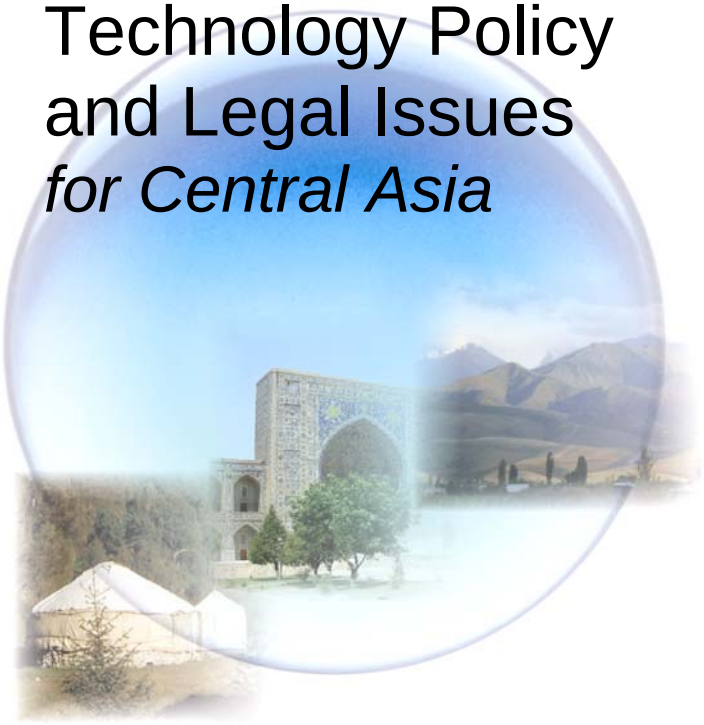
United Nations Economic Commission for Europe

Information and Communication Technology Policy and Legal Issues *for Central Asia*



Guide for ICT Policymakers

UNITED NATIONS
New York and Geneva, 2007

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

ECE/CECI/1

Printed at United Nations, Geneva (Switzerland)

UNITED NATIONS PUBLICATIONS

***Sales No.* 07.II.E.21**

ISBN: 978-92-1-116974-4

FOREWORD

The development of information and communications technologies (ICTs) enables businesses and individuals to communicate and engage in transactions with other parties electronically, instantaneously and internationally. This gives rise to a variety of legal and regulatory issues for policymakers, from the validity of electronic methods of contracting and the security risks associated with them, to concerns over cybercrime and the ability to protect intellectual property rights online. ICT policymakers are constantly facing challenges in dealing with these issues. The promotion of harmonized law reforms, which would facilitate the sound development of eCommerce and related activities, that citizens have appropriate protection against harmful behaviour, is a way to address these challenges.

This guide has been prepared at the request of the Project Working Group on ICT for Development, created in December 2005 within the framework of the United Nations Special Programme for the Economies of Central Asia (SPECA). SPECA was launched in 1998 to strengthen subregional cooperation in Central Asia and its integration into the world economy. The United Nations Economic Commission for Europe (UNECE) and the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) provide technical assistance to the implementation of projects agreed upon by its members. The member countries of SPECA are Afghanistan, Azerbaijan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan. The guide is intended for use as a reference manual by ICT policymakers in countries with economies in transition. The content is designed to respond to the needs of SPECA member countries, incorporating feedback received during the series of capacity-building events conducted in 2006 and 2007.

UNECE is strongly committed to capacity-building activities in the countries with economies in transition, including projects targeting ICT policymakers, so that the countries can realize the full potential of the innovations in the ICT-related areas in supporting their knowledge-based economic development. It is our hope that this publication will contribute to that end.

Marek Belka
Executive Secretary
United Nations Economic Commission for Europe

ACKNOWLEDGEMENTS

This publication is one of the outcomes of the UNECE technical cooperation project, *Capacity-building for ICT policymaking* aimed at strengthening the capacity of ICT policymakers in Central Asia, implemented by the Economic Cooperation and Integration Division. The preparation of the publication was led by Michiko Enomoto. The guide was drafted by Professor Ian Walden (consultant) and Laura Edgar from the Institute of Computer and Communications Law, at the Centre for Commercial Law Studies, Queen Mary, University of London. Substantive comments were received from Andrey Vasilyev, Roumen Dobrinski, Michiko Enomoto, Geoffrey Hamilton and Hans Hansel. General support and formatting was provided by Tatiana Apatenko and Victoria Goudeva, the cover was designed by Yves Clopt and the text was edited by Alison Mangin.

The financial support from the United Nations Development Account is gratefully acknowledged.

CONTENTS

ABBREVIATIONS

CIS	Commonwealth of Independent States
EBRD	European Bank for Reconstruction and Development
EDI	Electronic data interchange
EU	European Union
GATS	General Agreement on Trade in Services
ICANN	International Corporation for Assigned Name and Numbers
ICT	Information and communication technology
IPR	Intellectual property rights
ISP	Internet Service Provider
IT	Information technology
OECD	Organisation for Economic Cooperation and Development
PICS	Platform for Internet Content Selection
PIN	Personal identification number
RCC	Regional Commonwealth in the field of communications
SPECA	United Nations Special Programme for the Economies of Central Asia
UNCITRAL	United Nations Commission on International Trade Law
UNDP	United Nations Development Programme
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
WTO	World Trade Organization

EXECUTIVE SUMMARY

The development of information and communications technologies (ICTs) enables businesses and individuals to communicate and transact with other parties electronically, instantaneously and internationally. This gives rise to a variety of legal and regulatory issues for policymakers, from the validity of electronic methods of contracting and the security risks inherent in them, to concerns over cybercrime and the ability to protect intellectual property rights online.

This guide examines distinguishes ICT legal issues into five distinct areas:

- **Legal infrastructure**, which considers some of the key legal and regulatory facilitators for electronic commerce, from adherence to law reform principles such as 'technology neutrality', to regulatory structures and market liberalization.

- **Legal certainty**, which examines the legal status of electronic communications and forms of contracting, specifically the need to **explicitly** recognise the validity, enforceability and admissibility of electronic means of executing legal acts.

- **Legal security**, which examines the security risks inherent in an electronic environment and considers the methods used to **overcome** these, in particular the use of digital signatures and certification services.

- **Legal protection**, which reviews **intellectual** property rights and how such intangible property is protected in an online environment, as well as the consumer protection issues which the Internet raises.

- **Legal deterrence**, which examines the development of cybercrime and the regulatory approaches to criminalising such **harmful** conduct and ensuring that law enforcement are able to investigate and prosecute offenders.

The guide examines the legal issues raised in each of these areas and highlights relevant developments and best practice initiatives at an international level, such as the UNCITRAL model laws and the 2005 Convention, and regional level, particularly the European Union; as well as within the seven SPECA member countries: Afghanistan, Azerbaijan, Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan.

The guide concludes by making recommendations to the SPECA member countries about how to facilitate the law reform process with respect to ICT issues.

I. LEGAL INFRASTRUCTURE FOR ICT

It is well-established that economic development is dependent on a country having appropriate infrastructure to facilitate such development. It should also be recognized that the legal and regulatory framework of a country comprises one element of such an infrastructure. This section briefly reviews these areas, highlighting international developments.

A. Legal principles

Translating policy objective into workable laws and regulations can obviously be a difficult task in any area of human endeavour; technology however presents particular challenges to law-makers, primarily due to the pace of change that occurs in the subject matter itself, e.g. software, computers and networks, and the manner in which such technology is utilized. The limits of our imagination are as manifest in our ignorance of where the technology is developing as it is about how it will be taken-up by users. Much has been written about the nature of regulation in an environment of ubiquitous information, computers and networks.

In response to the challenges, policymakers have attempted to discern principles that can guide regulatory initiatives in the field. The leading, most oft-quoted, regulatory principle is that of "technology neutrality". Much reference and deference is made by policymakers to the concept of "technology-neutral" regulation, based on an acceptance that the environment is moving too rapidly to try and tie legal rules to a particular technology or market model. The principle, and variants of it, has been used in two key senses: that which is regulated off-line should be regulated on-line; as well as the need to treat different technologies similarly to the extent that they have the same effect[1]. However, disputes exist about the manner in which the principle should be applied when considering substantive law and procedural law reform.

The principle also fails to provide help to policymakers when making the choice between different regulatory models. The Internet, for example, is the perfect example of the convergence phenomenon, with different forms of content being transmitted across interconnected networks using a common protocol. But whether the IT/telecoms model or the broadcasting model of regulation should apply to the content being transmitted continues to test policymakers and regulators.

Coupled with technology neutrality, the declaration of the World Summit on the Information Society (WSIS) calls for policy and regulatory frameworks to be "pro-competitive" and that government intervention should only occur for limited and clearly necessary purposes. Within the WSIS process, competition in the marketplace is accepted as the primary regulator of market participants, with governments intervening where market failures arise and to maintain fair competition.

A range of other principles have been proposed, although with varying levels of support among governments and the public. Open source software, for example, is seen by some as not simply an alternative to the major proprietary software packages on the market, but part of

[1] See Koops, B-J., "Should ICT regulation be technology-neutral?", in Koops, B-J., *Starting Points for ICT Regulation*, Cambridge, 2006.

a broader movement against the use of copyrights laws as a means of restricting the free exchange of information. The need to promote a public "commons" of information is seen as key tool that can better foster the generation of future creative works than the environment created by the "all rights reserved" approach of traditional copyright.[2] Recasting intellectual property in an information economy environment in terms of open systems and open code is seen as having particular benefits for developing countries, unable to afford and police developed nation-style intellectual property regimes.

Layered on top of the principles that have emerged in respect of law reform in the Information and Communication Technology (ICT) sector, there are generic principles against which laws are traditionally assessed and evaluated, especially in respect of criminal matters. Legal transparency, for example, demands that those made subject to the law are aware, or have the possibility of becoming aware, of the rules applicable to a particular activity. Under European human rights law, transparency is one element of the requirement that restrictions on a person's rights be "in accordance with the law".

In our increasingly global economy, one crucial factor including the level foreign direct investment in a sector is the perceived certainty regarding the governing legal and regulatory framework. The greater the degree of instability in the legal and regulatory framework, both real and perceived, the greater the legal uncertainty and the consequential disincentives to investment. Legal certainty extends from the law-making process, to its implementation and enforcement. Investors will be particularly concerned with any discretionary decision-making process, carried out by ministers, ministries, regulatory authorities and judicial bodies. The exercise of discretion is an inevitable feature of all legal systems, but it must be subject to certain controls and limitations.

Closely related to certainty, is the demand that laws be sustainable. Sustainability can be seen as having two key aspects. Firstly, the length of time that a set of legal rules remains workable in terms of meeting the policy objectives in the environment in which it operates. Secondly, that the rules are enforceable against the prohibited conduct. While enforceability in any area of law is never attained, particularly in a cyberspace environment of multiple and conflicting jurisdictions, a large-scale inability to enforce undermines the value of any set of legal rule.

[2] http://www.creativecommons.org

B. Regulatory structures for ICT and actors

The role of government is to govern and, generally, to pass laws and adopt regulations designed to control certain forms of activity. It is broadly recognized, however, that governance and regulation extends beyond governments to encompass a broad range of institutions and mechanisms of control. For example, in some sectors, such as telecommunications, international best practice is to establish an independent regulator to oversee the competitive liberalization of the sector, a key infrastructure and driver behind electronic commerce development.

Effective regulatory institutions require adequate expertise and resources, which developing countries may find difficult to support. To address such barriers, capacity building in the regulatory field is a line of activity in most developmental programmes, including training and exchange programmes with developed nation regulatory institutions. However, such formal institutions can also be supported by non-public sector entities, both commerce and civil society, which can operate in a regulatory capacity, whether directly or indirectly. Self or co-regulation, for example, looks to industry to establish, monitor and enforce rules over its members.

While we traditionally conceive of regulation in terms of laws and rules, we must also be aware of other processes occurring at a national and international level that effectively regulate the way a society embraces the manifestations of the Information Economy. The standards and protocols that underpin the operation of the Internet and its various services, from email to VoIP (Voice-over-Internet Protocol), for example, facilitate or restrict the way we interact with such technologies, either through deliberate design, as an inevitable by-product or by accident. Market conditions govern the way we use the Internet; the cost of telephony, for example, limits our usage when operating on a time-sensitive basis. Cultural norms also determine how people use and abuse the Internet as a means of communications and economic activity.

One approach to promoting and coordinating government activity towards ICT economy issues is to establish new institutional entities with a specific remit to address such matters. Both developed and developing nations have followed such an approach. In some cases, there is a need to enshrine such institutions in law, such as the Kazakhstan Agency for Information Technology Development and Telecommunications[3], to improve transparency and ensure independence from existing government departments and public authorities, which can enhance the status and stature which the institution is able to assert.

However, while independence is important, it is also necessary to ensure good cooperation and coordination between the different parts of government, which will generally include the major ministerial departments responsible for finance, revenue and trade. In addition, however, political support will often be key, especially in the face of competing political priorities, which may require that such an institution should be associated with the key political actors in a country.

[3] Established in 2003 and taking over functions and authority previously held by a committee within the Ministry of Transport and Communications.

The Digital Opportunity Initiative[4], a public private partnership of Accenture, the Markle Foundation and the United Nations Development Programme (UNDP), in its report, *Creating a Development Dynamic*, recognizes the importance of involving all stakeholders in an ICT development strategy, from the public and private sectors, civil society and international organizations, which they label "strategic compacts", both at the design and implementation phase.

Allied to the operation of competition as a regulatory principle is the idea of self-regulation, where suppliers of products and services in the ICT sector are left to regulate their own behaviours, or at least co-regulation, through a partnership between government and industry. Governments' increasing willingness to rely on self-regulation on a general level reflects a range of different drivers, from acceptance of the overwhelming complexities of modern commerce, to a concern to reduce the cost to public finances. In the ICT sector, such drivers are supplemented by a broad recognition that the Internet and its associated services developed to its current state relatively absent from substantial intervention from governments.

One element of self-regulation is the role of standards in all aspects of Internet activity. In addition to standards related to the technological elements of electronic commerce systems, industry standards have also been developed in respect of the content being transmitted. The Platform for Internet Content Selection (PICS)[5] specification, for example, has been developed to enable labels to be associated with particular types of Internet content. It was originally designed to enable parents to prevent their children accessing content deemed unsuitable. In the fields of consumer protection and privacy, electronic commerce-labelling schemes have been developed to provide users with a visual indicator of compliance with certain minimum standards of protection. Such schemes may include dispute resolution procedures designed to improve individual enforcement of rights.

In terms of enforcement, industry-funded bodies have been established to monitor and report Internet-based activities for certain types of illegal content, from material infringing intellectual property rights, which are generally enforced through civil action, to child pornography, a matter of criminal law (e.g. the Internet Watch Foundation)[6].

Self-regulation does, however, raise certain issues in respect of legitimacy. Through adopting self-regulatory schemes, legislators may be seen as abdicating themselves of the functions conferred upon them through the democratic process. Accountability and oversight also needs to be ensured, to prevent conflicting commercial interests from superseding the policy objectives underpinning the regulatory scheme over time.

Whether governments adopt a distinct or self/co-regulatory approach to ICT issues, the cost of regulation will clearly be a critical factor, specifically the establishment of a dedicated entity being excessive for many developing countries without assistance from development organizations. Whilst a self-regulatory or co-regulatory approach may be appealing in terms

[4] http://www.opt-init.org/
[5] http://www.w3.org/PICS/
[6] http://www.iwf.org.uk

of minimizing the public costs of regulation, its success depends on a sufficiently strong and active private sector, willing and able to fund the regulatory activity. To mitigate the costs involved, the entity may be able to coordinate other revenue generating activities related to electronic commerce. Country level domain name administration, for example, provides a potential source of licence revenues.

C. Sector liberalization

From a regulatory perspective, liberalization involves the opening up of the sector to competitive forces. While the Internet as an environment for economic activity is seen as extremely competitive, the means by which citizens gain access to the Internet may be considerably less competitive. In particular, the telecommunications market is a key enabler in the growth and development of electronic commerce.

At an international level, liberalization of the telecommunications sector has been driven primarily through the World Trade Organization (WTO), under the auspices of the General Agreement on Trade in Services (GATS), the Telecommunications Annex and the Reference Paper[7]. Of the members of the United Nations Special Programme for the Economies of Central Asia (SPECA), only Kyrgyzstan is a WTO member and has formally committed to full liberalization of its telecommunications sector[8]. However, the other SPECA member countries have made substantial strides in the sector through assistance from developmental funding, particularly from the European Bank of Reconstruction and Development (EBRD), which has extended to law reform initiatives as well as more traditional financing activities, in recognition that a modern regulatory framework serves to attract private investment into the sector[9]. Kazakhstan's Law on Communications[10] is an example of such sector liberalization.

The GATS is concerned with four modes of supplying services: (a) from one territory to another, i.e. cross-border supplies, (b) the provision to foreign consumers in the service providers territory, i.e. consumption abroad, (c) the establishment of a commercial presence in the another state, and (d) through the presence of a natural person in another state[11].

Under the GATS, member states' specific obligations address the role of "domestic regulation" (Article VI). First, there is a general requirement that all measures be administered in a "reasonable, objective and impartial manner". Second, it requires that "judicial, arbitral or administrative" bodies and procedures be established to provide service suppliers with an opportunity to appeal against decisions that have an impact on trade in services. Third, authorization procedures, which an entity is required to complete prior to engaging in a specified activity, should be completed "without undue delay". Fourth, recognition is given to the role of technical standards in the regulation of activities, and obliging member states not to adopt standards that are more burdensome that are necessary, lack transparency and are subjective in nature.

---

7 See further http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm

8 As from 1 January 2003.

9 See EBRD Report, Telecommunications, Informatics and Media, January 2000.

10 Dated 5 July 2004.

11 GATS, Art. I(2).

One element of the process of liberalizing the telecommunications sector is the authorization and licensing process. The more complex and time-consuming the process of obtaining a licence from government granting the right to supply a service, build a facility and related matters, the greater the obstacle to market entry, whether from national or international competitors.

However, the telecommunications sector is not the only area where issues of authorization and licensing arise. In some countries, the right to import, market, connect and maintain various categories of ICT equipment may be made subject to authorization and licensing regimes, which can operate as non-tariff trade barriers. While the justification for such a regime may be perfectly sound in terms of preventing identified harms, such as public safety, and other non-economic public interest objectives, the manner in which such schemes often operate may create obstacles to ICT development, such as the time and/or cost of obtaining the appropriate authorizations and licences. The WTO has adopted a declaration on "Trade in Information Technology Products"[12], to which Kyrgyzstan has acceded, however it only provides for binding commitments in respect of tariff reductions, not non-tariff barriers.

D. Harmonizing ICT laws

In our global information economy, law reforms that are substantially out-of-step with those frameworks present in other countries may act as a significant barrier to economic development. As such, states will often be concerned to reflect regional or international best practices when reforming national laws. Several model laws have been developed since the late 1990s which may serve as a useful guide to any country amending its regulatory framework to facilitate electronic commerce. This section provides a brief overview to those Model Laws and Directives which are then discussed in further detail later in the report.

1. UNCITRAL Model Laws and Convention on electronic communications

The United Nations Commission on International Trade Law (UNCITRAL)[13] is a leading forum for legal harmonization initiatives designed to facilitate electronic commerce. Although SPECA member countries are not currently members, UNCITRAL measures have influenced law reform initiatives in the area. As far back as 1985, UNCITRAL recommended that member states review existing rules governing the use of computer records as evidence, form requirements and the acceptability of electronic submissions to public administrations[14].
The UNCITRAL Model Law on Electronic Commerce was adopted on 12 June 1996 (1996 Model Law). The purpose of this model was to facilitate the use of electronic means of communication and storage of information. The model provides a set of internationally acceptable rules whose aim is to provide for a stable and secure electronic commerce environment by removing the existing legal obstacles. The model considers the functions of the various form requirements and provides for a functional equivalent in electronic media of these paper-based concepts such as writing, signature and original.

[12] Came into force on 1 July 1997. See generally http://www.wto.int/english/tratop_e/inftec_e/inftec_e.htm
[13] See generally http:// www.uncitral.org
[14] UNICTRAL, 'Recommendation on the Legal Value of Computer Records', 1985.

By producing these rules in the form of a model law, the model can act as a guide for countries to use in preparing national legislation. The model can be modified to meet the needs of a particular jurisdiction or individual provisions can be selected as necessary instead of adopting the model as a whole. A guide accompanies the model law which provides information on the background to the model and also provides explanatory information on the provisions of the model.

When the model law was drafted in 1996 although several jurisdictions had introduced provisions within their legislation to take into account electronic means of contracting, none had yet developed a regulatory framework governing e-commerce per se. The situation is quite different a decade later. For example the model law itself has served as a basis of electronic contracting legislation in a wide range of different jurisdictions, including Australia, Bahrain, Bermuda, Canada, Columbia, Dominican Republic, Dubai, France, Hong Kong, Ireland, Mexico, Philippines, Singapore, Slovenia, the United Kingdom and the United States.

UNCITRAL also adopted a Model Law on Electronic Signatures in 2001 which expands on the electronic signature provision in Article 7 of the 1996 Model law. The model focuses on the key functions of signatures – authentication and integrity – to ensure equal treatment of signature technologies. It lays down certain requirements which a signature must meet to be considered valid and also provides for the responsibilities of certification service providers.

Although the Model laws have proved to be very useful in forming a basis, or as a reference, for many countries when developing their own model laws they do not have any formal status as legal instruments. In order to promote further reform and harmonization in the field of electronic commerce the UNCITRAL Commission therefore commissioned its Working Group on Electronic Commerce to draft the Convention on the Use of Electronic Communications in International Contracts in November 2005 (2005 Convention) and this was adopted by the United Nations General Assembly and opened for signature in January 2006.

The aim of the Convention is to enhance legal certainty where electronic communications are used in relation to international contracts. The Convention sets forth provisions on the formation and performance of contracts using electronic communications in relation to international contracts. The Convention does not therefore cover all of the issues raised in the 1996 Model law, for example it excludes issues concerning evidential value of electronic communications. It also excludes certain types of contract such as contracts for personal or family matters and certain types of financial agreement such as interbank payment systems.

2. European ICT Directives

There have also been regional developments which may prove useful guidance to SPECA member countries, particularly by the European Union.

The European Union (EU) has produced relevant Directives on e-commerce, e-signatures, data protection and distance selling[15]. These are the Directive 1999/93/EC on a Community Framework for Electronic Signatures (E-Signatures Directive) and Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (E-Commerce Directive). the Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) and the Directive (97/7/EC) on the Protection of Consumers in respect of Distance Contracts.

The Directives differ from Model laws as EU member states are required by law to implement the rules contained within the Directive in their national laws within a specific time period. The Directives do not provide for the exact language to be used in adopting the provisions but instead focus on the aim to be achieved in amending national legislation.

3. Regional Commonwealth in the field of Communications

The Regional Commonwealth in the field of Communications (RCC)[16] was set up in December 1991 by representatives from the Commonwealth of Independent States (CIS). It is a formally recognized interstate body to coordinate activities in the fields of post and telecommunications, including law reform initiatives:

> "Improvement and harmonization of normative technical and normative legal base in the field of communications and informatization of the RCC participants' countries including development of model acts in cooperation with Interparliamentary Assembly of the CIS member states taking account of international rules of law."[17]

The Interparliamentary Assembly of the CIS states has developed a model law "On e-trade", which is being finalized for submission to member state parliaments in October 2007.

[15] See generally http://europa.eu/scadplus/leg/en/s21012.htm#ECOMMERCE

[16] See generally http://www.rcc.org.ru/en/index.htm

[17] RCC, 'Strategic lines of the Regional Commonwealth in the field of communication activities", Decision No. 36/2 of 12 December 2006, at para.5.

E. Conclusions

Addressing ICT legal and regulatory issues raises some generic policy issues for a country to consider in addition to the specific concerns of a topic, such as electronic contracting or cybercrime. Piecemeal law reform may generate more problems and obstacles than it solves, therefore a comprehensive and consistent approach needs to be considered within the broader context of a nation's ICT development strategy. Such an approach needs to adopt certain principles against which law reform measures can be evaluated. In addition, consideration needs to be given to any regulatory structure required to support, supervise and enforce any obligations placed upon public or private entities. Finally, regional and international legal harmonization in an age dominated by the Internet is often a critical element in achieving the goals of law reform, helping avoid entities engaging in regulatory arbitrage between nations.

II. LEGAL CERTAINTY

This section of the guide deals with the legal validity, enforceability and admissibility of electronic communications which can hinder the adoption of, and reliance on, electronic commerce.

In many countries there are potential restrictions on the use of electronic means of communication because of the incorporation of terms into the regulatory provisions which stipulate certain requirements of form such as writing, signature and original. These form requirements within national regulations have given rise to a degree of uncertainty as to the legal validity of using electronic communications for certain purposes such as entering into contracts, sending invoices or submitting electronic evidence. Problems may arise not only on a national scale but such legal uncertainty may also seriously hinder international trade. Since electronic communications are becoming a very important part of many communications and transactions there is great impetus around the world to assure that legal frameworks are amended to ensure their validity.

Some SPECA member countries have already adopted measure to address issues of legal certainty. In Kazakhstan, a Law on Electronic Documents and Electronic Digital Signatures was adopted in 2003[18]; Tajikistan adopted a Law on Electronic Documents in 2002[19]; while Turkmenistan passed a law on Electronic Documents in 2000[20].

This section aims to outline some of the issues which arise when using electronic communications and to highlight the relevant international developments in this field. This section will cover the following issues:

- Legal recognition of electronic messages
- Form requirements for writing, signatures and original documents
- Retention of Data Messages
- Recognition of foreign electronic documents and signatures
- Admissibility of electronic evidence
- Formation and validity of contracts
- Recognition by parties of data messages

[18] Dated 7 January 2003. A version in Russian is available at http://www.cis-legal-reform.org/document.asp?id=8048

[19] Dated 10 May 2002. A version in Russian is available at http://www.cis-legal-reform.org/document.asp?id=6037

[20] Dated 19 December 2000. A version in Russian is available at http://www.cis-legal-reform.org/document.asp?id=4979

A. Legal recognition of electronic messages

Electronic commerce is carried out through the exchange of electronic messages, or data messages. Ensuring that messages are not considered illegal or invalid solely on the grounds of their electronic form is vital if electronic commerce is to thrive. Measures may therefore need to be taken to ensure that national legislation does not discriminate against generating, storing or communicating information in electronic form.

This is achieved in the UNCITRAL 1996 model law through the provision in Article 5

> *Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.*

Rather than approaching the validating of data messages in a piecemeal fashion, the aim of the 1996 Model Law is to provide an overarching provision which will cover all forms of electronic communication and the provision of electronic information. The purpose of the provision is to ensure that discrimination cannot arise solely on the basis of the electronic nature of the communication.

In terms of the scope of the Model Laws they both provide for wide definitions of the terms used. The term data message is used to cover both data information and data communication, thus the provision will cover both the electronic communications of offer and acceptance which make up an electronic contract and also data messages which simply confer information such as an electronic invoice or a message indicating the arrival time of a ship. The aim is to cover all types of situation where information is generated, stored or communicated, irrespective of the medium used.

B. Requirements of form

Many regulations stipulate requirements for documents to be produced in writing, or for a contract to be signed. There is no such certainty as to the validity and enforceability of electronic communications or signatures. To facilitate electronic commerce it may therefore be necessary to amend regulatory provisions to remove the legal obstacles to electronic communications, either by removing the requirement for writing, signatures and original altogether or by creating an alternative valid form which can be met through the use of electronic communications.

Paper-based documents serve several possible functions including ensuring that the contents of the document remain unaltered over time and also ensuring that information is provided in a form which would be admissible in court and accepted by public authorities. Particularly as regards high value transactions the ability to point to a document as evidence that a certain transaction has taken place has been considered a necessary measure to ensure against fraud. Elimination of fraud is not the only reason behind such a requirement. The form requirements may also serve as a reminder to the parties involved in a transaction of the significance of the undertaking. There is therefore still legitimate reason for maintaining such form requirements.

An electronic equivalent to a requirement for a paper document, or for a signature, must therefore look to the purpose behind the requirements of writing, signatures and original documents in order to provide a way of achieving these functions by electronic means.

1. Writing

Within most jurisdictions there will be many regulations stipulating that certain contracts should be concluded in a written document or in a specific form. These requirements may be provided for in general interpretation statutes or in the specific regulatory provisions themselves. Such provisions could exclude contracts which are, for example, made through electronic means or may at least give rise to a question of whether or not a contract has been validly formed.

A means for broadening the form requirement can be found in Article 9(1) of the 2005 Convention:

> *Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.*

It goes on to state in Article 9(2)

> *Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.'*

This provisions looks to the purpose of the writing requirement – that the information is accessible and readable in the future – and provides accordingly that electronic communications are capable of meeting this requirement where they are sent in such a form as to be accessible when necessary. Within Europe the E-Commerce Directive follows a similar approach in Article 9(1) requiring member states to "*ensure that their legal system allows contracts to be concluded by electronic means*".

A broad approach which validates the use of electronic messages and documents provides for a more encouraging environment for electronic commerce to thrive than a piecemeal approach which requires individual pieces of legislation to be amended as and when. The latter approach has the potential to overlook the updating of certain relevant legislation and also to potentially stall the development of electronic commerce if it is implemented in such a narrow way as to limit the use of new technological developments and means of communicating.

It may be necessary to include exclusions to this principle to exempt certain types of contracts. The 1996 Model Law provides in Article 6(3) a basis for states adopting this model to incorporate exclusions

> *The provisions of this article do not apply to the following…*

While the 2005 Convention provides in Article 3

The parties may exclude the application of this Convention or derogate from or vary any of its provisions.

2. Signatures

National regulatory provisions also lay down requirements for writing to be signed in certain circumstances, for example in some countries a contract for the sale of goods above a certain amount must be signed to ensure its enforceability. Even where national law does not provide for a pen and ink definition of a signature there may still be some ambiguity as to whether an electronic signature is considered valid and enforceable within the jurisdiction.

A signature has several functions which include identifying a person or associating the person with the contents of the document. Depending on the type of document the signature could also serve the function of indicating the signatory's intention to be bound by the contents of a contract, or the fact that someone was at a given place at a given time. Therefore the signature can be used for several different functions depending on the type of document to which it is attached. Some regulations, for example wills, may provide in addition that the signing of the document must be witnessed thus providing a further level of security.

As signatures provide different functions depending on whether they are witnessed or not, different levels of security are associated with them. One option in amending legislatory provisions is to provide electronic equivalents for all the different types and levels of signature requirement. However, even though different levels of electronic signature may serve to replicate the varied purposes of traditional signatures the provision needed to implement such functions might prove to be overly technical and complex. This may not be desirable for several reasons, the provisions may not readily take into account new technological developments, they may also be too closely tied to a particular technology which may not be reflected in commercial use. The wording of the provisions would therefore link the regulations to a particular period in development of the technology rather than providing a legal structure based on the underlying legal principles.

The models therefore have generally focused on two of the main functions of signatures, to identify the author of a document and to indicate that the author has approved the contents of the document.

The 2005 Convention provides in Article 9(3)

Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication.

(b) The method used is either:

(i) As reliable as appropriate for the purposes for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement, or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

This approach considers the functions that a signature provides rather than prescribing the form that the electronic signature should take. To be valid the provision requires that an electronic signature must be able to identify the party and to validate the integrity of the contents of the message.

The Model Laws generally also rely on the phrase that the method used should be "as reliable as appropriate for the purposes" for which the data message is generated or communicated. This enables the provision to steer away from making provisions for technical requirements and does not prevent electronic signatures from being used for different functions. Various legal, technical and commercial factors are likely to be considered in determining whether the method used was appropriate. The suitability of the method used will also depend upon the nature of the commercial activity, the value and size of the transaction and the relationship between the parties involved, the purpose of the signature, the acceptance of such methods within the particular industry and any provisions for insurance mechanisms.

The aim of the 1996 Model Law is not to provide that a functional equivalent of a signature will of itself confer validity, instead the question of validity should be settled under the national law. The requirement of both the 1996 Model law and the 2005 Convention is to ensure that electronic signatures satisfy signature requirements in the law. The approach taken therefore is that of providing a minimum standard for signatures. The issues of electronic signatures are discussed further in section III.C below.

3. Originals

When an electronic message is sent the recipient does not receive the actual message typed by the sender but instead receives an exact copy of this. Whenever this message is stored, read or sent a copy is made of it. The copy may itself go through various processes in the sending, or storing, such as being compressed, decompressed, encrypted or formatted in a particular way. This is in contrast to a paper based copy where on sending a letter the recipient receives the original letter rather than a copy of the letter in most circumstances.

Legal requirements for an original document to be produced are particularly relevant in relation to documents of title and negotiable instruments. The purpose of requiring an original document to be produced is generally as a means of ensuring the integrity of the contents of the document and to ensure that it has not been altered since it was originally created or sent. The electronic equivalent should endeavour to provide these same assurances of integrity.

Regulatory requirements for an "original" document to be produced are therefore not likely to be met through the submission of electronic documents unless some changes are made to the nature of these provisions.

The 2005 Convention achieves this recognition of electronic documents through the provision in Article 9(4) and (5) that

> *4. Where the law requires that communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:*
>
> *(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and*
>
> *(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.*
>
> *5. For the purposes of paragraph 4(a):*
>
> *(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communications, storage and display;*
>
> *(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.*

This provision in the 2005 Convention focuses on the function of ensuring the integrity of a document and enables electronic documents to meet this requirement where there is a reliable means of ensuring that the contents are unchanged. The fact that the formatting of the document has been changed in the processing of the electronic document, or that an electronic certificate has been added to the end of the message to attest to its originality, will not be a sufficient reason for invalidating the document. What is considered reliable will depend on the relevant circumstances. A further requirement in the provision is to ensure that the information is capable of being accessed by anyone who is entitled to see it.

C. Retention of data messages

The keeping of records is vitally important in many spheres of commercial life. The retaining of documents electronically can provide an efficient and space saving means of retaining large quantities of data. This form of record holding also has the advantage of being easily searchable. Many regulations require the maintenance of written records for a period of time for purposes such as accounting, tax, or auditing. Records may also be maintained to provide evidence of the existence of a contract or the ownership of certain intellectual property rights.

The requirements for retaining documents therefore need to be amended to provide for legally valid storing of documents in an electronic format.

The 1996 Model Law provides for the retention of data messages in Article 10.

> *(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:*
>
> *(a) the information contained therein is accessible so as to be usable for subsequent reference;*
>
> *(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and*
>
> *(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.*
>
> *(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.*

This provision enables messages to meet the retention requirement even if the message is subject to changes, for example in its formatting, if the information contained within the messages is an accurate reflection of the data message as it was when originally sent. Although some transmittal information may be important to retain, for instance the information contained in a data message when it was created or stored, or an acknowledgement of receipt of the message, the provisions do not lay down any obligation to retain additional transmittal information which is not relevant to the information contained in the message. This takes into account the fact that data messages are subject to various alterations which do not actually impact on the information contained therein but which are necessary for the purposes of sending and storing data messages. This includes methods for compressing, decompressing, encrypting or converting the data in order to store it.

D. Recognition of foreign electronic documents and signatures

International commerce clearly necessitates the legal recognition not only of nationally produced electronic documents and signatures but equally of foreign records. An issue to be considered when implementing such changes is whether recognition should be provided on exactly the same terms as national documents. Should the presumptions be any different? If facilitating international electronic commerce is the goal of a state, then providing for equal recognition of foreign documents and signatures will be necessary.

E. Admissibility of electronic evidence

Where the validity of electronic messages is under scrutiny the admissibility of electronic evidence may also prove to be contentious. A court of law may require evidence of a fact in resolving a dispute. Whether or not electronic messages and records will meet the evidential requirements of the court will need to be determined. While some countries have open evidentiary rules, there will still often be formalities required for certain types of document such as wills. In other countries there are very strict procedures and rules which must be followed before evidence can be validly presented in court.

The purpose of submitting evidence is that the court can rely on this evidence to a greater or lesser extent to help in determining the outcome of a case. A certain degree of reliability is therefore required before evidence may be put forward in court. Many jurisdictions have rules both on the admissibility of documents and the evidential weight of those documents. Some jurisdictions have rigorous formalities as to the presentation of documents, such as that they are notarized, while others place obligations on the party introducing evidence, to uphold the status of the evidence, by attesting for example to the proper functioning of a computer system from which an electronic record is produced. Such an obligation may be rather onerous to prove as it could involve the use of several experts who are able to testify as to the proper functioning of a computer system at a given time. Once the evidence has been found admissible, the court will then take the step of evaluating the evidence to determine what level of evidential weight should be ascribed to it using various factors such as the type of technology used.

One way of promoting the reliability of an electronic record is by showing that the system on which it is produced has been functioning properly.

Article 9 of the 1996 Model Law provides for the admissibility of electronic messages by ensuring that

> *(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:*
>
> *(a) on the sole ground that it is a data message; or,*
>
> *(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.*
>
> *(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.*

This therefore prevents evidence from being excluded solely on the grounds of being provided in electronic form. Provision 1(b) clarifies that where the principle of "best evidence" is

applied, whereby a party must produce the best form of the evidence available, such as the original document rather than a copy, then electronic evidence cannot be precluded simply because it is not in its original form.

In terms of the evidential weight ascribed to the submission of electronic messages and records, the provision provides several factors which can be used to determine the appropriate level of evidential weight to be prescribed.

F. Formation and validity of electronic contracts

Prior to the commercialization of the Internet electronic contracting did exist in a business to business context through the use of Electronic Data Interchange (EDI). This differs from communications through websites or email as in EDI the messages sent between computers are based on a standard or code agreed between the parties. A variety of EDI standards have been produced both on a national and international scale and more recently various model trading partner agreements have been developed.

Although EDI is still used by businesses, the Internet has provided for new opportunities for conducting business as it enables commercial parties who have no previous trading relationship to enter into transactions quickly and easily even where they live in different jurisdictions. Although this has its advantages it means that the trading parties are not entering into contracts on the basis of a trading partner agreement. This may therefore give rise to some legal uncertainties over the enforceability and treatment of electronic contracts.

National law on formation of contracts may be adequate to deal with many aspects of electronic contracting but certain issues such as where and when the contract is formed and what steps are required to incorporate terms and conditions may give rise to problems. The procedure to follow for correcting errors in the input of information is also a new issue which arises as a result of entering into contract online. The increased opportunities for business to consumer sales will also give rise to many consumer protection issues.

New provisions may need to be introduced in national law in order to provide for a greater degree of certainty as to the conclusion of the contract by electronic means.

1. Contract formation and validity

The 2005 Convention and the 1996 Model Law contain various provisions relating to the contract formation process. These provide for legal certainty over the use of electronic communications in contract formation and ensure that the contract is not deemed unenforceable simply as a result of it being entered into through electronic means. The provisions do not stipulate how a contract will be formed, or the steps to be taken to form the contract, but instead simply ensure that a valid contract can be formed electronically assuming all the requisite elements are met. These rules do not therefore replace traditional contract rules but instead supplement them in so far as providing for communication in electronic form. The provisions also do not place any obligation on parties to accept electronic means of contracting or communicating should they not wish to do so.

In recognition of electronic contracting the 1996 Model Law provides in Article 11 that

> *In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.*

The wording used in this provision makes it clear that a contract will not be denied validity or enforceability simply as a result of being formed through electronic communications but it may be denied validity on other grounds.

The 2005 Convention also makes provision for the formation of contracts through electronic means. Article 8 provides

> *(1) A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.*

These provisions ensure that the sending of an offer or acceptance in electronic form is not sufficient to invalidate a contract, but what about clicking on a button to agree to the contract terms? Is this sufficient to constitute an offer or acceptance of an offer? The only model to specifically provide for this issue is the Commonwealth Model Law on Electronic Transactions. This model provides in Article 18 that

> *(1) Unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed:*
>
> *(a) by means of information in electronic form; or*
>
> *(b) by an act that is intended to result in electronic communication, such as touching or clicking on an appropriate icon or other place on a computer screen, or by speaking.*

The only reservation about including such a term within a national regulatory provision is whether it may prove too restrictive in terms of encompassing future developments in technology. Although clicking on an icon may currently be a popular method for entering into contracts online, whether it continues to be used or whether a new method replaces this remains to be seen. Provisions which seek to enable electronic commerce and contract formation through electronic means should attempt where possible to remain neutral as to the approach used to achieve this goal.

While electronic forms of communication are clearly useful their use should not necessarily be imposed upon parties. For example, the United Nations Convention 2005 provides in Article 8

> *2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.*

Article 8(2) ensures that no obligation is placed upon parties to a contract to accept electronic communications unless they choose to do so either expressly or impliedly through their actions. Clearly if an offer is made by electronic means the offeror cannot refuse to recognize an acceptance issued in the same form.

States may also wish to restrict certain types of legal agreement from being formed electronically.

2. Use of automated message systems

Developments in technology and software have enabled computer programs to automatically issue and receive electronic orders without any human involvement. The ability of electronic agents to independently form contracts may give rise to questions over the legal validity of these contracts, particularly in countries where an expression of intent of the parties is required.

The 2005 Convention provides for the valid use of automated message systems for contract formation in Article 12 where it states

> *A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems of the resulting contract.*

This provision ensures that where the electronic messages communicating offer and acceptance are generated without human intervention this is not sufficient to render the contract unenforceable.

3. Incorporation by reference

Contractual terms will generally be provided for in the agreement between the parties, either expressly in the body of the agreement or impliedly by law, custom and practice or the actions of the parties. However in certain circumstances where there is an on-going relationship between the parties the terms and conditions are often referred to in a separate document rather than being expressly stated. This incorporation by reference is a recognized commercial practice. In order to ensure that such incorporation is valid in an electronic environment the 1996 Model Law provides in Article 5bis

> *Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.*

4. Invitation to make offers

Whether a website selling a particular product is to be considered as making an offer of a product or simply treated as an invitation to make an offer is an issue which has undergone much debate. If the structure of the website is such that it is considered to be making an offer of the products listed, then assuming unconditional acceptance was made of this offer a valid contract would be concluded. Where there is a limit to the number of goods for sale a website owner could find himself in a difficult position if more contracts are concluded than goods for sale. For this reason the website is generally considered to be an invitation to make offers. A similar principle may be applied to bulk emailings.

In order to clarify this position the 2005 Convention provides in Article 11 that:

> *A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.*

5. Incorporating contract terms

Ensuring the valid incorporation of terms into a contract may involve taking certain steps to draw the party's attention to these terms. The availability of contract terms is addressed by the 2005 Convention in Article 13:

> *Nothing in this Convention affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those electronic communications which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.*

Contract law generally requires the party to a contract to be able to review the terms of that contract before entering into an agreement. Failure to do so may in certain cases result in the terms not being effectively incorporated into the contract and therefore not binding on the party.

A popular method for incorporating terms into a contract through a website is where the supplier requires the customer to click on a button agreeing to the contract terms before being able to conclude the contract. Alternatively, the supplier may provide a hypertext link within the context of the webpage which provides a link to the terms and conditions. Incorporation of terms through this method is not quite as reliable though as the consent is implied rather than express. The binding nature of the terms may therefore be subject to challenge for lack of transparency, for example if the link was not sufficiently obvious to the user.

Not only should terms and conditions be made available but they should also be capable of being retained by the customer for subsequent reference. This is provided for in the E-commerce directive in Article 10(2) where it states:

> *Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.*

6. Provision of information on the contract formation process

The question of how and when an electronic contract is formed is also a controversial issue. Is it for example when the acceptance message is sent, or when it is received? What about where the contract is formed? Does formation take place in the location where the customer clicks on an "I agree" button on his computer screen or in the location of the supplier?

National contract law provisions will determine these issues. However for the purposes of resolving uncertainty, particularly in relation to consumer contracts, specifying exactly what each step in the contractual process means and when and where this will lead to the formation of a contract is desirable.

The EU E-Commerce Directive ensures that a customer should be made fully aware of the steps which must be taken to conclude a contract. Article 10 (1) provides:

> *In addition to other information requirements established by Community law, Member States shall ensure, except where otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:*
>
> *(a) the different technical steps to follow to conclude the contract;*
>
> *(b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;*
>
> *(c) the technical means for identifying and correcting input errors prior to the placing of the order;*
>
> *(d) the languages offered for the conclusion of the contract.*

These requirements, which are primarily aimed at website disclosures, do not apply to the exchange of emails.

7. Error Correction

Inevitably mistakes will be made in the process of entering into electronic contracts. An order may be placed twice accidentally or the quantity required of a product may be mistyped. How can this mistake be rectified? Is there provision on the website to revoke an order made by error or a means of communicating with the sender to explain the mistake?

The 2005 Convention provides in Article 14 that:

> *1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:*
>
> *(b) The person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and*
>
> *(c) The person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.*

This provision applies only to natural persons, it is therefore a consumer protection mechanism rather than a provision applicable to business to business transactions.
The E-Commerce Directive goes further by requiring service providers to provide effective technical mechanisms to correct input errors. Article 11(2) provides:

> *Member States shall ensure that, except where otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.*

8. Attribution of data messages

As with written documents there may be a question as to whether or not the alleged sender of the message did actually send the document. In the case of a paper document it may be suggested that the signature on the document has been forged. In an electronic environment it may be alleged that the person who actually sent the message was not authorized to do so.

The 1996 Model Law establishes a presumption that in certain circumstances a data message would be considered as originating from the sender though this presumption is qualified where the addressee for any reason knew or should have known that the data message did not actually come from the sender. It clarifies that the originator is bound by a data message if the message has been sent by him. Where a message is sent by someone acting under the authority of the originator then the presumption also applies.

Article 13 provides:

> *(1) A data message is that of the originator if it was sent by the originator itself.*
>
> *(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:*

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

Where the addressee receives notice that the originator has not sent the message then the presumption ceases to apply as provided in Article 13(4)

Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

This provision provides that the originator is not bound by the data message from the time when the addressee received notice that it was not from the originator. Up until that point the addressee would be able to rely on the assumption that the message was sent by the originator.

9. Acknowledgement of receipt

After confirming an order many online companies will send a receipt to acknowledge the order. This provides the purchaser with the assurance that the ordering process has been successful and that the contract has been effectively concluded. Within Europe an obligation is placed on a supplier to acknowledge receipt of the order when conducting business with consumers and also with businesses unless otherwise agreed.

Article 11 of the EU E-Commerce Directive provides that:

> *The service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.*

This issue is also addressed in the 1996 Model Law though the model law is based on the assumption that the originator may choose whether or not to use an acknowledgement procedure. The provision simply provides for when an acknowledgement is received and does not consider any other legal consequences arising from the acknowledgement.

Where an acknowledgement is requested but is not received, and the originator has not made it clear that the data message is not effective until the acknowledgement has been received, what is the position? Is the originator of the message still under a legal obligation to the party or can he then make the offer to another party? The obvious answer to this would be to ensure that a deadline is provided for acknowledging the offer and outlining the consequences of not receiving an acknowledgment within this time but where this is not the case problems may arise. The 1996 Model Law attempts to address this situation by providing in Article 14 (4) that

> *Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:*
>
> *(a) may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and*
>
> *(b) if the acknowledgment is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.*

The provision makes it clear that the originator of the message cannot immediately dismiss the data message as if it had never been sent but must provide the addressee with further notice.

10. Time and Place of Dispatch and Receipt

While national law and/or contractual provisions will determine what steps are necessary to conclude the contract, there is still the question of at what point the message is considered to be sent and from where. This has legal significance in terms of where and when the contract was created and may also be relevant in cases of dispute in determining choice of law or choice of forum under private international law rules.

There are several possible interpretations of when a message is considered to be sent. Should a data message be considered to have been sent as soon as it is dispatched? What happens if the sender's communications system is not functioning properly? When is the message

considered to be received by the addressee? Is this when the addressee actually reads the message or when the message is capable of being read by the addressee?

The 2005 Convention takes a pragmatic approach to clarifying the issues of time and place of dispatch and receipt of electronic messages in Article 10:

> *1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.*
>
> *2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.*

The determination in the 2005 Convention of when something is sent or received relates to who has control of the particular message. The message is considered to be dispatched when it enters an information system outside the control of the sender. In a similar way receipt is considered to be effective when the message enters a designated information system of the recipient. However if there is no designated information system the message will not be considered to have been received until the recipient actually receives it.

Where a message is sent from or received may give rise to even greater uncertainty. This is because the physical location of the parties may not be known at a particular time or may be subject to change. The 2005 Convention therefore also provides for further clarification of the place where the electronic communication is deemed to be sent and received.

Article 10 provides that

> *3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.*
>
> *4. Paragraph 2 of this article applies not withstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.*

The Convention also lays down rules for determining the place of business of the parties in Article 6.

> *1. For the purposes of this Convention, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.*
>
> *2. If a person has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this Convention is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.*
>
> *3. If a natural person does not have a place of business, reference is to be made to the person's habitual residence.*
>
> *4. A location is not a place of business merely because that is: (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information system may be accessed by other parties.*

The Convention also provides in Article 6(5) that the use of a country specific domain name or email address does not determine the place of business:

> *The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.*

G. Recognition by parties of data messages

Ensuring recognition of data messages which do not form part of a contract but which do relate to the specific performance of contractual obligations, such as an offer to pay or recognition of a debt, is also important. Although this is provided for through the adopting of a provision that provides for non discrimination on the basis that a communication is electronic, many of the models have considered that it is important that there should also be a provision specifically providing for recognition by parties of data messages.

Article 12 of the 1996 Model Law provides that

> *(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.*

H. Conclusions

This section serves to highlight some of the important issues raised in relation to the validity, enforceability and admissibility of electronic messages. It also provides an indication of the approaches that have been taken on an international and regional level. However in determining the most suitable approach for a national law to take, regard must be had to the existing provisions in the national law of form, writing and signature requirements, evidentiary requirements and also the particularities surrounding contract formation.

The issues arising from this section on legal certainty include the following:

- Providing for legal recognition of electronic information and communications
- Ensuring that requirements of form, writing, signatures and originals, can be met by electronic means
- Providing for legal recognition of electronic means of data storage
- Ensuring the legal recognition of foreign electronic documents and signatures
- Permitting the admission of electronic evidence
- Providing for the formation and validity of electronic contracts.

I. Further reading

International Chamber of Commerce (ICC), General Usage for International Digitally Ensured Commerce, 2001, available at http://www.iccwbo.org/home/guidec/guidec.asp

United Nations Convention on the Use of Electronic Communications in International Contracts - Text and Explanatory Note by the UNCITRAL Secretariat: available at http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.

III. LEGAL ICT SECURITY

This section of the report deals with the issues surrounding security of electronic commerce. To ensure a trusted environment for businesses, administrations and individuals requisite levels of security are required. A commercial environment cannot thrive without assurances that electronic data, signatures and evidence will all be legally valid and admissible in contract formation as discussed in Section II of the report. Likewise trust in a banking network is not going to persist unless customers are assured of the confidentiality and security of electronic communications. From the point of view of public administrations, information and communications technologies must be able to make available data as and when necessary and also be able to ensure to a reliable degree that this data has not been altered.

This section will consider the issues of integrity, authentication and confidentiality and will examine the approaches to managing security risks online, in particular the use of electronic signatures.

A. Issues

1. Integrity and authentication

Paper and ink documents are difficult to change without leaving evidence that an alteration has been made. The amendment of electronic data, unlike the amendment of a handwritten document, cannot be detected as readily. The ease of altering a document makes it difficult to determine in what way a document has been altered and when the alteration took place. For example an electronic contract could be altered by either of the parties at some point after the agreement was reached. Electronic signatures have been developed to overcome these security issues and provide for an adequate level of legal certainty when communicating and contracting electronically.

2. Confidentiality

Within the traditional environment security methods have long been used to ensure the security and confidentiality of paper documents and files. Measures to protect the security of documents have traditionally involved locked offices and filing cabinets and perhaps alarm systems to detect entry into office buildings. Depending on the nature of the documents to be protected different levels of security may be deemed necessary, from bank vaults to protect money or bonds to simply a filing cabinet to maintain records.

Both individuals and commercial entities have reasons for wanting to retain the confidentially of certain information. Businesses will often insert confidentiality clauses into the contracts of their employees if there is concern about the revealing of trade secrets or information processes to competitors. Certain professions lay down confidentiality requirements as a part of the professional duties of the employee, for example the non-disclosure of information about clients for lawyers and patients for doctors. Public authorities will equally be under obligations to maintain confidential information in respect of individuals and companies.

Individuals may likewise want to limit the use of their personal details. Protecting the use, collection and transfer of personal data has been recognized within certain jurisdictions in data protection regulations.

B. Managing ICT security risks

Recognition of the need to take security measures seriously can be seen in the increased use of firewalls to protect an organization's data and virtual private networks to control access to an organization's data or network.

Individuals, businesses and public authorities all need to consider the impact electronic commerce has on the security of their personal details, electronic data and business infrastructure. Particularly in the financial sector ensuring the availability of information systems at all times is very important. Being unable to access a system could potentially lead to legal action as a result, for example, of financial losses where a payment was not processed within a particular time.

Security of information is an area which has developed very quickly and continues to develop as a result of technological advances. Much work has been undertaken to determine the risks which the electronic environment poses and to try and find methods of reducing or managing the risks. In particular mechanisms have been developed to identify where the risks lie and to introduce standards or procedures which can be followed in order to mitigate the risks.

Codes of practice such as the ISO/IEC 17799:20000 "Code of Practice for information security management" outlines the security objectives. These include allocating responsibility for management of databases, files, software and procedures to reduce the instance of fraud or misuse by screening employees and using confidentiality agreements in the workplace to bind employees. The code also provides methods to prevent unauthorized access to systems and business premises and also means of ensuring compliance with applicable laws. Such codes therefore try to provide an overarching means of ensuring a commercial entity has considered all of the security risks and taken steps to manage these in as effective a way as possible.

C. Digital Signatures

Some of the legal measures to facilitate the use of electronic (or digital signatures) are referred to in Section II.B.2. This section will focus more on the security functions of electronic signatures, to enable the authentication of parties to a transaction and ensure the integrity of the contents of a document, and the means of regulating these functions.

When communicating in an electronic environment parties to an online transaction need to be able to ensure that the messages sent and received between them will reach their intended recipient unaltered. They also need to verify that the other party to a transaction is who he or she claims to be. The technological measures for creating digital signatures vary widely and likewise so does their reliability to achieve the purpose required. The degree of reliability varies according to the method which may be used which may be something as simple as writing a name at the bottom of an email, using Personal Identification Numbers (PIN) or

passwords to biometric systems such as retinal scans or thumbprints and cryptography. The data or signature (such as the fingerprint) which is attached to the message indicates the source of the message (who it comes from), acting as a functional equivalent to a handwritten signature.

Depending on the level of risk (financial or non-financial) involved in the type of transaction, differing levels of security and therefore different levels of signature will be appropriate. A scanned handwritten signature will not provide a high level of security because it does not authenticate the person sending the message nor ensure the integrity of the message. The scanned signature could be attached to a completely different document or the contents of the document could be amended without this being readily detectable by the recipient. On the other hand a signature developed using public key cryptography provides a higher degree of security because it involves mathematical algorithms which are virtually impossible to decode and because such signatures can be used both to verify the identity of each party to the transaction and to ensure that the message has not been altered in transit.

1. Public Key Cryptography

Cryptography, basically a method for encrypting information, and in particular public key cryptography has been developed to enable an electronic signature to achieve the function of authenticating the signatory and ensuring the integrity of the message.

Public key cryptography enables two or more parties to a transaction to exchange data messages even without a prior relationship and provides a way for them to ascertain the identity of the other party. This system generally involves the use of a certification service provider who will issue a certificate verifying the identity of the party. The technology involves the use of a public key and a private key which can be used to encrypt and decrypt messages sent between the parties. Where a message is encrypted using for example A's public key it can then only be decrypted using A's private key and vice versa. The private key is always retained by A while the public key relating to that private key can be provided to any intended recipient of the message. The certification service provider's purpose is to ensure that a public key corresponding to A actually does so and that A is who he or she claims to be. This method therefore allows parties to a transaction to be able to determine the identity of their correspondent and also to ensure that any message sent from the particular correspondent has not been altered in transit.

2. Regulatory Approaches

Many countries have introduced legislation giving legal effect to electronic signatures. The 2005 Convention and the various Model Laws provide for the recognition of electronic signatures where used in a way that is considered sufficiently reliable (see section II.B.2).
UNCITRAL has also developed a specific Model Law on electronic signatures. The 2001 Model law provides for a definition of electronic signatures in Article 2:

> *Electronic signature means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in*

> *relation to the data message and to indicate the signatory's approval of the information contained in the data message.*

A neutral definition is used in order to be adequate to cover new and developing technologies. The 2001 Model law enables the use of electronic signatures in Article 6(1):

> *Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

This question of what is considered as being sufficiently reliable for the purpose is further clarified by Article 6(3) which provides:

> *An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:*
>
> *(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;*
>
> *(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;*
>
> *(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and*
>
> *(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.*

Such a provision therefore ensures that the signature achieves the functions of being linked to the signatory and also ensures that the signature has not been altered. The Model tries to ensure a technologically neutral approach by ensuring through Article 6(4) that other ways may be used for establishing the reliability of an electronic signature.

While public key cryptography may currently provide the best means of achieving the aims of a handwritten signature this may not be the case in years to come. Many legislative models have therefore avoided tying their enabling legislation to this particular type of technology. A technologically neutral approach allows the legislation to be effective to cover future developments without requiring significant alterations.

The EU approach in the Electronic Signatures Directive has been to provide recognition to two different categories of signature. These are classified as electronic signatures and advanced electronic signatures. The Directive provides that "advanced electronic signatures" based on a qualified certificate and created by a secure-signature-creation-device (some form of encryption) can be considered as equivalent to a handwritten signature and be admissible as evidence in court proceedings. Qualified certificates are certificates which meet the standards

laid down in the Directive and which are issued by certification service providers meeting certain requirements. An advanced electronic signature is a signature which meets the following requirements laid down in Article 2(2):

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

Under the EU approach electronic signatures which do not comply with those requirements, although not considered equivalent to a handwritten signature, cannot be denied legal effect or refused as evidence in the courts solely because they are in electronic form. It will therefore be up to the court to determine according to the facts and circumstances the weight to be given to a particular signature. The advanced electronic signature is given greater weight in terms of legal presumptions and admissibility due to the presumption of greater security due to the technological methods used to achieve the goal.

This approach has caused some debate as to whether it is the best way of facilitating use of electronic signatures. Some concern surrounds the question of whether it relies too heavily on technology rather than legal principle. The provisions therefore may be seen as tying themselves to particular technologies which may be superseded at some point down the line therefore rendering the regulations obsolete. It would seem however that precise regulations on the means of electronic signature used may be necessary in certain spheres – particularly as regards electronic communication with government and administrative bodies such as tax authorities. However whether this should be prescribed in a general electronic commerce enabling legislative framework or whether it should be left to regulation on that particular sphere should be considered.

3. Certificates

Certificates can be used to confirm the identity of the person electronically signing a message. Certification service providers are the intermediaries who provide certificates which verify that the signature creation device belongs to the signatory and also validates the identity of that person.

The 2001 Model Law provides for certain standards which must be met by certificate service providers. In Article 9:

> *1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:*

(a) Act in accordance with representations made by it with respect to its policies and practices;

(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

(c) Provide reasonable accessible means that enable a relying party to ascertain from the certificate:

(i) The identity of the certification service provider;

(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise;

(i) The method used to identify the signatory;

(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) That the signature creation data are valid and have not been compromised;

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1(b), of this law; and

(vi) Whether a timely revocation service is offered.

The obligation on the certification service provider therefore includes ensuring the accuracy of the information contained within the certificate and that at the time of issuance the signatory identified in the certificate held the signature creation data when the certificate was issued.

A certificate could contain limitations as to the value of the transaction for which the certificate is used or it may concern the types of uses of the certificate.

Article 9(2) provides for the liability of a certification service provider for failing to meet the legal requirements:

A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

D. Data Protection

The use of the Internet and electronic communications, with the ability to process large quantities of data, gives rise to significant concerns over how that data will actually be used, by whom and for what purposes. The electronic environment has increased the scale of the data collected as a result of the ability to store large volumes of records in a fully searchable manner. It also enables the transfer of this data quickly and easily to other parties across national boundaries. Finally the use to which the data can be put from identity theft for the purposes of credit card fraud to manipulation of accounts and records make the data more vulnerable to attack from outside.

Data is collected by both private and public bodies for a variety of purposes, from marketing activities, such as the profiling of individuals to target suitable audiences for a particular product, to the governmental steps to maintain databases of taxpayers, criminal records or electoral rolls.

Jurisdictions have taken quite different approaches to the collection and use of personal data. The United States for example provides little restriction on the buying and selling of personal data in the form of mailing lists while the EU takes a more restrictive approach which limits the sale of such lists to those comprised of individuals who have agreed to the transfer of their personal data.

Protecting the use, collection and transfer of personal data has been recognized within certain jurisdictions as being important. Europe in particular has been at the forefront of regulating the use of personal data. The EU Data Protection Directive provides for restrictions on what data can be collected, the uses to which it can be put and the methods which should be implemented to protect personal data against accidental or unlawful destruction or accidental loss.

A controversial issue in this area is the transfer of personal data between jurisdictions particularly where those jurisdictions have completely different approaches to the protection of the data. Such transfers will often impose obligations on companies located within countries without data protection regulations where they accept data from countries with strict data protection restrictions. These obligations may be performed through contractual requirements restricting the use of the personal data to purposes other than those agreed upon and which meet the sending countries' data protection regulations.

E. Conclusion

This section highlights the security issues inherent in electronic commerce. While these risks cannot be completely eradicated, by identifying the risks steps can be taken to manage them more effectively.

The issues arising from this section on legal certainty include the following:

- Determining the security risks posed by electronic commerce and taking measures to manage them
- Providing for the use and regulation of electronic signatures

Determining appropriate rules for protecting personal data.

F. Further reading

International Chamber of Commerce (ICC), *General Usage for International Digitally Ensured Commerce*, 2001, available at http://www.iccwbo.org/home/guidec/guidec.asp

Organisation for Economic Cooperation and Development (OECD) *Guidelines for the Security of Information Systems and Networks*, 2002, available at http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD, *Privacy Online: OECD Guidance on Policy and Practice*, 2003, available at http://www.oecd.org/

IV. LEGAL PROTECTION

The flow of information and goods across borders gives rise to international concerns over the enforceability and protection of intellectual property rights ("IPRs"), including copyright and related rights, patents and trademarks. Trading goods across national borders has been gradually increasing over time but the extent of trading which the Internet allows for and the type of goods which are being traded has expanded exponentially. Intellectual property rights are generally national in scope but the Internet has placed great emphasis on the ability to protect and enforce these rights on an international scale.

There are a number of international agreements on various aspects of intellectual property, including the Paris Convention for the Protection of Industrial Property[21] (1883) and the Berne Convention for the Protection of Literary and Artistic Works[22] (1886), to which most SPECA member countries are signatories and have implemented appropriate provisions in national law. The most significant harmonization initiative in the field is the Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS"), which is administered by the WTO[23].

The Internet has also changed the face of business to business and business to consumer supplies. It has opened up channels for trading with consumers on an international scale which were not previously possible. While this increases levels of business it can also give rise to particular legal issues as regards the customers, particularly issues of data protection and consumer protection.

A. Trademarks

A trademark is a word, logo, design or other features which is used in trade in conjunction with particular goods or services to denote the source of those goods and services and distinguish them from those of other traders. Owners of trademarks have the right to prevent others from using their trademark on identical or similar goods in the course of trade. The policy aims of the trademark legislation are both to prevent the consumer from being confused about the source of a particular product and to prevent the dilution of the reputation of a mark through its use in association with inferior goods or services.

Trademarks are generally protected through registration on a national basis in association with particular goods or services. Therefore it is possible and in many cases likely that the same name will be registered in association with different classes of goods and services. The registration of a trademark has only national effect so registration must be carried out in each country where an individual wishes to receive protection of the mark. There have been various measures to harmonise the trademark system of registration and classification. It is

[21] There are some 164 signatories to the Convention, of which only Afghanistan of the SPECA member countries is not a signatory.

[22] There are some 150 signatories to the Convention, of which only Afghanistan and Turkmenistan of the SPECA member countries are not signatories

[23] See generally http://www.wto.int/english/tratop_e/trips_e/trips_e.htm

also possible for names or logos used in association with particular goods or services to be protected even without registration in certain jurisdictions. In the United Kingdom for example, the tort of passing off can be successfully used against someone who misrepresents an association with the product of a competitor in an attempt to use the goodwill associated with a particular product to sell his own products. For an action to be successful there must be some damage or likelihood of damage caused to the trademark of the claimant.

1. Domain names

The area which has caused the greatest amount of controversy is the use of domain names comprising trademarks. The domain name system operates in a very different way to that of the trademark system, for example the domain name is not associated with a particular product, and this has therefore given rise to a large number of disputes.

When a computer connects to the Internet it will be allocated a unique identifying number called an IP address. When searching for a website it is necessary to use this IP address to identify the computer which hosts the website. The IP address consists of four numbers, each between 0 and 255, and each separated by a full stop. As these numbers are not particularly memorable in themselves the domain name system was developed in order to make these addresses more easily accessible. A domain name is used to map to the IP address of a computer, and this enables the computer to be readily identified. Within the domain name categories there are two levels of top level domain – country codes such as .uk and generic codes such as .org.

In order to identify a website it is common to incorporate a trademark within the domain name. The domain name containing a trademark is therefore of great value to a trademark holder.

Although domain names also need to be registered, the system works in a completely different way with the domain name system working on a first come first served basis with little or no evaluation of the merits of an application. Domain names can also be registered for commercial or non-commercial use and most importantly they are not registered in relation to any particular class of goods or services. There are categories in the generic top level domain names such as .org, .com and .edu but these are far more limited than those applicable on a national basis to trademarks.

While trademarks allow the same name to be used by multiple users in multiple classes or categories, domain names must be unique in order to act as an address for an individual computer and to direct users to the computer required. These differences between domain names and trademarks have inevitably led to disputes. Firstly those between trademark holders with the same name but different goods. In terms of domain names it will be the first one to register the domain name who will attain the name. Secondly disputes arise where individuals have purchased certain domain names with the intention of selling them for profit to the trademark holder of that name. Such activity is often called cybersquatting. Several jurisdictions, such as the United States with its Anticybersquatting Consumer Protection Act, have already developed regulatory measures to attempt to prevent abusive registration of domain names.

The International Corporation for Assigned Name and Numbers (ICANN) is in charge of administering the domain name systems. To deal with the domain name disputes which have arisen ICANN implemented a Uniform Dispute Resolution Policy in 1999. Claims arising from a domain name dispute can therefore either be brought to one of the ICANN accredited resolution service providers, such as the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center for domain name disputes[24], or taken before a national court.

2. Hyperlinking and framing

Another area giving rise to legal dispute is that of hyperlinking, in particular deep linking. This is where a link is made from one website owner's homepage to an interior page on another website. This gives rise to some controversy as by linking to a page within the website rather than to the website owner's homepage the user when clicking on the link may bypass the homepage and potentially any advertising materials contained on that homepage.

Framing occurs when a website links to information contained on another website and this information is presented in a particular format using frames rather than taking the user to the other website directly. Confusion may arise as to the source of the information.

While linking is a necessary part of the Internet there is still some question as to the legality of deep linking. Courts in several jurisdictions have been asked to determine whether deep linking and framing give rise to issues of passing off, unfair competition or copyright infringement.

Website owners may try themselves to prevent such deep links being created through the use of cookies on the website or other technological measures.

3. Meta-tags

Meta-tags are used to ensure that a page is listed when someone searches for a particular topic. The issues or topics related to a particular webpage will be invisibly inserted into the hypertext language used to create webpages to allow search engines to identify relevant webpages for its search results. The more frequently a word is used in a meta-tag the more chance that it will be listed in the search results. Although meta-tags can be a useful means of describing the contents of a webpage, they can also be used solely for the purpose of trying to increase user access to their page. This can be achieved by, for example, incorporating the trademarks of competitors into the meta-tag. Various disputes have arisen where trademark owners have argued that meta-tags have been used by competitors to unlawfully make use of the goodwill of the trademark owner in the name.

Measures used to deal with these issues include the use of disclaimers which for example explain that the website has no association with the owners of the trademark. Linking

[24] See generally http://www.wipo.int/amc/en/domains/index.html

agreements and various technological approaches such as the use of cookies, or filtering requests for the website from certain URL's may be useful.

B. Copyright

Copyright protection covers original literary, artistic, musical and dramatic works as well films, sound recordings and typographical arrangements. There is no formal registration process for copyright works, therefore by simply recording the work, for example by producing a webpage, this will give rise to copyright protection. The contents of a webpage will therefore generally be subject to protection whether or not it incorporates the © symbol.

Copyright protects the expression of an idea but cannot be used to protect the idea itself. Therefore copying the text of a fictional story will give rise to infringement but simply using the basic idea behind the story may not. A copyright owner has the exclusive right to carry out certain activities in relation to the work such as copy it, issue copies to others and make adaptations of the work. The right to do these activities may be assigned to others or licensed. Infringement of copyright occurs when someone carries out one of these activities without the authority of the copyright holder.

1. Open source

Copyright works will generally be made available subject to a "licence" detailing the terms under which the work can be used. From a legal perspective, a "licence" may be characterized as either a unilateral grant of permission by the licensor to use the work in certain ways, or may comprise a contractual agreement between the licensor and licensee. In an online context, such licence agreements are often referred to as "click-wrap" licences. Legal acceptance of the user is achieved by an indication of his assent to the terms by clicking his mouse usually on a specified icon.

The prevailing culture of openness expressed by many Internet users, particularly technically sophisticated earlier adopters, has also led to the growth of alternative licensing schemes designed to facilitate the sharing of information, rather than restrict its use through copyright. In the software field, the LINUX operating system was developed cooperatively based on a licensing mechanism whereby anyone was freely able to copy and amend the work, on condition that any work product that is based on the original work must also be licensed to freely and at no charge. This has come to be known as "open source" licensing. The term "open source" is used in a range of contexts, but primarily denotes a software development model and/or a licensing model. As a software development model, communities of programmers or code writers from individuals, to employees, to companies, contribute to the writing of the source code for a program, such as LINUX, which is then distributed under an "open source" licensing model.
There are a large number of "open source" licences, but they share some common features[25]. First, a licensee is free to redistribute the program. Second, a licensee should be given access to the source code, the language in which the program was written (e.g. C+), as well as the

[25] See further the Open Source Initiative (OSI) at http://www.opensource.org

object code (i.e. machine code). Third, the licensor must permit modifications to be made to the original work, or derivative works. Fourth, there should be no discriminatory licence terms in respect of either the use or user of the program. Fifth, no other collateral or tying restrictions may be imposed on the licensee. The most famous of the open source licences is the GNU General Public Licence (GPL) issued by the Free Software Foundation.

In contrast to "open source", schemes have also been established for so-called "public domain" materials (e.g. http://www.creativecommons.org), where the legal owner of the copyright surrenders his copyright over the material and allows free re-use, adaptation and redistribution. While "open source" licensing utilises existing copyright regimes to facilitate the widespread distribution, use and development of source code, public domain software and information discards the operation of the copyright regime altogether.

2. Infringement

Copying of works online clearly gives rise to copyright infringement if the consent of the copyright owner is not granted. Some argue that by placing a work online there is an implied consent for the work to be copied though this has not been upheld by the judiciary. The development of digitized products also extends the possibility for the types of work which can be copied and freely distributed over the Internet.

Websites which allow users to post content should be aware that the content posted may itself infringe copyright. They should also require users to grant a non exclusive license to the forum host or assign copyright to enable the host to edit, copy and delete the contents.

3. Internet Service Provider Liability

Placing work on the Internet may give rise to several issues in relation to copyright. Even the methods by which webpages are downloaded and viewed involves the copying of a work. Internet Service Providers (ISP) will often store copies of popular webpages in their "caches" in order to improve their efficiency in retrieving these pages. If such copying were to give rise to infringement then this would hinder the development of e-commerce. ISPs would also be found liable for transmitting webpages or storing copyright works in the course of their everyday activities. Many jurisdictions have therefore provided within their national legislation that these activities which are necessary for downloading and viewing webpages will not give rise to infringement.

In the United States the Digital Millennium Copyright Act 1998 provides exemption from liability for ISPs for copyright infringement for infringement that arises as a result of transmitting, caching or hosting copyright material as long as the copyright holder is not aware of the infringing nature of the material. Once aware of the infringing material the ISP must remove it or disable access to it. The EU also provides for a similar level of immunity for ISPs so long as they are unaware of the infringing materials.

4. Technological Protection Measures

Some of the steps taken to facilitate protection of IPR involve the development of technological protection measures. These technological approaches, such as the use of copy protection measures, have given rise to new legal issues of their own. Copy protection mechanisms enable a copyright owner to restrict access to, and copying of, their work. Some argue that this prevents lawful users from accessing works for the purposes of fair dealing or fair use. Laws have been introduced in various jurisdictions including the EU and the United States to prevent the use of devices to circumvent the copy protection measures.

The Internet creates numerous challenges for the owners of IPRs. The fast and effective way of displaying and sending products across national boundaries also gives rise to issues of cross border enforcement of rights.

C. Consumer protection

Existing consumer protection laws will often encompass Internet-based transactions without the need for amendment[26]. However, various measures have been taken to increase consumer confidence in relation to online transactions, from the provision of specific information regarding the supplier and the product to greater levels of protection in relation to the fraudulent use of payment cards for online transactions.

1. Transparency

The provision of information to the consumer to enable him to adequately identify the supplier and to compare the characteristics of several products allows him to make an informed decision as to which product to buy.

The E-commerce directive also provides for the provision of certain information to the consumer and stipulates when this information should be provided.

2. Fraudulent use of payment cards

A particular concern for consumers is the safety of using their credit card (or other payment card) details online. Security issues arise in relation to the potential interception of card details while making the transaction or the misuse of those payment details by the recipient. Various technological measures can be used to provide for safer transmittal of payment details such as the use of the Secure Socket Layer on web browsers to ensure the details cannot be intercepted in transmission. The inability to properly identify the supplier however still poses security concerns for the consumer. Although electronic signatures do provide a method for doing so, such e-signatures have proved too cumbersome and costly to use for low value consumer transactions.

[26] E.g. Law of the Republic of Kyrgyzstan on the protection of consumers rights, December 1997.

To enhance consumer confidence the EU in its Distance Selling Directive makes provision for issuers of credit and debit cards to compensate consumers for any loss arising from fraudulent use of their payment card online. Article 8 provides that

> *Member States shall ensure that appropriate measures exist to allow a consumer:*
>
> - *to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts covered by this Directive,*
> - *in the event of fraudulent use, to be recredited with the sums paid or have them returned.*

These measures do enhance levels of consumer confidence but there is still a need to consider appropriate methods for resolving disputes when they do arise.

3. Dispute resolution

Major challenges to resolving consumer protection disputes in relation to electronic commerce are the issues of cross border claims, the uncertainty as to what law applies and the problems of enforcing consumer protection law. Individual consumer complaints often involve small value transactions therefore resorting to court action is inappropriate due to the expense and time involved. Where cross border disputes arise the cost, time and difficulties of getting access to justice are exacerbated. There have been steps taken to improve international cooperation and the harmonization of consumer protection standards but there is also a need to consider other low-cost measures to address consumer claims.

In the consumer protection field alternative methods of dealing with disputes can be provided for through Codes of Conduct and trustmarks and also through alternative dispute resolution schemes which provide for cost-effective redress outside the court system.

D. Conclusion

Electronic commerce gives rise to new ways of infringing intellectual property rights. These new threats need to be explored in order to ensure that the right holders are protected under existing legislative provisions. Products and services comprising IPRs are such an important part of electronic commerce that this area should not be overlooked

To encourage and facilitate the development of business to consumer electronic commerce measures for enhancing consumer confidence must be taken into account.

The issues arising from this section on protection of legal rights include the following:

- Impact of domain names on trademark law
- New forms of possible trademark infringement such as meta-tags, deep linking and framing
- Liability of ISPs for copyright infringement
- Development and legal protection of copy protection measures
- Ensuring adequate levels of consumer protection are provided for electronic commerce, particularly in relation to the provision of information and use of payment cards
- Access to adequate dispute resolution mechanisms.

E. Further reading

WIPO, *Intellectual Property on the Internet: A survey of the issues*, 2003, available from http://www.wipo.int/ebookshop

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999), available at http://www.oecd.org/dataoecd/18/13/34023235.pdf

V. LEGAL DETERRENTS

Electronic commerce gives rise to new security risks and new ways of committing crimes. The global access which the Internet provides, while beneficial from a commercial point of view, also opens up many opportunities to the cyber criminal. For instance, while the Internet allows us to enter into commercial agreements on an international level it may also enable the cyber criminal to get access to the computer systems of enterprises on the other side of the world.

A. ICT crimes

The use of the information society has given rise to various new types of crime and new ways of committing existing crimes such as money laundering, fraud and terrorist attacks.

New forms of criminal activity include:

1. Denial of Service Attacks

Denial of service attacks are methods of interrupting the proper functioning of a website. The attack on the website involves the sending of high volumes of bogus requests for information which will slow down the performance of the website or may overload it to the point where the system hosting the website will crash. In order to carry out such attacks anonymously the activity will often involve the use of third party computers which are controlled by the perpetrator without the owner's knowledge. These computers are instructed to bombard a website until the system is no longer able to function.

2. Viruses and malicious code

These are programs which are designed to run on home and office computers. They have various destructive intents which may permanently or temporarily disable a computer. Some programs such as worms are self replicating and can therefore infect large numbers of systems in a very short space of time.

3. Unauthorized access

Unauthorized access to electronic data or to a computer system can result in the misuse of that data. For example there have been several instances where the credit card databases of various companies have been fraudulently accessed and the credit card details of all of the customers of the company posted online.

B. Regulating ICT crime

The development of communication technologies has not only resulted in new ways for crime to be committed but also provides different methods for investigating crimes. A particular method which has been used to prevent and to deal with information and infrastructure breaches is that of emergency response centres, such as the Computer Emergency Response Team (CERT) at Carnegie Mellon University in the United States.

Criminal procedural law provides law enforcement agencies with certain powers to investigate criminal activity such as the right to intercept communications and to search and seize items thought to be involved in the criminal activity. The development of information and communication technologies has created new issues in relation to these procedural powers. For example, it is no longer simply a matter of taking away the computer that an alleged criminal was using but instead it may be necessary to ensure measures are taken to prevent data being lost or deleted. There is also the possibility that criminal activities may extend across several jurisdictions thereby making the tracing of activities and the enforcement of regulations much more difficult.

Many jurisdictions have introduced new regulations designed to prevent or at least deter computer Crime. These regulations generally criminalize unauthorized access to a computer system, commonly known as "hacking", as well as the unauthorized interference of a computer or the programs and data that it holds, through the use of "viruses" and others forms of malware. Among the SPECA members, Azerbaijan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan have all adopted provisions to criminalize conduct targeting a computer's confidentiality, integrity and availability[27].

The areas where it is considered that amendments need to be made to criminal procedure law, in order to enable law enforcement agencies to operate efficiently, are in relation to:

- Search and seizure;
- Interception of communications; and
- Regulation of cryptographic products.

1. Search and seizure

The search and seizure of electronic information may be particularly difficult to instigate due to the technological developments. Changes to the law need to take into account various factors such as the ability to maintain the integrity of evidence from the time it is seized until it can be presented in court, or the ability to overcome cryptography, or other technical aspects, that may make it very difficult to access information. In order to achieve this there must be suitable funding in order to train employees in suitable forensic skills to be able to access and carefully preserve the information obtained.

[27] For the relevant criminal code provisions see http://www.crime-research.org/library/Criminal_Codes.html

2. Interception of Communications

Although interception of communications is not a new field, the type of communications which may need to be intercepted has dramatically expanded to include Internet communications, mobile telephones and other communication systems. Determining which systems to intercept and whether regulations enable the interception of particular types of communication are all issues to be determined.

Regulations in this field therefore need to be technologically neutral to deal with new forms of communication technology. There also needs to be consideration of how interception will be facilitated and whether other parties such as communications providers need to be involved, for example in maintaining intercept capability. There are also questions as to whether certain data should be retained and for how long, and who bears the cost of this.

3. Regulation of Cryptography

Cryptography is an important tool in protecting and securing information. With the growth of information and communication technologies there has also been rapid expansion in the use of cryptography. Even standard applications such as Internet web browsers and email applications readily use encryption technologies to make their software capable of secure communications.

There has been concern that such technologies would be used for a variety of criminal purposes. Some countries have therefore placed restrictions on the use or import and export of such technologies. Kazakhstan, for example, regulates the import and export of cryptographic products, as well as domestic development, manufacture, repair and sale[28]. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies has provided a level of international harmonization on this issue[29].

Strict controls over the use of cryptographic products may however create unnecessary restrictions on their use within business organizations. This has led to jurisdictions such as the United States easing its regulatory control over certain types of encryption technology. The OECD has produced a guide for governments in this area in its Guidelines for Cryptography Policy[30].

[28] Resolution No. 1037 Article 266 (30 June 1997) and Regulation No. 29; and Resolution No. 967, Article 240 (13 June 1997) and Regulation No. 27, respectively.
[29] http://www.wassenaar.org
[30] http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm

C. International cooperation

In the field of cybercrime international coordination and cooperation is vital. Cybercrimes are not limited to national boundaries and the detecting and prosecuting of these activities will likewise necessarily cross these boundaries. Cybercriminals may choose to route their communications through several jurisdictions in order to try to avoid detection and likewise the evidence of their crimes may be located across a variety of jurisdictions.

Multinational agreement to provide for assistance in the investigation and prosecution of crimes is therefore necessary. In 2005 the Virtual Global Taskforce was established by Interpol in connection with national forces in the United Kingdom, the United States, Australia and Canada to deal with child pornography.

There have been several initiatives designed to promote international coordination in this area including the OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security[31].

The Council of Europe has drafted a Council of Europe Convention on Cybercrime which since 2001 has been signed by 38 out of 47 members of the Council of Europe; although Azerbaijan, as the only SPECA member country who is also a member of the Council of Europe, has not yet signed. Canada, Costa Rica, Japan, Mexico, South Africa and the United States are also signatories to the Convention[32]. The Convention addresses issues of substantive and procedural criminal law, which Member States are obliged to take measures to implement in national law, as well as issues of international cooperation.

In terms of offences, Section 1 of the Convention distinguishes four categories of offence:

- "Offences against the confidentiality, integrity and availability of computer data and systems": i.e. Illegal access, illegal interception, data interference, systems interference and misuse of devices (arts. 2-6).
- "Computer-related offences": i.e. Forgery and fraud (arts. 7-8).
- "Content-related offences": i.e. Child pornography (art. 9)
- "Offences related to and infringements of copyright and related rights" (art. 10).

Section 2 of the Convention addresses procedural provisions that Member States are obliged to implement in national law. These include measures to enable the "expedited preservation of stored computer data" (art. 16); "expedited preservation and partial disclosure of traffic data" (art. 17); the production and search and seizure of computer data (arts. 18-19); the "real-time collection of traffic data" (art. 20); and the interception of content data (art. 21). Section 3 addresses the issue of jurisdiction (art. 22).

[31] http://www.oecd.org/pdf/M00034000/M00034292.pdf
[32] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

In terms of international cooperation, the Convention addresses issues of extradition (art. 24), mutual legal assistance between national law enforcement agencies (arts. 25-34) and the establishment of a 24/7 network of points of contact to support such assistance (art. 35). The contact network is based on a concept first established among the G8 states to facilitate cooperation through informal channels of communications, to supplement the formal mutual legal assistance procedures. The network already has over 39 participant countries.

The comprehensive nature of the Convention, as well as the geographical spread of its signatories, means it is likely to remain the most significant international legal instruments in the field for the foreseeable future. In 2005, the international police organization, Interpol, adopted a resolution describing the Convention as "providing a minimal international legal and procedural standard" and recommending that its 186 member countries consider joining it[33]. All SPECA member countries are members of Interpol.

After the adoption of the Convention in 2001, an additional protocol to the Convention was agreed by member states, "concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems", in January 2003[34]. Such issues were considered during the drafting of the main instrument, but consensus could not be reached, therefore the approach of drafting a separate instrument was agreed.

D. Conclusions

The Council of Europe Cybercrime Convention lays down clear provisions on the type of conduct which should be criminalized and the procedural requirements needed to assist in the investigation and prosecution of such conduct. It is therefore a very good starting point for any jurisdiction attempting to strengthen its regulatory provisions on cybercrime.

The issues arising from this section on legal deterrents are the following:

- Regulations should be amended to incorporate new forms of criminal activity
- Criminal procedural methods should be adapted to take into account the new types of criminal activity

Levels of international cooperation and enforcement should be maintained and enhanced.

E. Further reading

Explanatory Report to the Council of Europe Convention on Cybercrime (ETS No. 185), available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[33] http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp

[34] European Treaty Series No. 189 ('Additional Protocol').

VI. CONCLUDING REMARKS AND RECOMMENDATIONS

This guide reviews the main legal and regulatory issues raised by the adoption of ICTs and their deployment in eCommerce, eApplications and eServices, whether for adoption in a business or consumer environment or in respect of public administration. The guide also provides suggestions of how to address any identified issues in order to promote harmonized law reform to promote eCommerce and related activities; as well as constrain, where necessary, certain harmful behaviours for the protection of SPECA member countries and their peoples.

Concerns about the legal validity, enforceability and admissibility of legal acts carried out electronically can hinder the take-up of eCommerce. Legal uncertainty constitutes a barrier to adoption whether or not the concerns are in fact real, since people and entities will often not be in a position to discover the true legal situation and may choose to be risk averse. National laws, regulations and administrative practices will often require that legal acts be executed through the use of physical documents, together with signature and witnessing procedures, which preclude the use of electronic alternatives. Such requirements of form are often as much to do with inertia and innate conservatism within public authorities, including the judicial system, as they are the subject of specific legal provision. As such, while law reform explicitly recognizing the validity, enforceability and admissibility of electronic means of communication is a critical step towards establishing legal certainty, it is also important that governments embark on a campaign to promote the use of such techniques by public officials and administrators.

The desire to facilitate eCommerce and create legal certainty has received considerable attention among international intergovernmental institutions. As such, considerable progress has been made towards promoting a harmonized approach to the various issues raised under the legal certainty category. The most important forum for addressing such issues has been the United Nations Commission for International Trade Law (UNCITRAL), through a series of reform initiatives in the area, dating from 1985 until its Convention in 2005.

In terms of legal security, the concern is to ensure that eCommerce, eApplications and eServices are deployed in a secure manner. Security concerns extend to issues of authentication (e.g. knowing with whom you are communicating); integrity (e.g. knowing that what has been communicated has not been changed); confidentiality (e.g. knowing that no unauthorized person has had access to your communications); availability (e.g. knowing that the system will be available when required), and accountability (e.g. knowing that a record of events can be generated at a later date). While security primarily involves physical, organizational and logical measures, the law can facilitate the adoption of such security measures. Particular attention has been given to two areas where the law has played a key role in the promotion of legal security – electronic signatures and data protection. The former focuses on the desire for legal acts carried out electronically to be authentic and have integrity; while the latter is concerned to prevent the abuse of personal information obtained in the course of eCommerce and related activities.

Electronic signatures straddle the legal certainty and security categories. In terms of legal certainty, requirements for legal acts to be “signed” mean that electronic alternatives to the

traditional handwritten signature should be given legal recognition. However, since such requirements are often based in security concerns, the policy issue is to what extent different types of electronic signature should be granted legal recognition. Techniques range from the typing of a person's name at the end of an email, to the use of complex cryptographic techniques supported by an infrastructure of trusted third parties, generally referred to as certification authorities, capable of verifying the veracity of the techniques used. The approach taken by countries can be broadly distinguished into two streams, those adopting a permissive, technology and methodology-neutral regime and those being more prescriptive about what techniques are considered acceptable and establishing a regulatory regime designed to support such an approach. Based on market developments to date, the former approach is recommended as more appropriate for developing countries, such as the SPECA member countries.

Data protection laws are primarily concerned with the use and abuse of personal information, i.e. data that directly or indirectly identifies an individual. One element of such regimes concerns the need to implement appropriate data security measures, to protect against both accidental and deliberate interference with such data. In some countries, such as the United States, entities are also required to notify persons or regulatory authorities when they have been subject to a breach of security. Data protection laws are not often seen as directly facilitating the development of ICTs and eCommerce. In addition, the relatively low level of penetration of ICTs among the general population within developing countries reduces the likelihood that large-scale abuse of personal data is taking place. In the short term, the most likely policy driver for the adoption of data protection laws is to encourage entities in developed countries to locate their outsourced data processing facilities, since concerns about data security and privacy within developed countries are seen as a potential obstacle to such off-shoring.

The section on matters of legal protection addresses two key issues, the protection of intellectual property assets and the protection of consumers against unscrupulous traders in an online environment. There is a high level of international harmonization in respect on the substantive protections granted to the major forms of intellectual property, including patents, trademarks and copyright. Differences often arise with respect to national procedures governing the granting and enforcement of such rights, which are beyond the scope of this report. Attention has been given to some of the areas where the growth of the Internet as an environment for doing business has challenged existing regimes and/or has generated new issues for policymakers to confront. The interaction of national trademark regimes and the international domain name system and related practices is a clear example of the challenges confronting on-line businesses.

Consumer protection laws are generally designed to protect consumers on the basis of an inequality in bargaining power and an inability to adequate protect against unscrupulous practices. Governments have a traditional role as guardian to those perceived as being in the weaker position in commercial arrangements. However, consumer protection initiatives can also be viewed as a demand-side mechanism to support the development of eCommerce. If consumers trust the Internet as an environment in which to engage in an expanding range of their daily activities, from simple transactions to the submission of tax returns, then eCommerce will grow.

There are several consumer protection concerns that must be addressed. Because of the anonymity of the Internet it is more difficult to verify the identity of persons interacting on the Internet. This can be addressed, in part, through the legal security techniques discussed above. A related issue is that of applicable law and consumer redress in cross-border transactions. Not only is it often unclear which law applies to a transaction, but it will also be much more expensive and difficult for consumers to obtain redress if things go wrong. In an attempt to address such concerns, cooperative mechanisms have been established between national consumer protection authorities and alternative on-line dispute resolution procedures are being developed.

Another broader concern affecting consumers, as well as citizens in general, is that of social exclusion. Large parts of the world's population continue to have no access to the telecommunications infrastructure, no access to computers or are computer illiterate. Such "digital divide" issues are beyond the scope of this report, but must always be borne in mind by policymakers.

The final section on legal deterrents was concerned with the criminality that inevitably exploits the opportunities presented by ICTs. Law reform initiatives have tackled both substantive and procedural criminal law. In terms of substantive law, national criminal codes may not adequately cover the involvement of ICTs in the criminal conduct, while new types of crime emerge, such as hacking and viruses, which require *sui generis* provisions. Procedural criminal law concerns the powers of law enforcement agencies to be able to investigate and prosecute those engaged in criminal acts. New powers have been required to support law enforcement efforts in an eCommerce environment.

A. Law Reform

One major issue for countries with economies in transition is how to successfully take the process of law reform from initial recognition of the issue and the preparation of draft measures to their formal adoption by the national political institutions and implementation in a manner that has a real impact on business and administrative attitudes and practices.

Addressing the process of effective law reform will often involve a number of elements and steps. First, there is the need for express political commitment to the law reform process at the highest level of governments. Second, a relevant government ministry must claim ownership over the matter and be prepared to devote sufficient internal resources, both to carry out the necessary work internally as well as liaise and coordinate actively with other relevant stakeholders in the process, particularly other ministerial departments. A third element is the need to identify and appoint relevant technical and legal expertise to support the lead ministry, internal to the authority and/or external, whether located nationally or internationally. The work of the expert(s) must then be supported through the establishment of a stakeholder review group, chaired by the lead ministry, including representation from the public and private sectors. Obvious potential candidates include people from the ministry of justice, the national law reform commission and local commercial practitioners. Any draft measures prepared by the experts would then be subjected to a process of scrutiny by the stakeholder review group, which should both substantially improve the quality of the final draft and facilitate awareness and build support for the proposal among the wider community. Finally,

the draft measure should be steered through the parliamentary process by the lead ministry, ensuring that steps are taken to fully explain the purpose, nature and consequences of the measure to the political representatives.

Envisaging law reform has always been substantially easier than achieving law reform. To successfully address the legal aspects of ICT development requires that states devote as much time and resources to the process of law reform as to the various subject matters identified in this guide.

B. Recommendations

This guide highlights some important issues that the SPECA member countries may take into consideration in their future policy reforms with respect to the ICT sector. The main among them are the following:

- Political commitment from the Heads of State of the SPECA member countries would be a key precondition for successful law reforms in support of national ICT strategies within a specified timescale.

- Further efforts need to be made to familiarize SPECA member countries with the legal and regulatory implications arising from the use of ICTs and eCommerce.

- Efforts should be made to facilitate a transfer of experience in the area between SPECA member countries, though regional training seminars and workshops.

- SPECA member countries would be better off if they were better aware of international best practice on the various topics and the existence of model laws and other international instruments. Sufficient existing model laws and legal instruments exist to assist SPECA member countries in the various issues identified. In particular, it is recommended that SPECA member countries consider signing and ratifying the Council of Europe Convention on Cybercrime (2001) and the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

- Coordinated and harmonized initiatives should be promoted among SPECA member countries, enabling significant savings in terms of time, experience and resources required for such activities.

- All the different stakeholders, from business, public administration and civil society, need to be represented in discussions at a country level aimed at facilitating the law reforms.

- SPECA member countries need to better recognize the special role that public administrations can play in the adoption and take-up of electronic means of doing business and communicating with government.

* * *