and electronic commerce. Most legislation has been based or a greater or lesser degree on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (MLEC) and Model Law on Electronic Signatures.[3] The purpose of the Model Law on Electronic Commerce is to offer national legislators a set of internationally accepted rules on how to remove obstacles to effective e-commerce and create a more stable legal environment for commerce carried out through electronic media.

---

[1] Taken from the Ontario (Canada) *Electronic Commerce Act*, 2000, S.O. 2000, c.17, section 6(1).

[2] Mauritius, *Electronic Transactions Act*, s. 6. ncb.intent.mu/mitt/ ministry/etb/etbp2.htm

[3] www.uncitral.org/english.texts/electcom/ml-ecomm.htm
The UNCITRAL Model Law is being subject to continual discussion and potential revision. For example, the Working Group on Electronic Commerce is in the process of developing a Model Law on Electronic Signatures, discussed in the text below.

2.3.7 Individuals may also use the principles of the Model Law to draft contracts to overcome legal obstacles to the increased use of e-commerce. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level can create barriers to international trade, a significant amount of which is carried out using modern communication techniques. The Model Law is not intended to cover every aspect of electronic commerce, but is likely to be supplemented by procedural regulations. The intention is, however, that each enacting state pay particular attention to the need to maintain a flexible approach in a rapidly changing technological environment.

2.3.8 Two examples of the extension of the principles of the UNCITRAL Model Law into other model legislation can be found in the Uniform Law Conference of Canada: Uniform Electronic Commerce Act[4] and the U.S. Uniform Electronic Transactions Act.[5] The U.S Uniform Act, expanding on the U.S. Uniform Commercial Code, applies to business, commercial or governmental transactions. Signatures and records that are not part of a transaction are not covered by the U.S. Uniform Act.

2.3.9 On the other hand, a number of jurisdictions (e.g., Australia and New Zealand) saw no reason to limit their legislation to commercial transactions. Since the general intent is to be enabling and since generally people are not required to use electronic communications, the policy makers saw no reason why the legislation should not be extended to all transactions.

2.3.10 The basic tenet of the model laws is that a transaction or a contract is not invalid solely by virtue of the fact that it is electronic.[6] Similarly, a signature or record may not be denied legal effect or enforceability solely because it is electronic. The Canadian Uniform Act sets out basic equivalence rules (examples above) and states that they apply when the people involved in a transaction agree, explicitly or implicitly, to use electronic documents. People are not required to use electronic communication, but when they choose to, the legal effectiveness of electronic transactions should not be in doubt. General equivalency rules avoid the need to amend all statutes that state or imply a particular medium of communication.

2.3.11 In some legislation, governments are allowed to set rules for incoming

[4] www.law.ualberta.ca/alri/ulc/current/euecafa.htm
[5] National Conference of Commissioners on Uniform State Laws; www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm
[6] Note that other factors may invalidate, for example, a contract. Thus a contract entered under duress or where there is no agreement on material issues is not a valid contract; this is a matter of contract law and has nothing to do with the electronic or non-electronic form of the contract.

electronic documents to avoid dealing with a variety of formats; private sector parties can set their own rules by contract or other agreements. Under the Canadian federal *Personal Information Protection and Electronic Documents Act*,[7] federal departments and agencies may "opt in" to the e-government initiative and begin using electronic means of doing business when they have the necessary technology in place in order to deal with the issue of whether government departments are technologically equipped to deal with e-government. There is a provision for making regulations using electronic versions of forms and methods of filing or otherwise submitting information to a department or agency. The Canadian province, Ontario, takes a different approach in the *Electronic Commerce Act, 2000*.[8] While no one is required to make or accept an electronic document, consent may be inferred from a person's conduct if there are reasonable grounds to believe that the consent is genuine and is relevant to the government ministries and other public bodies, however, consent must be explicit. Thus, a public body need only do business electronically when it is in a position to do so. In New Zealand, the rules of courts and tribunals will govern whether and to what degree they will accept the use of electronic technology for court purposes (as opposed to accepting electronic documents as evidence in a case). In addition, New Zealand expects government departments to issue guidelines as to when they will or will not accept electronic communications: e-government websites with forms and the availability of e-mail addresses on websites will imply, of course, that electronic communication is welcome.

2.3.12 The Canadian statutes do not apply to wills, powers of attorney for property or personal care, trusts created by will or codicil, deeds and mortgages, and election documents. Part of the rationale for this is that these are documents where there should be only one copy, an original in the traditional sense, and part is that these documents may require the more ceremonial act of a traditional handwritten signature. Most e-commerce laws provide for some exceptions and these are the common ones. In New Zealand, in addition to similar exemptions, certain types of notices must continue to be in writing. Some jurisdictions make exceptions for notices of cessation of service from utility companies, for example.

2.3.13 E-commerce legislation takes a functional approach. For example, legal requirements found in statutes that documents be in writing is considered to be based on the need to ensure that the document be

[7] S.C.2000, chapter 5.
[8] S.O. 2000, chapter 17.

accessible for subsequent reference. Thus language to the effect that an electronic document that is "readily accessible so as to be usable for subsequent reference" is considered to create a functionally equivalent document and meet the requirements of a statute for a written document.

2.3.14 Similarly, because electronic documents can be reproduced in multiples, legislation may provide that a legislative requirement that X number of copies be provided will be functionally satisfied by providing one electronic copy that can be reproduced. There is no point in providing the same electronic file multiple times.

2.3.15 The discussion of digital signatures, below, will provide more detail on how legal or practical signatures may be met. The functional approach of the New Zealand legislation, for example, states that requirements for a signature can be met if:

- The electronic signature adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature is attached;
- The signature must be as reliable as appropriate given the purpose for which, and the circumstances in which, the signature is required; and
- Where information that must be given to a person is required to be signed, the recipient must have consented to receiving the electronic signature rather than a traditional paper-based signature.

2.3.16 The test of whether the signature is as reliable as appropriate in the circumstances, etc. is an evolving one. The UNCITRAL Model Law on Electronic Signatures sets out some guidelines; this would be an appropriate area for elaboration by regulations or guidelines, as well as through court decisions. In Ontario, regulations have been developed describing "reliability" and "prescribed information technology standards" for electronic signatures etc. Similarly, regulations define the equivalency requirements for sealed documents.

2.3.17 In some cases, legislation may be so inter-twined with language that implies a paper-based system, such as the Botswana *Stock Exchange Act*, that legislation establishing functional equivalency may authorise the use of electronic communication, but only at a cost of confusion and uncertainty. In such a case, it may be better to specifically amend an individual statute and create an electronic regime tailored to that statute. That has been done in some jurisdictions with respect to corporations and securities law, as well as legislation dealing with financial and banking settlement activity.

2.3.18 Provisions for dealing with record retention are also important since experience has shown that difficulties of reading electronic material when technology changes rapidly and the medium is not necessarily well suited to archival conditions. For example, it may be necessary to ensure that changes in format do not compromise accuracy. It may also be necessary to clarify that legal requirements for document retention are satisfied by electronic copies, again possibly with certain exceptions.

2.3.19 Historically, courts have generally preferred oral testimony of witnesses to the presentation of information in documents. To be admissible, a document must be relevant (as must oral testimony) and it must be at least somewhat reliable for showing the facts—i.e., must not be counterfeit or altered. Authentication of a document is fundamental to its admissibility and this may include developing a foundation for its authenticity—including testimony on how and where it was made, stored, copied etc.) If the original document cannot be authenticated, then even reliable evidence with respect to its conversion to another format will not render it credible or admissible. Consequently, various "rules of evidence" and commercial rules have developed to deal with such matters as business records made in the course of business or the time and place when a contract is made. Electronic documents and e-commerce raise new issues. For example, is a computer printout an "original"? What is the impact of migration to a new format when information is being archived or kept for a similarly long time? What is the status of computer-generated information?

2.3.20 The evidentiary value of documents is linked, of course, to the provisions in an Electronic Commerce Act. Meeting the provisions of such legislation, however, does not guarantee that a document will be admissible but it allows certain presumptions, such as the time and place of the making of a contract, to be established. It also provides a framework that the court can look to in determining the reliability of the authenticity of an electronic signature, for example, and the weight to be given to attribution. The creation of equivalency rules and statements that electronic documents may be legally recognised provides the courts and other tribunals (including arbitrators and other practitioners of dispute resolution) with guidance and authority to accept electronic documents in evidence.

2.3.21 The Uniform Law Conference of Canada developed a Uniform Electronic Evidence Act,[9] which is intended to provide examples of amendments to existing rules of evidence to facilitate the admissibility

[9] www.law.ualberta.ca/alri.ulc/current/eeeact.htm

of electronic records in court proceedings. The "best evidence rule"[10] could be applied to electronic records by providing a method to evaluate the integrity of an electronic record by considering the reliability of the record-keeping system that generated the electronic record. The person seeking to introduce an electronic record has the burden of proving the integrity of the record by adducing evidence of the reliability of the record-keeping system that created and stored the electronic record. A court or tribunal may consider adherence to record-keeping standards as a relevant factor in determining the reliability of the system.

2.4 Recommendations:

- The Ministry of Communications, Science and Technology, in consultation with such stakeholders as the Bank of Botswana, financial institutions, the Botswana Stock Exchange, brokerage houses, the financial and commercial bar, business groups, and labour and consumer groups, develop legislative proposals for an e-commerce act.
- The Ministry of Trade and Industry, in consultation with such stakeholders as the Bank of Botswana, financial institutions, the Botswana Stock Exchange, brokerage houses, the financial and commercial bar, business groups, and labour and consumer groups, examine corporate and securities legislation to determine whether equivalency legislation for e-commerce is adequate and what, if any, additional legislative amendments may be required.
- The Ministry of Finance and Development Planning in conjunction with the Bank of Botswana and in co-operation with other stakeholders, such as financial institutions, the Botswana Stock Exchange, brokerage houses, the financial and commercial bar, business and consumer groups, examine the needs of financial institutions for specific legislative authority for additional use of electronic transactions.
- The Attorney General's Chambers examine the *Rules of Criminal Procedure* and the *Rules of Civil Procedure*, in consultation with the Law Society, to identify amendments to the Rules required to ensure that electronic documents receive equivalent treatment in judicial proceedings.
- All Ministries and parastatals review their records retention policies to ensure that they are up-to-date to meet the requirements of an electronic environment.
- All Ministries review their legislation and policies to identify restrictions on the implementation of e-Government

[10] An original document should be presented to a court; if it is not available due to loss or is unduly burdensome to obtain, a copy may be presented but it is likely to be given less evidentiary weight.

communications, e.g., requirements for the paper filing of documents, etc.

3.0 Enforcement of Consumer Rights in e-Commerce

3.1 Objective:

- Ensuring that consumers in Botswana are not disadvantaged by the use of e-commerce and have access to the same remedies and protection that they would have in face-to-face transactions.

3.2 Issues:

- Ensuring that consumers are educated about their rights and what they should expect from reliable vendors on the Internet.
- Developing a culture in Botswana where businesses operating on the Internet adhere to high standards of consumer information and protection.
- Developing the capacity to enforce consumer protection legislation, in particular, developing the arrangements and capacity to co-operate with enforcement colleagues in other jurisdictions.
- Providing and encouraging the provision of self-regulatory regimes and dispute resolution mechanisms.

3.3 Discussion:

3.3.1 Whether consumers purchase locally or internationally through the Internet, they should continue to have access to the same remedies for defects or breaches of contract that they would have if they purchased in person. Unfortunately, extra-territorial enforcement of consumer protection laws presents a major challenge in the e-commerce environment and has a continuing negative effect on the growth of consumer trust and confidence in e-commerce. Private international law is inadequate to deal with the problems of the average consumer and, indeed, with all but the larger and more sophisticated of businesses.

3.3.2 The Organisation for Economic Co-operation and Development approved *Guidelines* to help ensure that consumers receive the same level of protection when they shop online as they do when they buy from a local store or order from a catalogue.[11] The Guidelines set out core characteristics of effective consumer protection for on-line business transactions and reflect existing legal protections available to consumers in more traditional forms of commerce.

---

[11] *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* www.oecd.org/dataoecd/5/34/1824782.pdf

3.3.2 The OECD *Guidelines* are in the forefront of public and private sector activities on business-to-consumer (B2C) electronic commerce. A number of governments and businesses have carried out public education and information initiatives based on the Guidelines; legislation has been reformed to reflect the principles in the Guidelines; and codes of conduct, trustmark programmes,[12] and self-regulatory regimes have been developed to implement the Guidelines.

3.3.4 Several countries are working on bi-lateral and multi-lateral law enforcement arrangements to ensure consumers receive effective protection no matter where they shop or from whom they buy. For example, information sharing and enforcement cooperation agreements have been signed by a number of country regulators, including the Australian Competition and Consumer Commission and the U.S. Federal Trade Commission. Canada, Australia and New Zealand have also recently signed a cooperation agreement relating to the application of their competition and consumer laws. International "sweep days" are becoming a regular event as law enforcement authorities from the international community focus on particular scams and evaluate internet sites according to a number of key consumer protection principles outlined in the *Guidelines.*

3.3.5 Many countries issue press releases and distributed copies of the *Guidelines* to businesses. In Norway and Switzerland, the government expanded its education initiatives into the schools to teach teenagers and children their responsibilities as consumers in the electronic marketplace. Australia, Finland, France, and Portugal have set up websites to provide consumers with up-to-date information, references and hyperlinks on a range of consumer issues, including tips for better and safer online shopping. Many countries have been developing information and education programmes for consumers using e-commerce and businesses using the Internet to reach consumers.

3.3.6 Several countries have been pursuing codes of conduct as a means of self-regulation by e-vendors. In Norway, the National Consumer Council and representatives of business established a voluntary and independent label, N-safe. Businesses allowed to display the N-safe label are subject to the principles defined by the label requirements. The

[12] See, for example, TrustUK, where the trustmark on a website indicates that the vendor abides by commercial standards. www.trustuk.org.uk; the U.S. Better Business Bureau's BBBOnline (www.bbbonline.org) has a set of good business guidelines that, if a firm abides by them, can be displayed on a website. The Global Business Dialogue provides an inventory of trustmarks (which may be out of date): www.consumerconfidence.gbde.org/t_inventory.html

European Commission is working with a group of consumer and industry organisations to identify key principles for business-to-consumer electronic commerce codes.

3.3.7 All these activities are backed by several pre-conditions. The countries have adequate consumer protection legislation, including provisions dealing with misleading advertising, telemarketing and deceptive marketing practices. The countries have active consumer protection units in appropriate ministries and enforcement agencies. Officials work closely with industry sectors, particularly with business leaders who are anxious to have a reputation for fair dealing and probity. International arrangements and co-operative agreements are in place to allow for investigations and enforcement actions across jurisdictional lines. Furthermore, the governments and industry actively support the development of alternative dispute resolution mechanisms, including on-line dispute settlement services. E-Government is used as an active tool to educate consumers and provide help with dispute settlement and self-enforcement. Communities and the education system are interested and involved in consumer rights generally, as well as the new problems presented by e-commerce. Government has a strong, but challenging, role to play in ensuring that these pre-conditions are met.

3.4 Recommendations:

- The Ministry of Trade and Industry in consultation with the Law Society, and consumer and business groups review consumer protection legislation to ensure its adequacy in an electronic environment and consider adoption of the OECD Guidelines.
- The Ministry of Trade and Industry work with the Ministry of Education and consumer, business and parent groups in developing programmes for schools educating students about consumer rights in general and e-commerce in particular.
- The Ministry of Communications, Science and Technology and the Ministry of Trade and Industry work with consumer groups and industry and community leaders to develop net trust labels and consumer information standards for Botswana businesses doing transactions on the Internet.

4.0 Protection of Personal Privacy

4.1 Objective:

- Ensuring that Botswana has in place a legal framework and policies to protect personal privacy and personal data; in particular, to ensure that Botswana has a privacy regime that would be considered "adequate" to meet the principle of Article 25 of the European Community Parliament and Council *Directive on the Protection of*

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

4.2 Issues:

- Acceptability to Botswana of the Basic Principles established in the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.
- Identifying sectors where highest priority should be placed in ensuring that the framework and implementing systems meet European Community standards for acceptability of receipt of European personal data.
- Identifying the appropriate role for legislation and self-regulation through industry codes of conduct to meet international standards and the particular needs and capacities of Botswana.
- Identifying the role of Government and the institutional and programme elements that will be necessary to implement legislation and policy decisions dealing with the protection of personal privacy and personal data.
- Specific issues of translation into statutory language include: how to regulate secondary uses of personal data; degree to which organisation should have to justify the relevance of data for specific purposes; the circumstances in which "express" rather than "implied" consent should be required; distinctions among collection, use, and disclosure of information; exemptions for public security, health protection, historical research, etc.

4.3 Discussion:

4.3.1 The protection of personal information[13] first became a concern to governments and citizens with the development of automatic data processing and the potential to store vast quantities of information about individuals, their lives, their interests, and their transactions. The possibility of "data matching" and "data mining" of information that, by itself, seems relatively innocuous but, when combined with other data, gives a clear and intimate picture of an individual or a transaction further raised concerns about the protection of personal privacy.

[13] "Personal information" generally refers to information about an identifiable individual, that is, one can identify to whom the information relates rather than information about an anonymous person.
The U.K. *Data Protection Act 1998* defines "sensitive personal data" as information as to racial or ethnic origin, political opinions, religious or similar beliefs, membership in a trade union, physical or mental health or condition, sexual life, commission or alleged commission of an offence, or proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings.

4.3.2 The first international attempt to develop principles to deal with the protection of personal privacy in the context of computer data and the potential for trans-border flows of personal information was the 1980 Guidelines developed by the Organisation for Economic Co-operation and Development (OECD).[14] These Guidelines have since formed the basis for most privacy legislation around the world.

4.3.3 The Basic Principles of OECD *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data* are:

1. *Collection Limitation Principle*
There should be limits to the collection of personal data [defined as data about an identifiable individual] and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. *Data Quality Principle*
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for these purposes, should be accurate, complete and kept up-to-date.

3. *Purpose Specification Principle*
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. *Collection Limitation Principle*
There should be limits to the collection of personal data [defined as data about an identifiable individual] and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

5. *Data Quality Principle*
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for these purposes, should be accurate, complete and kept up-to-date.

6. *Purpose Specification Principle*

[14] *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*; www.oecd.org/dsti/sti/it/secur/index.htm

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

7.Individual Participation Principles
An individual should have the right:
(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him (i)within a reasonable time; (ii)at a charge, if any, that is not excessive; (iii)in a reasonable manner; and (iv) in a form that is readily intelligible to him;
(c) to be given reasons if a request is made under subparagraph (a) and (b) is denied, and to be able to challenge such denial; and
(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8.*Accountability Principle*
A data controller should be accountable for complying with measures that give effect to the principles stated above.

In addition to the eight privacy principles, the Guidelines set out principles for free flow of data and legitimate restrictions, national implementation and international co-operation.

4.3.4 These eight principles are generally agreed to deal with the most important issues regarding the protection of personal privacy in an electronically connected world. More importantly for Botswana and other jurisdictions wishing to do business globally through electronic media, they are reflected in the European Community Parliament and Council *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[15] Noting that data processing systems are intended to be servants and must respect fundamental rights of individuals, including privacy, the Directive sets out Principles Relating to Data Quality.

4.3.5 Article 6 indicates that Member States [through their national legislation] must provide that personal data must be:
- Processed fairly and lawfully;

[15] Directive95/46EC, October 24, 1995, Official Journal L 281, 23/11/1995 P. 0031-0050.

- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provide that Member States provide adequate safeguards;
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down safeguards for personal data stored for longer periods for historical, statistical or scientific use.

4.3.6 Article 7 states that Member States shall provide that personal data may be processed only if:

- The data subject has unambiguously given his consent; or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [note: defined term] or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party of parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject that require protection under Article 1(1) [Note; object of the Directive relating to fundamental rights].

4.3.7 Additional provisions deal with special categories of processing (e.g., medical data); information to be given to the data subject; the data subject's right to access to data; exceptions and restrictions; data subject's right to object; confidentiality and security of processing; judicial remedies, liabilities and sanctions. In addition, Chapter IV, Transfer of Personal Data to Third Countries, sets out the provisions that

have critical implications for non-EC countries, including Botswana. The first principle of Article 25 states:

> "The Member State shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection".

4.3.8 The second principle states:

"The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surround a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures that are complied with in that country".

4.3.9 To date, the Commission has determined that personal data can flow from the EU Member Countries (and Norway, Liechtenstein and Iceland) to the following recognised "third" countries: Switzerland; Canada; Argentina; Guernsey, Isle of Man; and in the United States, companies following the U.S. Safe Harbor Rules and Air Passenger Name Records to the U.S. Bureau of Customs and Border Protection.

4.3.10 The EC Directive, coupled with the Principles outlined in the OECD Guidelines have informed most of the legislation and practice in privacy protection in developed and developing countries. The legislative and institutional form of privacy protection may vary significantly, however. The primary differences are not in the underlying principles but in the degree to which industry takes responsibility for implementation and the degree to which coverage applies across commercial and government sectors. The consideration of these factors and the institutional and legislative design decisions will be very important to Botswana and to the successful implementation of a privacy regime that will be both effective and meet international standards while not being unduly burdensome in terms of resources, including expertise.[16]

[16] A specific role identified for the Hong Kong Privacy Commissioner is to ensure "all other jurisdictions with data protection laws are aware of the robustness of the protection of the privacy of the individual with respect to personal data so as to prevent interference with the free flow of personal data to Hong Kong." www.pco.org.hk/english/about/role.html

4.3.11 Most countries, with the exception of the United States, have set up data protection agencies (i.e., Data Protection Commissioners, Privacy Commissioners) with varying degrees of oversight, enforcement power, and regulatory or advisory powers. In some regimes, self-regulation through industry codes of practice plays a stronger role than in others.

4.3.12 Canada has taken an approach with both broad coverage across the public and private sectors generally and legislative regime that has proved to be controversial and, some would argue, confusing and burdensome to implement. These concerns may be indicative of the fact that the regime is in its early stages and that there are a mix of federal and provincial legislation, but do raise questions of whether Botswana should look to Canada as a model. The federal Canadian legislation, which is coupled with e-commerce legislation (discussed above), is the *Personal Information Protection and Electronic Documents Act*.[17] Like most personal privacy protection regimes, the Canadian legislation provides for exceptions to the application of the Principles. For example, information about an individual may be collected without his knowledge or consent in the course of an investigation into a contravention of laws or if it is for the purpose of acting in respect of an emergency that threatens life or health. Disclosures may be made for such purposes as national security, law enforcement or where required by law. These are common exemptions, but statutory language and scope require careful consideration.

4.3.13 Australia, New Zealand, the Netherlands, Ireland, the United Kingdom and Hong Kong (among others) have approaches to personal privacy protection that place a more specific emphasis on industry or situational codes of conduct. For example, the UK Data Protection Registrar has developed a Code of Practice on Closed Circuit Television Cameras. New Zealand has several codes that may impose more or less stringent conditions on particular industries, including a Code for the Health Care Industry and a Telecommunications Information Privacy Code.[18]

4.3.14 Australia's *Privacy Act 1988* (Cth) was the first to establish National Privacy Principles that could be replaced by authorised industry-specific codes that met the objectives of the Principles. Each code must have a "code administrator" to enforce the code. Fewer codes have been registered than anticipated, but include the Market and Social Research Privacy Code; the General Insurance Information Privacy Code; and the

[17] S.C. 2000, c.5.
[18] See www.privacy.org/nz

Clubs Queensland Privacy Code. Codes currently being considered include the Australian Casino Association Privacy Code; the Internet Industry Privacy Code; and the Biometrics Institute Privacy Code. The Commonwealth Attorney General has recently asked the Federal Privacy Commissioner to conduct a review of, among other matters, the effectiveness of the co-regulation model using industry codes.

4.3.15 In addition to fostering industry codes, legislation or policy can mandate or encourage Privacy Impact Assessments (PIAs) as a method to anticipate privacy problems before they occur. PIAs, which have been used extensively in New Zealand and are now being adopted in other jurisdictions,[19] are useful to assess risks arising from new technologies or new applications of technology (e.g., electronic road pricing or intelligent transportation systems) or where the use of privacy intrusive technologies is being expanded (e.g., expanding data matching, drug testing, or the use of closed circuit TVs in public places). New endeavours, often initiated by governments, such as "smart cards" or mergers of public data registries may also be suitable for PIAs.

4.3.16 Self-assessment of privacy protection by organisations is encouraged by a number of countries. The Data Protection Commission in Ireland has created a *Data Protection Checklist*[20]that allows companies to self-assess the adequacy of their own data protection policies. The Checklist sets out a structured examination of data protection issues that can be converted into a clear policy position on data protection by the company. In Ontario, Canada, the Information and Privacy Commissioner has developed a set of Best Practices for on-line data protection.[21] These outline areas that should be addressed by an organisation to effectively protect the privacy of on-line customers and draw upon the OECD Guidelines. The OECD itself has published a Privacy Statement Generator, which provides guidance on conducting an internal review of existing personal data practices and on developing a privacy policy statement.[22] Similar guidance has been provided by authorities in a

[19] In Canada, for example, federal government departments are required to carry out a PIA for any activity or action that may have privacy implications; see Treasury Board of Canada, *Privacy Impact Assessment Policy*; www.tbs-sbt.gc.ca See also, the Guidelines issued by the Management Board Secretariat in Ontario, Canada: www.gov.on.ca?MBS/english/fip/pia; United States, *E-Government Act*, www.whitehouse.gov/omb/memoranda/mo3-22.html

[20] www.dataprivacy.ie/3k.htm

[21] *Best Practices for Online Privacy Protection*, www.ipc.on.ca

[22] www.oecd.org; see also, OECD Working Party on Information Security and Privacy, *Privacy Online: Policy and Practical Guidance*, 21-Jan-2003, DSTI/ICCP/REG(2002)2/Final.

number of jurisdictions.[23] Irrespective of the final institutional and legal arrangement chosen by Botswana, experience indicates a clear role for government in providing guidance and fostering self-assessment for compliance with internationally accepted data privacy principles.

4.3.17 In the United States, the approach to privacy protection has been the "Safe Harbor Privacy Principles",[24] which were accepted in part by the European Parliament as an "adequate" means of protecting personal privacy in trans-border data flows.[25] The European Parliament noted that "adequate" protection does not mean "per se that the third country should have the same rules as the Union, but that, regardless of the type of legislative protection in force in the third country, the data subject must be effectively protected." Objective criteria were to be used to assess effectiveness, such as the possibility of identifying the person to whom the data relates, the type of data being processed, and the mechanisms used to guarantee protection. Although there was no single piece of legislation governing the protection of personal privacy in the United States, there were pending individual sectoral legislative provisions and the US was a signatory to the OECD Ministerial Statement ratified in 1998. Since the European Parliament resolution, legislation has been passed to cover financial services, including banks.[26] In addition, over 150 companies have self-certified under the Safe Harbour framework, including Microsoft, Intel, Hewlett-Packard, and Proctor & Gamble.[27] If an organisation leaves the Safe Harbor for any reason, the obligation to continue to follow the Safe Harbor Principles for data collected under the Principles continues. The

[23] For example, Manitoba, Canada: *Privacy Compliance Tool Checklist*, www.ombudsman.bc.ca; Hong Kong, *Safe 2000*, www.pco.org.hk; New Zealand Privacy Commissioner, *Privacy Impact Assessment Handbook*, www.privacy.org.nz/comply/pia.html; Australia, Federal Privacy Commissioner, www.privacy.gov.au; Indonesia, www.gipi.or.id/page/php/Halaman%20Depan/Artikel/40.html

[24] The phrase is taken from securities legislation and practice where a regulator could determine that certain behaviour or actions constituted a "safe harbor" that was deemed to be compliant with the law.

[25] *European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce* (C5-0280/2000-2000/2144(COS)). See www.epic.org/privacy/intl/EP_SH_resolution_0700.html

[26] See, *Gramm-Leach-Bliley Act* (financial services); *Fair Credit and Reporting Act* (credit reporting agencies); the *Health Information Portability and Accountability Act* (health records). There is also federal U.S. legislation dealing with telemarketing, education records, and video store records. In addition, there are federal and state laws dealing with mailing lists; employment records; electronic surveillance; children's websites (e.g., *Children's Online Privacy Protection Act*), and the use of Social Security numbers.

[27] A list of "self-harborites" can be found on the website of the U.S. Department of Commerce. http://web.ita.doc.gov/safeharbor/shlist/nsf/webPages/safe+harbor+list

European Commission has developed contract clauses for companies to use to comply with the EU Directive.[28] Generally, enforcement is expected to be carried out by the private sector, backed by government enforcement under unfair and deceptive marketing and trade practices legislation.[29] The Principles require the "safe harborites" to use readily available independent third-party dispute resolution mechanisms, such as the American Arbitration Association or BBBOnline (a programme of the Better Business Bureau). Failure to comply with the Principles can result in an organisation's being removed from the Department of Commerce list.

4.3.18 The Safe Harbor approach has been subject to criticisms as being too piecemeal and scattered, lacking transparency, lacking potential for enforceability and possibly compensation, and possibly being less effective than more prescriptive and broader legislation. Nonetheless, the focus on industrial sectors where sensitive personal information is likely to be held (e.g., financial services), self-certification according to known standards, and contractual arrangements does have potential for adaptation in the Botswana context, particularly in early stages.

4.3.19 Privacy, which among other definitions, has been called "the right to be left alone," becomes an important element in the control of other electronic activities. Specifically, unsolicited marketing, automated calling, telemarketing, fax marketing, and "spam," Data protection legislation or telecommunications legislation in a number of jurisdiction deals with these electronic activities. Telemarketing may be a source of fraud, particularly when vulnerable persons are being preyed upon, and is often dealt with under deceptive marketing practices legislation (as well as penal legislation). Spam is increasingly recognised as a problem that has a significant negative effect on users' confidence in the use of e-mail and may be having a negative effect on the performance of the global e-mail network. According to some sources, unsolicited bulk mail volumes now account for as much as one-half of all e-mail traffic on the Internet. Some studies indicate that there are significant losses in productivity as workers spend increasing amounts of time clearing spam

[28] The European Commission has approved model contracts for data transfer both for controller-to-controller transfers (Commission Decision 15 June 2001 on standard contractual clauses for personal data to third countries, under Directive 95/46/EC, (2002) OJ L181/19) and for controller-to-processor transfers (Commission Decision 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, (2002) OJ L6/52.) Model contracts for data transfer have also been developed by the International Chamber of Commerce

[29] Any reliance by Botswana on a similar scheme should be connected with policy development on an independent and expert Competition Authority to enforce unfair trade practices.

from their computers and the content may be objectionable (see discussion of "unacceptable" content, below). One of the more recent legislative initiatives is that of Australia, the *Spam Act 2002*. The Act prohibits unsolicited electronic messages; in addition, commercial electronic messages must contain accurate information about the sender and a functional way for recipients to indicate that they do not wish to receive such messages in the future. Address harvesting software is forbidden. The Act does not impose any liabilities on Internet Service Providers for the transmission of spam, but the Australian Communications Authority is working with ISPs to develop industry codes of practice regarding acceptable use policies for consumers and the use of anti-spam filters. The Act applies to all Australian residents and any person sending an electronic message to an address that has an Australian link; the government recognises that extra-jurisdictional enforcement will be weak in the absence of increased partnerships with foreign countries and organisations to reduce spam.

4.3.20 In dealing with such matters as spam, it is important to make legislative or other rule provisions as technically neutral as possible—mobile phones, for example, are now capable of sending and receiving spam or being used in other ways that invade privacy. The European Commission's Directive on Privacy and Electronic Communications extends controls on unsolicited direct marketing to all forms of electronic communications, including mobile phones, and introduces controls on the use of cookies on websites. Cookies and similar tracking devices will be subject to a new transparency requirement that provides information and allows users to refuse to accept them if they wish. EC Members were required to implement the Directive by December 2003.

4.3.21 The South African *Electronic Communications and Transactions Act* regulates spam, among other matters; unsolicited electronic communications are not illegal, but they must contain an opt-out and disclose where they obtained the address when requested. The drafting of the statute has been criticised for lack of specificity regarding opt-out previsions, and lack of clarity regarding the definition of "sender" which could leave ISPs liable for what is sent. In the U.K., the *Privacy and Electronic Communications (EC Directive) Regulations 2003* are also aimed in part at spam, but have been criticised for weak and unwieldy enforcement provisions, which require filling out a five-page form and mailing it with a stamp to the Information Commissioner. In response to the increasing problem of spam, the OECD has recently set up a Task Force to co-ordinate the fight against spam and has called on governments to step up their fight against spam.

4.3.21 The OECD has noted that the privacy protection systems in many countries are hybrid approaches, combining self-regulation and legislative action, although the issue has often been approached as if these approaches are entirely separate. In fact, a combination of policy tools often leads to the strongest result and this may be particularly true in Botswana, which wishes to be able to deal at a sophisticated level and become a leader in connectivity and e-commerce in Africa while focusing on priorities and using resources wisely. Privacy protection is an area where the Government can provide leadership and guidance through information (using e-Government and other information and distribution media); early adoption of privacy-enhancing technology, techniques and policies; selective legislation in key sectors (such as financial services and health); and promotion of contractual safeguards and dispute settlement mechanisms.[30] In addition, key regulators and parastatals (e.g., the Botswana Telecommunications Authority and the Botswana Stock Exchange) can play an important role in fostering privacy principles and applications through a network of both regulatory requirements and internal compliance policies.

4.4 Recommendations:

- The Ministry of Communications, Science and Technology should lead a review in conjunction with the Inter-ministerial Legal Reform Task Force to establish policies and procedures, possibly including legislation, for the application of Privacy Principles to the activities and data holdings of Government.
- The Ministry of Communications, Science and Technology should lead a review in conjunction with the Botswana Telecommunications Authority and the Attorney General's Chambers, in consultation with such stakeholders as Internet Service Providers, Botswana Telecommunications Corporation and other providers of telecommunications services, and business and consumer groups, to develop recommendations for the appropriate approaches to the control of "spam".
- The Ministry of Trade and Industry in consultation with the Ministry of Finance and Development Planning, the Botswana Stock Exchange, the Bank of Botswana, the Ministry of Tourism, the Ministry of Local Government, and the Ministry of

[30] The OECD Report, Privacy Online: Policy and Practical Guidance", found that countries noted that contractual arrangements had worked well, but there were limitations, particularly for small users or business-to-consumer contacts. Specifically, contractual frameworks generally did not provide adequate redress mechanisms for consumers or small businesses. OECD Member countries therefore agreed to focus less on contractual solutions and more on how to ensure redress through alternative dispute resolution measures, including on-line dispute settlement.

Communications, Science and Technology and representatives of such sectors as tourism and financial services and consumer groups, should review the development of sector-specific legislation or regulation, possibly backed by industry codes of conduct, to ensure the adoption of the appropriate privacy protection principles by key industrial sectors.

- The Ministry of Health in conjunction with the Ministry of Local Government and in consultation with stakeholders from both the public and private health systems, such as the hospitals, local medical associations, the Health Professions Council, the National AIDS Coordinating Agency, and the Ministry of Communications, Science and Technology, and consumer and civil liberties groups should review the development of legislation or rules, possibly backed by sector and professional codes of conduct, that would ensure the privacy and security of personal data in health records.

5.0 Security of Information Systems and Networks: A Culture of Security

5.1 Objective:

- Ensuring that Botswana has in place a "culture of security," including legislation and policies that will allow for the effective implementation of legislation and policies regarding the protection of personal privacy and personal data, as well as other sensitive and significant data and infrastructure.

5.2 Issues:

- Co-ordination with work being done by the Infrastructure and Security Task Force to ensure that the implications of privacy and data protection are being taken into consideration in the planning and building of Botswana's telecommunications infrastructure.
- Co-ordination with work being done by the e-Government and Education and Training Task Forces to ensure that the appropriate policies and training are in place so that individuals in both the government and the private sector have in place and understand the importance of policies and procedures to maintain security dealing with the protection of data and personal privacy.
- Development of a public policy dealing with cryptology and encouragement of the use of appropriate cryptology (such as "Pretty Good Privacy" to encourage trust in the Internet and e-commerce.

5.3 Discussion:

5.3.1 The privacy provisions of the European Union *Directive On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, the OECD Guidelines

and other OECD statements, as well as laws and policies around the world,31 have direct implications for the security of data and electronic communications systems. Both implicit and explicit are the requirements that data be protected from intrusion and deliberate or accidental release or alteration. Related to this is also the issue of cryptography. Effective implementation of an ICT Strategy will depend, among other matters, on secure systems and networks. Businesses, governments, consumers, foreign investors, foreign governments and others will want to be assured that data is secure and that networks are secure.

5.3.2 The technical side of this issue is being handled by the Infrastructure Task Force and will be reflected in the observations and recommendations from that Task Force and the Action Plans being developed to implement the Infrastructure portions of Maitlamo. However, the development of proposals to implement protections of personal information and privacy must be accompanied by policies to ensure that personal data is secure in a practical sense. Some of these issues relate to network design, but others relate to organisational design and records management and data practices found in governments, parastatal organisations and businesses. Among the actions that should be considered are the dissemination and implementation of the OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.[32] Following the publication of the Guidelines in 2002, OECD Member Countries adopted Implementation Plans.

5.3.3 A number of countries and businesses have relied on internationally recognised standards. ISO/IEC 17799 is a standard code of practice that provides an organisation with default guidelines on the types of security controls the organisation should implement to safeguard its assets. BS7799, which is a management standard specification for Information Security Management Systems, sets up the necessary steps required to establish a management framework. ISO/IEC 15408 sets out "Evaluation Criteria for Information Technology Security". Formal certification and audit to these standards may be too elaborate and expensive for most businesses in Botswana, just as the ISO 9000 series of Quality Management Standards can be expensive to certify and maintain. Nonetheless, they can provide a structure against which government and

[31] See, for example, APEC Cybersecurity Strategy, www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html. Australia, E-Security National Agenda, September 2001, www.noie.gov.au/projects/confidence/Protecting/nat-agenda.htm.

[32] www.oecd.org/sti/security-privacy

business security systems and risk assessments and risk management can be judged.

5.3.4 Cryptography is an important component of secure information and communications systems and is an effective tool for ensuring both the confidentiality and the integrity of data. However, the widespread use of cryptography can raise several concerns. While cryptography has many legitimate and necessary uses and its use is promoted by privacy advocates, it can also facilitate illegal activity and affect public safety and national security. Governments, including the Government of Botswana, therefore face a challenge in balancing the various interests in developing policies and legislation to deal with the use and promotion of cryptography.

5.3.5 The OECD has set out *Guidelines for Cryptology Policy*[33] that are intended to promote the use of cryptology and foster confidence in information and communications infrastructures, networks, and systems. At the same time, there is no intention that cryptography will unduly jeopardise public safety and law enforcement. The balancing of interests is recognised through such principles as the right to secrecy of communications (Principle 5) while noting that national cryptography policies may allow for lawful access to plaintext, or cryptographic keys, of encrypted data (Principle 6). In addition, governments should cooperate to coordinate cryptography policies and avoid creating barriers to trade in the name of cryptography policy (Principle 8). Users should have a choice of cryptographic methods, which should be developed in response to market needs. The liability of individuals or entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

5.3.6 Partly in response to the OECD work and the EC initiatives and partly in response to the development of a mature global electronic environment, a number of countries are developing policies and legislation dealing with cryptography and on-line privacy.[34] A fully developed policy environment for Maitlamo should deal with the issue and provide appropriate policy guidance. Cryptography issues that specifically relate to digital signatures will be discussed, below.

---

[33] www.usdoj.gov/criminal/cybercrime/oeguide.htm. Adopted by the Council of the OECD on 27 March 1997. See also, OECD *Guidelines for Cryptography Policy: Report on Background and Issues of Cryptography Policy*; www.usdoj.gov/criminal/cybercrime/oeback.htm.

[34] For example, Canadian Task Force on Electronic Commerce, *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*;

5.4 Recommendations:

- The Ministry of Communications, Science and Technology, in conjunction with the Inter-ministerial Legal Reform Taskforce, should review the OECD Guidelines and Implementation Plan and other relevant information (e.g., APEC Cybersecurity Strategy, Australia E-Security National Agenda) for consideration of adoption of the Guidelines and the development of an Implementation Plan by the Government of Botswana.
- The Ministry of Communications, Science and Technology, in conjunction with the Inter-ministerial Legal Reform Taskforce, consider ISO/IEC17799/BS7799 as a tool for setting rules for government IT purchases and assessing compliance of government systems with the "Risk assessment", "Security design and implementation", "Security management" and "Reassessment" principles of the Security Guidelines.
- The Ministry of Communications, Science and Technology, in consultation with the Ministry of Trade and Industry, the Ministry of Finance and Development Planning, the Ministry of Health, the Botswana Telecommunications Authority, the Bank of Botswana, the Botswana Stock Exchange, the Law Society and such stakeholders as representatives of financial institutions, brokerage houses, hospitals, business and consumer groups, and civil liberties groups consider developing a National Policy for Security of Information Systems and Networks.
- The Ministry of Trade and Industry, in consultation with the Ministry of Trade and Industry, the Ministry of Finance and Development Planning, the Ministry of Health, the Botswana Telecommunications Authority, the Bank of Botswana, the Botswana Stock Exchange, the Law Society and such stakeholders as representatives of financial institutions, brokerage houses, and business and consumer groups explore the implementation of ISO/IEC17799/BS7799 for selected industries, such as financial institutions and brokerage houses to provide an independently certifiable standard of security and risk assessment.
- The Ministry of Health, in cooperation with the Ministry of Local Government and in consultation with stakeholders from both the public and private health systems such as the hospitals, local medical associations, the Health Professions Council, the National AIDS Coordinating Agency, and the Ministry of Communications, Science and Technology, should work to improve the protection of personal information, by considering the adoption of the ISO/IEC17799/BS7799 standards or basing internal security practices on the standards.

- Ministry of Trade and Industry publish a security guide for SMEs and share best practices, possibly as part of the e-Government initiative.

6.0 Electronic Signatures

6.1 Objective:

- Creation of a legal framework though legislation, policies, mutual recognition agreements and institutional arrangements that will allow Batswana to communicate electronically in an atmosphere of trust and privacy.

6.2 Issues:

- Identification of appropriate exceptions to the use of electronic signatures, e.g., wills, domestic law agreements.
- Development of criteria for various levels of security and determining what level of security should be required (or permitted) for particular uses.
- The role that Government plays with respect to certification authorities; e.g., should Government be a certification authority? Should Government licence certification authorities or create arrangements to recognise authorities licensed or recognised in other jurisdictions?
- Should there be a hierarchy of certification authorities reflecting such matters as degree of Government authorisation and/or security of system?
- What criteria should be used to recognise electronic or digital signatures originating in other jurisdictions?
- The liability regime that should be attached to certification authorities.
- Ensuring that different cryptography/digital signature methods are inter-operable (function together), mobile (function in multiple information and communications infrastructures); and portable (capable of being adapted and function in multiple systems);
- Working with appropriate partners, including foreign jurisdictions such as South Africa, to ensure the most flexible and least burdensome regime that provides adequate protection is created.

6.3 Discussion:

6.3.1 Signatures on documents perform a number of functions. These include identification, authentication, declaration of will or intent, authorisation, safeguarding against undue haste, non-repudiation of origin or receipt, notice of contents, integrity and originality. Signatures do not attest, of

course, to the validity or value of the information in a document. Both studies and common sense indicate, however, that the full potential of e-commerce will not develop until there is a sufficiently trusted means of communicating and authenticating communications—of performing functions similar to those of signatures. In an electronic environment, the original of a message cannot be distinguished from a copy; there is no handwritten signature; it is not on paper; and it can be manipulated or altered without being easily discernable—indeed, it can be altered without the direct intervention of a human. There is considerable scope for fraud or error. The purpose of electronic signatures is to offer some technical means by which the characteristics of a signature can be duplicated in an electronic environment.

6.3.2 Depending on the importance of the document, electronic signatures may be a necessary and inherent part of the communication under e-commerce or electronic transactions statutes. Phrases such as "secure electronic signatures" may not only satisfy provisions relating to signatures, but also with legislative language dealing with witnesses, notarisation, and statements made under oath. They may also be used to deal with requirements for "original" documents.

6.3.3 Cryptography can also provide technical solutions for protection of intellectual property in digital form. For example, a digital signature in conjunction with a verifiable time stamp can give authors some control over their work by tying an electronic document to a particular issuer and ensuring that it cannot be altered without detection. This technology can also be used to ensure the integrity of electronic archives, an increasingly important issue.

6.3.4 Virtually all OECD countries have some form of legislative or regulatory framework in place to provide for the legal effect of electronic signatures. While details differ, there is a consistent approach. All are theoretically technology neutral, although in some cases where a high degree of certainty was required, policies specified the use of technology that was asymmetric cryptography-based.

6.3.5 Digital signatures are an important application of public key cryptography, which must be considered in conjunction with policy development on cryptography, discussed above.[35] Other authentication models are possible, including biometric devices, use of personal identification numbers (PINS) or "passwords," digitised versions of

[35] Using cryptography for digital signatures should not be confused with the creation of confidential messages, which may be limited in some circumstances (or using some methodologies) for reasons of national security or defence. Digital signatures using cryptography may be appended to non-encrypted messages.

handwritten signatures, and clicking an "OK box." These have, of course, different levels of security and are appropriate for different circumstances.

6.3.6 Digital signatures that are created and verified by public key cryptography usually use algorithmic functions to generate two different, but mathematically related, "keys". One key is used for creating the signature and the other for verifying the signature. The key used by the signatory to create the digital signature is known as the "private key," while the more widely known key used to verify the signature is the "public key," It is important that the signatory keep the private key secret since that is the basis for authenticity, although the user does not need to know the key but can use a smart card or other device to "sign," The public key cannot be used to re-create the private key so it is possible for many people, including public institutions, to have a copy of the public key.[36]

6.3.7 Certification is an important element of digital signatures using public key cryptography. It is necessary that the relationship between the holder of the private key and its associated public key be capable of authentication or verification in order to prevent impersonation or fraud in an electronic environment. In order for key systems to work, the public key must accessible. If the parties know each other, this can be accomplished through prior arrangement or contract. Full use of e-commerce and the electronic environment, however, requires that trust be established when parties are strangers and, indeed, may not even know each other's full identities.

6.3.8 The solution to this problem is the development of "certificate authorities" or "certificate services" that certify the identity of the parties exchanging cryptographic information over the Internet. Certificate authorities can also perform other functions, such as notary and time-stamping services.

6.3.9 Certificate authorities can operate in either the public or the private sector. In examining the appropriate policy approach to public key infrastructures (PKIs) in Botswana, it will be necessary to determine the form and number of levels of authority that should be comprised in a PKI; whether the certifying authorities should be public authorities or licensed by public authorities; whether non-licensed certifying authorities should be permitted (presumably with a lower degree of

[36] There are other techniques, including cryptosystems based on elliptical curves and "hash functions," that may be used.

reliability in the commercial sense); and the degree to which cryptography should be permitted for confidentiality purposes.

6.3.10 Different countries have taken different approaches to electronic authentication in order to balance concerns about electronic commerce, lawful state access, human rights and civil liberties, and technical security considerations. The European Parliament issued a Directive in 1999 on a *Community Framework for Electronic Signatures*[37] aimed at enhancing the development of competitive cross-border certification providers. The certification service providers should be able to operate without the need for prior national authorisation and voluntary accreditation schemes should be developed to create a framework for the levels of trust, security and quality demanded by an evolving market. The legal recognition of electronic signatures should be based upon objective criteria and not linked to authorisation of certification service providers. In compliance with the Directive, EU countries tend not to have licensing regimes.

6.3.11 UNCITRAL develop a detailed *Model Law on Electronic Signature***s** in 2001[38] to expand on the guidance given in the Model Law on E-Commerce regarding signatures and to avoid the risk that different countries would develop divergent approaches to electronic signatures. The Model Law on Electronic Signatures offers practical standards against which the technical reliability of electronic signatures can be measured. In addition, it links the level of technical reliability to the legal effectiveness that may be expected from a given type of electronic signature. In this way, the legal effectiveness of a signature can be pre-determined or at least predicted with some certainty, thereby enhancing the confidence of relying on electronic signatures in significant transactions. The basic rules set out in the Model Law are flexible with respect to the various parties that may become involved in electronic signatures (e.g., signatories, third parties and certification service providers). The Model Law complements the Model Law on Electronic Commerce by technical neutrality, i.e., not discriminating among the various techniques that can be used to transmit or store information.[39]

---

[37] 1999/93/EC, dated December 1999.

[38] For a review of the Working Group's reports see:
canada.justice.gc.ca/en/ps/ec/UN2000rep.html
canada.justice.gc.ca/en/ps/ec/uncon98.html
canada.justice.gc.ca/en/ps.ec/rf2000.html

[39] The Model Laws on Electronic Commerce and Electronic Signatures should also be read in conjunction with the UNCITRAL Model Law on Electronic Funds Transfers and the Model Law on International Credit Transfers.

6.3.12 The South African *Electronic Communications and Transactions Act* regulates cryptography providers. A Cryptography Service is expected to register its name with the Director-General of the Department of Communications, who also acts as the Accreditation Authority. Accreditation in this context means recognition of an authentication product or services designed to identify the holder of an electronic signature to other persons. Accreditation is voluntary. The Accreditation Authority has the power to monitor through "cyber inspectors" the conduct, systems and operations of the authentication service provider to ensure that it complies with the Act. The Minister of Communications, by notice in the Government Gazette, may recognise the accreditation granted to any authentication service provider in any foreign jurisdiction. The Act sets out criteria for recognition (e.g., financial stability, quality of hardware and software systems, independent audits).

6.3.13 The American Bar Association Section on Science and Technology issued *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* in 1996. To provide some consistency in interstate commerce, the United States Government passed the *Electronic Signatures in Global and National Commerce Act* (the E-SIGN law).[40] The law is technology neutral so parties can choose the system they want to use to validate an on-line agreement. It does not apply to certain transactions or agreements, such as the creation and execution of wills, adoptions, divorces, notices of cancellation of utility services, repossession or foreclosure of mortgages or termination of health or life insurance benefits.

6.3.14 In Canada, the government issued *Principles for Electronic Authentication* in 2003.[41] These principles are also intended to be technologically neutral and emphasise proportionality (i.e., the degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have), data privacy, and international compatibility. The Canadian Government took the

[40] Public Law No. 106-229, 114 Stat. 464 (2001); see, United States Government, Office of Management and Budget, *Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (E-SIGN)*, relating to federal agencies. See also, U.S. Department of Commerce, National Telecommunications and Information Administration, *Electronic Signatures: A Review of the Exceptions to the Electronic Signatures in Global and National Commerce Act, June 2003*
www.ntia.doc.gov/ntiahome/frnotices/2002/esign/report2003/coverack.htm

[41] See also, Industry Canada, Task Force on Electronic Commerce, *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*, February 1998 www.strategis.gc.ca

view that a "secure electronic signature" would meet the following criteria:

- The signature is under the control of the person or entity using it and no other person or entity uses the signature;
- It is possible to independently verify the association of the person or entity with the signature; and
- The signature is linked to data in such a manner that if any part of the data is changed, the signature is altered.[42]

6.3.15 Digital signatures created under a PKI regime, and possibly under other technologies as well, can present issues regarding to the protection of personal privacy. Data trails may be created and data matching may be facilitated. Implementation policies and government policies dealing with the recognition of certificate authorities should consider the need to balance personal and commercial privacy against other interests (some of which will be dealt with under "lawful access", below).

6.3.16 In some jurisdictions, distinctions are made between the approach used for digital signatures used by government or for government transactions and those used by the private sector for its own purposes. For example, in Australia, accreditation is mandatory for PKI-based certificates used by and with government agencies, but not for the private sector.

6.3.15 The EU recommended that governments play a more facilitative than regulatory role with respect to certificate authorities. It may not be necessary for Botswana to expend resources on developing a full-blown regulatory structure to deal with authorisation, but rather may find that consumers and business are sufficiently protected by a combination of recognising certificate authorities in other jurisdictions and establishing criteria against which levels of security and the appropriateness of a particular technology or authority can be judged.

6.4 Recommendations:

- The Ministry of Communications, Science and Technology, in consultation with the Ministry of Trade and Industry and the Attorney General's Chambers and other stakeholders such as business and consumer groups, and the Law Society, should examine the implications of adopting different approaches to the recognition of digital signatures, which include:
  - Legislative or other requirements regarding the level of security required for certain types of key documents;

[42] Canada, Department of Justice, *Consultation Paper on Facilitating Electronic Commerce: Statutes, Signatures and Evidence*; canada.justice.gc.ca/en/cons/facilt7.html

- Criteria by which security can be assessed, by both users and the courts;
- Criteria by which certificate authorities based in other jurisdictions can be judged;
- The utility of co-operating with neighbouring countries to establish a common framework for digital signatures, authentication and authorisation of certificate authorities.
- Clarification of liability of ISPs and certificate authorities.
- Methods of enforcing safeguards regarding certificate authorities outside of Botswana.

7.0 Cyber Crime; "Inappropriate Content" and Lawful Access

7.1 Objective:

Ensuring that the legislation of Botswana, including the *Penal Code*, is up-to-date and provides the necessary framework to deal with cyber-crime; that the cooperative arrangements and policies are in place to deal with extra-territorial criminal behaviour; that the skills and resources to deal with new types of crime are available; that legislation and policies are in place to deal with inappropriate content; and that credible and internationally acceptable procedures exist to deal with lawful access to electronic data, as well as other forms of information.

7.2. Issues:

- Legislative language of crimes related to property must encompass the newer meanings related to data, including reflecting the value of more amorphous forms of property.
- An appropriate mix of criminal law, regulation and co-regulation (e.g., use of industry codes of conduct) should be found to deal with issues of cyber-crime, inappropriate content in a global electronic environment, and relationships among stakeholders in combating crime and proscribed behaviour.
- Legislative precision will be required to ensure technical neutrality to the highest degree possible, while also providing the certainty, transparency and clarity required of penal and regulatory legislation.
- Identification of responsibilities of ISPs and other carriers of data, including circumstances in which they would be held responsible for the carriage of proscribed content.
- A delicate balancing of interests must be achieved in policy and legislation; among the interests are individual's right to personal privacy; business right to protect competitive information; freedom from undue intrusion by the state, and the responsibility of the state to protect and ensure the safety of citizens.

- Botswana must have the technical capacity and resources to combat international and domestic cyber-crime, including trained, dedicated experts with appropriate legal authority and mandate.

7.3 Discussion:

7.3.1 The concept of "cyber-crime" covers a wide area of activity, from intrusion into personal affairs and endangerment of privacy by hacking or computer harassment to computer-specific economic crimes, such as computer manipulations, computer sabotage, computer espionage, and software piracy. Generally, cyber-crime can be divided into two broad areas—one where a computer or computer technology is used in the commission of a more traditional crime (such as theft, fraud) and one where the crime is intrinsically related to the computer or computer technology (such as the introduction of a virus, altering data or hacking). The lines are not hard and fast, of course, since hacked information can be used for fraud, theft or extortion.

7.3.2 In addition, the Internet provides new means of communicating unacceptable content, such as racist or pornographic images (discussed below). The previously unforeseen speed and breadth of communication permitted by computers adds a new dimension to otherwise unacceptable but previously limited behaviour, such as invasion of privacy through dissemination of confidential or embarrassing information or images, such as compromising photos of ex-spouses. There are also now new forms of unacceptable behaviour, such as cyber-stalking and harassment[43] and an increasing concern about "identity theft." A report of the United Nations Commission on Crime Prevention and Criminal Justice noted:

> "The field of high-technology and computer-related crime continues to be characterized by rapid evolution on the part of offenders, preventive, legislative and law enforcement efforts and the underlying technologies themselves. …Legislative reforms included the creation of new offences, the expansion of existing offences and the modernization of investigative powers such as search and seizure and wiretapping authority to deal effectively with crime in the new electronic environments." [44]

[43] For example, someone may post an internet notice seeking partners for a particular (unusual) sexual act, listing the victim's name and home telephone number. There is no direct contact between the harasser and the victim, yet the reputational damage and inconvenience to the victim may be considerable.

[44] "Effective measures to prevent and control computer-related crime," 29 January 2002, E/CN.15/2002/8

7.3.3 Most governments find that a combination of approaches will be necessary to effectively combat cyber-crime. The provisions in modern penal legislation generally provide sufficient safeguards against traditional crimes, such as theft or fraud, committed with the aid of a computer. While the e-legislation initiative may provide an opportunity to update certain provisions in the *Penal Code*, it is likely that the theft and fraud provisions are adequate. Computers and electronic communication, however, present particular problems with respect to investigation and the gathering of evidence, especially in an era of rapidly changing technology. Traditional investigative techniques relied heavily on paper documents and pre-digital telecommunication. These issues will be discussed in further detail below with respect to "lawful access."

7.3.4 Traditional criminal law concepts (including underlying concepts of "property" and "value") may need adjustments, however. The law may not recognise that a particular configuration or arrangement of electromagnetic impulses is corporeal and capable of being destroyed. In fact, it may have considerable value that is not recognised simply by recognising the lost value of a computer that has been destroyed or tampered with. It may be necessary to amend legislation to recognise the value of data. For example, the Canadian *Criminal Code*[45] was amended in 1985 to create an offence of mischief in relation to data where a person wilfully and without colour of right or lawful excuse alters or destroys data or renders it useless, meaningless or ineffective or interferes with its lawful use or access. The provision also covers the alteration of data or "denial of service," where the objective is to disable a target system rather than necessarily gain access to it. Such a legislative provision probably could also be used to deal with the introduction of a virus into a system or network, but more explicit legislation may be desirable. The federal *Computer Fraud and Abuse Act* [46]in the United States protects computers that "facilitate interstate and international commerce and communications."[47] For example, it is a crime to access a computer without or in excess of authority to obtain financial information from a financial institution or any information in the possession of the government. Similarly, the Act creates a crime to knowingly cause the transmission of a computer program, information,

[45] R S.C. 1985, c. C-46, as amended, s. 430. Part of the importance of this provision hinges on the statutory definition of "property" in the provisions dealing with crimes against property.
[46] 18 U.S.C. ss. 1030.
[47] Because of constitutional limitations, much of the American cyber-crime legislation is found at the state level; see, Susan W. Brenner, "State Cybercrime Legislation in the United States of America: A Survey," (2001) VII *Richmond Journal of Law and Technology* 28 at www.richmond.edu/jolt/v7i3/article2.html

code, or command that results in unauthorised damage to a protected [under the Act] computer.

7.3.5 Botswana legislation, specifically the *Telecommunications Act* and the *Botswana Telecommunications Corporation Act*, prohibit interference with the networks. This legislation should be reviewed to ensure that it is sufficiently broad or, alternatively, these provisions should be superseded by more general legislation.

7.3.6 The model that should serve as the beginning of an examination of Botswana legislation in relation to cyber-crime is the Council of Europe *Convention on Cybercrime*,[48] which came into force on 1 July 2004. Thirty-one countries, including South Africa, have signed the Convention; seven have ratified it. The Convention itself does not create substantive criminal law offences or set out detailed legal procedures. It deals with offences committed through the use of telecommunications networks, e.g., the Internet, such as illegal money transactions, offering illegal services, violations of copyright, and offences that violate human dignity and the protection of minors (see discussion, below, relating to inappropriate content). The Convention calls for the criminalisation of certain offences relating to computers, the adoption of procedural powers to investigate and prosecute cyber-crime, and the promotion of international cooperation through mutual legal assistance and extradition.

7.3.7 Domestic national legislation will be required to fully implement the Convention and the Convention does raise a number of issues that would require careful consideration and analysis before legislation is drafted. For example, the Convention requires mutual assistance among jurisdictions, a matter that is both laudable and necessary for effective enforcement in a globalised information economy. In particular, ratification of the Convention implies a requirement to ensure intercept capability in the domestic and international infrastructure, and search and seizure provisions that would allow for production orders and data preservation orders (discussed at greater length, below, dealing with "lawful access"). There are criticisms, however, that the Convention provisions might require assistance to investigate behaviour that is not criminal in the country being requested to cooperate.

7.3.8 The Australian *Cybercrimes Act of 2001*, for example, implements some provisions of the Convention following a review and creation of a Model Criminal Code. The Act creates offences for unauthorised access,

[48] Conventions.coe.int/Treaty/en/Summaries/Html/185.htm

modification or impairment of data to commit a serious offence; unauthorised modification of data to cause impairment; unauthorised impairment of electronic communication; possession of data with intent to commit a computer offence (similar to the idea of possessing burglary tools); supplying data with intent to commit a computer offence; unauthorised access to restricted data; and unauthorised impairment of data held in a computer disk, credit card, etc.

7.3.9 An important issue when reviewing legislation to consider whether all the tools are in place to deal with an emerging electronic environment is "inappropriate content." While there may be debate about what exactly constitutes "inappropriate" content on the Internet, there is general agreement that such content exists. The concept is also not new, as a long history of censorship and restrictions to literary texts shows. The European Union, however, has published examples of illegal or harmful content that may affect the following interests:

- Matters dealing with national security (e.g., instructions on bomb-making, illegal drug production);
- Protection of minors (e.g., abusive forms of marketing, violence, pornography);
- Protection of human dignity (e.g.,incitement to racial hatred or other discrimination);
- Economic security (e.g., fraud, instructions on identity theft);
- Information security (e.g., malicious hacking);
- Protection of privacy (e.g., unauthorised communication of personal data; electronic harassment);
- Protection of reputation (e.g., libel, unauthorised comparative advertising);
- Intellectual property (e.g., unauthorised distribution of copyrighted works, software or music).[49]

7.3.10 It should be noted that harmful content may not necessarily be illegal nor may it be harmful in all circumstances. The protection of minors, for example, is an important concern in dealing with harmful content and a similar concern may apply to other media—movies, computer games, books, photographs, or even highly persuasive advertising. In some cases, there are also strong competing values of intellectual freedom and fears of censorship to consider in creating a regulatory regime.

7.3.11 One aspect of control of "inappropriate" content will no doubt be the application of the *Penal Code* or other regulatory legislation, such as the

[49] European Union, Communication from the Commission, *Illegal and harmful content on the Internet*, November 16, 1996; http://www2.echo.lu/legal/en/internet/content/communic.htm

Copyright and Neighbouring Rights Act. It may be necessary, however, to review legislation to ensure that the full range of behaviours to be targeted is dealt with under the appropriate legal regime. For example, in Canada, amendments were made to the *Criminal Code* to deal explicitly with exploitation of children through the dissemination of child pornography over the Internet. Thus new provisions created crimes for:

- Internet luring, making it illegal to communicate with a child over the internet for the purpose of committing a sexual offence against that child;
- Transmitting (distributing) child pornography over the Internet;
- Making child pornography available by posting or offering information on where to find it on the Internet;
- "Exporting" child pornography across national borders (this provision fulfils Canada's obligations under the Optional Protocol to the United Nations Convention on the Rights of the Child, on the Sale of Children, Child Prostitution, and Child Pornography); and
- Possessing child pornography for the purposes of transmitting, making available or exporting.

7.3.12 In addition, the Canadian amendments provide courts with the power to order *ex parte* a custodian of a computer system (e.g., an Internet Service Provider) to remove from its server any material that could reasonably be considered to be child pornography. In addition, a judge may order forfeiture of any materials or equipment used in the commission of a child pornography offence. The EU *Convention on Cybercrime* (which must be operationalised through national criminal law) also states that possession, copying and distribution of child pornography should be penalised.

7.3.13 The European Commission against Racism and Intolerance of the Council of Europe has also adopted a General Policy Recommendation on combating the dissemination of racist, xenophobic and anti-Semitic material on the Internet, which recommends inclusion of an additional protocol in the Convention on Cybercrime.[50]

7.3.14 Establishing a structure or framework to deal with inappropriate content pre-supposes that there is some acceptable definition as to what is unacceptable, at least in certain circumstances (e.g., to minors). Generally, reference is made as to what is considered acceptable or unacceptable in the physical offline world. Indeed, this applies to cyber-crime generally: fraud perpetrated through the Internet via e-mail should not be treated differently as a matter of substantive criminal law and procedure than fraud perpetrated through, for example, the mail

[50] http://www/ecri.coe.int/en/08/02/06/Rec%206%20en.pdf

("snailmail"). Distribution of racist literature through the Internet is as unacceptable as distribution by hand or through the mail; similarly, distribution of child pornography or "snuff" films is unacceptable irrespective of the medium of distribution. In this sense, Botswana, like other countries, should look to its general criminal law and social policies for guidance on dealing with Internet content. In a number of cases, existing legislation is sufficient to deal with the issues of illegal (as opposed to unacceptable—to some) content. The policy question is how to identify and communicate information about content to users, as well as enforcement of existing legislative provisions regarding illegal content.

7.3.15 Censorship has been attempted in some jurisdictions (e.g., South Korea through its *Electronic Communications Business Law*, which established the Information and Communication Ethics Office), but a more general approach has been the development of self-regulatory or co-regulatory systems[51] that place responsibilities on the various players, particularly Internet Service Providers.[52]

7.3.16 The EU has put in place an Internet Action Plan which focuses on self-regulation, supports a network of hotlines where offensive content can be reported, benchmarks content filtering and rating, and supports a European network of safer internet awareness centres. The Safer Internet Directions for 2003-2004 extend to new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real time communications, such as chat rooms and instant messages. A study of the implementation of the Internet Action Plan[53] has indicated that adequate resourcing is key to successful self-regulation and that significant economies of scale can be realised through the functional integration of key aspects of content regulation

[51] Self-regulation is defined in this context to mean a scheme under which bodies draw up their own regulations or rules to achieve certain objectives and take full responsibility for monitoring and enforcing compliance with the rules. Participation is generally voluntary and the rules often take the form of industry codes of conduct. Co-regulation is based on a self-regulatory framework except that a state authority either lays down the basis for the self-regulatory framework, providing it with the authority to function and potentially enforce its activities, or integrates the self-regulatory framework into an existing public authority framework. There are a number of possible co-regulatory combinations of industry and public authority. Germans often use the term "regulated self-regulation" for co-regulation, which is the common European and Australian term.

[52] See Decision No 276/1999/EC of the European Parliament and European Council of 25 January 1999, Official Journal L 033, 06/02/1999

[53] A report of the self-regulatory regime in Europe from 1999 to 2004 can be found at the Oxford University Centre for Socio-Legal Studies, Programme in Comparative Media Law & Policy, "Self-regulation of Digital Media, Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis," 30 April 2004.

across sectors and across EU Member States. Computer games-rating, for example, has the potential for developing into a pan-European structure. Clear procedures for auditing self-regulatory structures are required, however.

7.3.17 The Australian co-regulatory scheme is found in the *Broadcasting Services Act*, which now addresses risks associated with illegal content and with content that is unsuitable for children. The scheme is based on the development of codes of practice by industry and the operation of a complaints hotline by the Australian Broadcasting Authority (ABA). The codes, which govern Internet Service Providers and Internet Content Hosts, were developed by the Internet Industry Association in consultation with the community, industry and a community advisory body, NetAlert. The codes apply to all Australian ISPs and ICHs and the ABA may direct an ISP or ICH to comply; failure to comply with an ABA direction constitutes an offence under the *Broadcasting Services Act*. The codes require such matters as encouraging Content Providers to use appropriate labelling systems, and providing information to users about procedures that parents can use to control children's access to Internet content through the use of filtering software and labelling systems. The ISPs themselves are not required to classify or censor material and are protected from legal action from content providers whose material has been blocked if they were complying with a code or an ABA direction. Similarly, ICHs are protected from legal action from content providers or civil proceedings in respect of anything they have done in compliance with the code or an ABA direction.

7.3.18 A co-regulatory approach has a number of attractions for Botswana. There are strong international models, particularly in Europe and Australia/New Zealand, on which Botswana can rely. Indeed, as noted, in some cases, it would be possible to adopt or adapt ratings systems that are already in place, such as those for computer games. A co-regulatory approach is likely to be more flexible and allow for technological flexibility, an advantage in an area where convergence and rapid change are important factors. At the same time, a "softer" regulatory hand may allow for fuller consideration of the competing values and interests that are at play in matters of "inappropriate" content. In addition to preventing, investigating and prosecuting unlawful conduct (such as exploitation of children or incitement of hatred), society has an interest in promoting free speech, artistic expression, providing broad access to information from around the world and domestically, protecting reasonable expectations of privacy, and supporting legitimate commerce and personal relationships.

7.3.19 While the issue arises in dealing with illegal or inappropriate content or with the new types of crime that electronic communication fosters, the form and procedures for lawful access are important in combating crime of any nature. Not surprisingly, lawful access provisions are among the most controversial in the fight against cyber-crime and for policing authorities operating in a cyber-environment. "Lawful access" or authorised access refers to how law enforcement agencies will intercept and search and seize electronic information. This applies, of course, not only to information about cyber-crime, but also to information about other criminal activity. Lawful, in the sense of being authorised, access is an essential tool to criminal investigations (and, with appropriate safeguards, regulatory investigations) and "wiretapping" has been used for scores of years. National security concerns have raised the importance and profile of these issues. In jurisdictions operating with a strong tradition of the Rule of Law, independent authorisation (often from a court) is required for information interception. Rapidly changing technologies, however, create a significant challenge to authorities wanting to carry out effective investigations.

7.3.20 The implementation of Maitlamo is intended, among other objectives, to draw investment and business to Botswana. It is important, therefore, that the Government look to international norms in establishing any new regime for lawful access. These include independent authorisation of interception and mechanisms for accountability for activities or behaviour that intrudes on the privacy of citizens and businesses operating in Botswana.

7.3.21 The EU *Convention on Cybercrime* does not require any specific lawful access procedures since the Convention will be implemented through domestic European legislation. It does, however, deal with procedural powers relating to data preservation, production, search and seizure, and real time collection. There are some fine distinctions of language that must be considered in developing any Botswana policies that rely on the Convention; for example, preservation of data means to keep data that already exists while retention of data means to keep for the future data that is currently being generated. One can certainly see situations where either or both powers would be useful or necessary, but lawful access provisions such as these have implications for network design and costs to ISPs and others in the system that need to be considered in policy development. It is also important to remember that communication data collection (e.g., e-mails) always involves intrusion on at least two parties, one of whom may be entirely innocent of any suspicion of wrongdoing. There may also be different levels of information that can be obtained: for example, the name of a URL versus the data on the URL itself.

7.3.22 Australia has developed a means of clearly setting out the responsibilities of Internet Service Providers to respond to requests for authorised access by law enforcement authorities. The Internet industry, working in cooperation with law enforcement agencies, developed a Cybercrime Code of Practice.[54] The Code sets out the sort of customer-related personal data the ISPs would be expected to retain and thus make available to authorities: name, address, e-mail address, billing records, type of service, credit card data if collected, and other information collected on an application for service. It identifies the operational data that the ISP would be expected to retain, as well as other data if collected. Minimum retention periods are set out, as well as what responses to warrants would be required. Evidence collection and handling guidelines are also established.

7.3.23 Canada is in the process of implementing new provisions for lawful access, primarily through *Criminal Code* amendments. Canada has signed the Convention but has not yet ratified it. The U.K. has passed the Regulation of Investigatory Powers Act 2000 that compels assisted disclosure of encrypted data and passwords; its stated target is child pornography and human trafficking. There has been a strong international push following the attacks on September 11th in the United States for increased policing capacity to investigate crime and terrorist activity that has resulted in more extensive lawful access provisions. The *U.S.A. PATRIOT Act, 2001*[55] deals with lawful access to traffic data over all media, including cable. It limits judicial oversight of electronic surveillance, removing probable cause requirements and requiring judges to authorise requests and implements roving wiretap orders. Its provisions have been widely criticised as abuses of civil liberties and may be subject to adjustment in the future.

7.3.24 The South African *Regulation of Interception of Communications and Provision of Communications-Related Information Act, 2002* ("*Interception and Monitoring Act*") sets out a complex regime relating to lawful access, prohibitions on access by unauthorised persons, exceptions (e.g., to prevent serious bodily harm or locating an individual in case of an emergency), real-time and archived information, provision of warrants, and assistance to be provided by service providers. The Act also prohibits the provisions of telecommunications services that do not

[54] Internet Industry Association, *Codes for Industry and Self Regulation and Rules of Engagement with Law Enforcsment Agencies in Respect of Investigation Procedures Regarding Online Fraud and Other Criminal and Terrorist Activity*, Public Consultation Draft 2.0, July 2003; www.iia.net.au

[55] Public Law No. 107-56, 115 Stat. 272.

have the capability to be intercepted and sets out what costs are to be borne by the service providers, who must establish "interception centers," Certain cryptography technology is permitted. The Act has been subject to criticism as being too broad, intrusive and without sufficient provisions for oversight.

7.3.25 Botswana's legal and regulatory structure dealing with privacy, data protection, and data security should also take into account the growing problem of data theft. Countries with high levels of credit card use are particularly concerned about this emerging problem, but Botswana's aspirations to be a financial services centre and a centre for tourism will require that consumers and businesses have assurances that their personal and financial information will not be used or "stolen" for unauthorised use.

7.4 Recommendations:

- The Attorney General's Chambers in consultation with stakeholders such as the Directorate on Corruption and Economic Crime, the Law Society, the Bank of Botswana, the Botswana Stock Exchange, the Botswana Telecommunications Authority, Internet Service Providers and the Botswana Telecommunications Corporation and other telecommunications service providers, review the *Penal Code*, taking into account such examples as the EU Convention on Cyber-Crime, to ensure that adequate legislative criminal law authority exists to deal with such matters as:
  - Content-related crimes, such as child pornography disseminated through the Internet by users within Botswana
  - Illegal access to data and computer systems
  - Recognition of the value of data
  - Misuse of devices that can be used for illegal access or manipulation of data and computers systems
  - Cooperation with foreign authorities to deal with enforcement of extra-territorial criminal activity, including child pornography

- The Ministry of Communications, Science and Technology, in consultation with the Botswana Telecommunications Authority, the Botswana Telecommunications Corporation and other telecommunications service providers, the Internet Service Providers, Internet Content Hosts, the Botswana Police, the Directorate on Corruption and Economic Crime, and the Ministry of Trade and Industry, the Ministry of Education, the Law Society, groups representing arts and entertainment industries, and civil liberties groups explore:
  - Fostering a vibrant and cohesive industry organisation of Internet Service Providers and Internet Content Hosts who can work

together with Government to develop and administer a regime of co-regulation to deal with inappropriate content and authorised access.

- Similar arrangements can be made with telecommunications service providers operating under the authority of the Botswana Telecommunications Authority.

- The Ministry of Communications, Science and Technology, in consultation with the Ministry of Education and stakeholders such as education leaders, parent groups, importers, retailers, and arts and entertainment industries examine the development of a rating system for computer games and similar electronic content that may be inappropriate for certain ages or in certain circumstances.

- The Minister responsible for policing ensure the establishment of a specific cyber-crime unit in police authorities; training of police authorities in cyber-crime issues and resourcing of computer experts as necessary.

- The Attorney General's Chambers, in consultation with policing authorities, citizen groups, the Law Society, the Directorate on Corruption and Economic Crime, the Botswana Telecommunications Authority, Botswana Telecommunications Corporation and other telecommunications service providers, Internet Service Providers, civil liberties groups, and other interested stakeholders, review provisions for lawful access and develop proposals to deal with lawful access in an electronic environment.

8.0 Ancillary Matters

8.1 Objective:

- Ensuring that the legal and legislative policy environment in Botswana continues to move forward to meet the objectives of Maitlamo.

8.2 Issues:

- Ensuring that the tax structure does not either lose revenue from e-commerce transactions with a sufficient taxation nexus to Botswana or, conversely, does not double tax transactions and thereby discourage use and innovation.
- Ensuring that the Botswana intellectual property regime remains not only up-do-date in an evolving connected world, but also is appropriately enforced to encourage innovation and creative efforts.

- Meeting the demand for access to Government information through a structured regime that both creates rights of access and provides adequate protection for personal and commercial privacy.
- Ensuring that legislation and policies remain technology neutral or, in the alternative, where a technology is favoured, that it is done after careful analysis of the costs and benefits.
- Examining the use of the .bw domain and ensuring that adequate dispute resolution mechanisms are in place regarding domain allocations.

8.3 Discussion:

8.3.1 The Legal and Policy Task Force identified selected priorities, which are outlined above. These priorities were identified taking into account the objectives and priorities of the other Task Forces. For example, both the Health and the Economic Development Task Forces stressed the importance of establishing a regime for secure electronic signatures in order to move their recommendations forward. The discussion in this Annex deals with the identified priorities, as well as with some related items, such as security and cyber-crime. There are a number of other issues that will have to be dealt with in time, however.

8.3.2 A procedure should be put in place to ensure that these issues remain in Government Action plans as medium to longer-term matters. This is not to say that there are necessarily less important in many ways than the matters initially identified for action, but only that a realistic assessment of resources and capacities requires that priorities be established.

8.3.3 The Government may wish to consider requiring Ministries that put forward recommendations for legislation, policies, or procurement to justify any decisions that can be seen to limit technological innovation by moving away from, e.g., technological neutrality.

8.4 Recommendations

- The Inter-ministerial Legal Reform Task Force coordinate and implement the policy and legislation required to fulfil the initial tasks identified by the Legal and Policy Task Force; in addition, the Legal Reform Task Force be asked to develop medium-term plans (2 to 6 years) to explore policy and legislative development in other ICT-related areas.
- The Ministry of Communications, Science and Technology report to the Inter-Ministerial Legal Reform Task Force for inclusion in their first six-month report to Cabinet the progress that has been made regarding telecommunications liberalisation, including providing a transparent process for spectrum allocation and dealing with issues of the convergence of telecommunications and broadcasting.