The Regulatory Framework for E-Commerce –
International Legislative Practice

May 21, 2002

It is not easy to identify a single model law for the Internet – the issues comprising the legal framework within which the Internet flourishes are too disparate and legal systems in various countries are too different. Nevertheless, there are certain issues that any nation needs to consider in assessing its policies and there are certain international models to draw upon for elements of an Internet regulatory framework. This memorandum offers an outline of key issues that comprise an e-commerce framework and points to the relevant international models, in seven areas: telecommunications liberalization, recognition of electronic documents (including their legality as contracts and evidence), consumer protection, electronic funds transfer and the use of credit and debit cards, dispute resolution, ISP liability, and domain names.

Part I. Telecommunications Liberalization

Perhaps the single most important thing that any country can do to improve the climate for e-commerce is to "liberalize" its telecommunications introducing competition at all levels (local, long distance and international) and for all technologies (wireline, wireless, and cable), and by privatizing its state-owned carriers. (International consensus today is that enforceable competition should come before privatization, but the timing and structuring of both pose many complex issues.) Telecom liberalization is important because the Internet depends heavily on the telecommunications system.

It has been demonstrated that telecommunications competition and privatization –

- drive down prices and thereby make all services, including the Internet, more affordable;
- spur innovation, infrastructure development, and improvements in the quality of service;
- attract foreign investment that will support infrastructure modernization and expansion.

Countries should examine their laws, regulations and licensing practices to identify and remove barriers to competition, innovation, and the development and deployment of advanced services, taking into account the global trend toward convergence of voice, text and video technologies. Recommended steps include:

- require competition in local loop, long distance and international services
- allow the use of cable TV networks for the delivery of two way services;

- allow the use of Internet for voice (VoIP);
- open up full use of the wireless spectrum, including technologies that use wireless to span the last mile;
- permit the creation of an Internet exchange point (IXP) for the country and in the major cities, to avoid expensive international transit for Internet communications;
- remove unnecessary licensing requirements and streamline other licensing processes

Primary international models:

- The WTO Annex on telecommunications: http://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm (1997) and the WTO principles on the regulatory framework for basic telecommunications regulation http://www.wto.org/english/news_e/pres97_e/refpap-e.htm (1996)
- The European Union directives dealing with telecommunications and information technology http://europa.eu.int/information_society/topics/telecoms/index_en.htm
- The US interconnection statute, 47 United States Code Section 251, offers a good outline of the obligations that should be imposed on incumbent carriers to promote competition.

Part II. Recognition of Electronic Documents

Purpose: to create the legal framework for recognition of electronic contracts, the admissibility of electronic evidence and the acceptability of electronic submissions to government agencies

An important step in paving the way for electronic commerce is to remove any legal obstacles to the recognition of contracts entered into by electronic means.

In many countries, the law requires certain contracts to be in writing, or to be signed. The question arises, is an exchange of electronic messages a "writing? Can an electronic notation serve as a "signature?" Other specific questions arise in the making of electronic contracts – when will an email message be considered sent, and when is it received, such that a party is bound by it? The law often has answered these questions in terms of postal mail – do those laws cover delivery and receipt of e-mail?

Similar questions arise in –

- The law of evidence – Can electronic documents be introduced in evidence in judicial or administrative hearings? What is an original in the context of electronic messages? In legal systems that require the production of the "best evidence," can electronically stored information suffice?
- Bringing e-government to regulatory requirements – When rules call for the submission to a government agency of a written application, report or form, can an electronic record suffice (assuming the government has created the technical capacity for online submission)?

Governments should amend their laws to answer these questions, permitting the use of electronic documents to satisfy legal requirements of a "writing," a "signature" or an "original." If not resolved, these questions can pose barriers to e-commerce; at the least, the uncertainty the create discourages businesses and consumers from taking advantage of e-commerce.

A. General rule on legal requirements of a writing

Provisions to address these issues can be drawn from the Model Law on Electronic Commerce, promulgated by the United Nation Commission on International Trade Law (UNCITRAL) in 1996. http://www.uncitral.org/english/texts/electcom/ecommerceindex.htm The UNCITRAL Model takes a straightforward, functional approach. Rather than requiring amendments throughout a country's entire legal code (finding every use of the words "writing" or "signature" and variants thereof), it establishes several principles of general applicability. We recommend that the following UNCITRAL provisions be included in an IT Act:

- **Legal recognition of data messages:** Information shall not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form. (Article 5.)
- **Writing:** Anytime the law requires a writing, that requirement is met by information in electronic form if it is accessible so as to be useful for subsequent reference. (Article 6.)
- **Signature:** Where the law requires a signature of a person, that requirement is met in relation to a data message if a method is used to identify that person and to indicate that person's approval of the information contained in the data message, and that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of the circumstances, including any relevant agreement by the parties. (Article7.)
- **Original:** An electronic data message meeting certain functional criteria can be treated as an "original." (Article 8.)
- **Retention of data messages:** Where the law requires that certain documents, records or information be retained, the Model Law specifies that such requirement is met by retaining data messages, provided certain specified criteria are satisfied. (Article 10.)

Exceptions: The UNCITRAL Model Law recognizes that there might be some exceptions to the use of electronic documents -- cases of special sensitivity where the existence of a signed paper original is still desirable. For example, land transactions, divorces, adoptions, and wills are categories where the law in many countries has traditionally required greater assurances that the parties have agreed on a common set of binding commitments (such as seals, signatures, or notarization requirements). The exact list of exception is up to each nation to specify, based on local considerations.

B. Evidence Law

Admissibility and evidential weight of data messages: The UNCITRAL Model Law also is the best starting point for dealing with evidentiary issues. It includes model language specifying that, in legal proceedings, nothing in the application of the rules of evidence shall

apply so as to deny the admissibility of an electronic document in evidence on the sole ground that it is in electronic form or, if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that it is not in original form. The UNCITRAL Model Law goes on to state that information in the form of a data message shall be given "due evidential weight." (Article 9)

C. Contract Law

The UNCITRAL Model also includes provisions on the formation of contracts:

- **Formation and validity of contracts:** In the context of contract formation, an offer and the acceptance may be expressed by means of electronic messages, and that a contract cannot be denied legal effect or enforceability on the sole ground that it was formed by electronic messages. (UNCITRAL Model, Article 11.) See also Article 5.2 of the EU Directive on a Community framework for electronic signatures (1999) http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf
- **Recognition by parties and attribution of data messages.** (Articles 12-13).
- **Acknowledgement of receipt, time and place of dispatch and receipt of data messages.** (Articles 14 – 15)

Special note – issues to reserve for later consideration

The foregoing provisions, if enacted based on the UNCITRAL Model, would remove immediate barriers to e-commerce. There are other distinct and more difficult questions that arise in the context of authenticating electronic documents that need not be resolved in an initial IT Act, but we mention them here since they often arise in policy discussions and are sometimes confused with the issues we discuss above:

Cryptography-based Digital Signatures: *Modern techniques of encryption make it possible to verify the identify of a person online and to link a document to a particular person, ensuring that a sender of a message is the person he claims to be. Cryptography can also ensure that a document has not been tampered with in transmission or storage. In practice, however, achieving these goals is very complicated. The challenges are more technical than legal, requiring the establishment of a public key infrastructure that can make keys available in a trustworthy way. Some governments have tried to hasten the resolution of these issues by creating a regulatory structure for licensed certificate authorities, who mange the key infrastructure. In our view, these efforts are as likely to impede the development of a PKI as to promote it, since governments, especially in developing countries, may not be able to create a regulatory structure for a complex and still evolving industry. If there is a desire to adopt a regulatory scheme for certificate authorities, the best models are the European Directive on a Community framework for electronic signatures (1999)*

http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf and the UNCITRAL Model Law on Electronic Signatures (2001) available in PDF at *http://www.uncitral.org/en-index.htm*

Electronic Notaries: *Another complex set of issues concern electronic notarization. A few countries have adopted e-notary laws, but at this point we are not prepared to endorse or recommend any specific legislation. It should be noted that many developed countries have achieved an advanced state of e-commerce without having set up procedures for e-notaries, confirming that this is not a threshold issue.*

Part III. Consumer protection

E-commerce will flourish only if the legal system enforces both commercial and consumer contracts. This means that the court system must work effectively and without imposing excessive delays or costs on those seek to invoke the power of the courts to enforce contracts or settle other disputes.

Special protections are warranted in the case of consumers. A consumer can be defined as "any natural person who is acting for purposes that are outside his or her trade, business or profession." See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (the “EU Directive on E-Commerce”). The protection of consumers consists of laws --

- prohibiting misleading advertisements;
- regulating consumer financial services and consumer credit; and
- concerning liability for defective products.

In addition, specifically in the field of online contracts and other distance contracts, rules should ensure that consumers are provided the following rights:

Notice: Prior to the conclusion of any contract, the consumer must be provided with clear and comprehensible information concerning key matters such as:

- the identity and the address of the supplier;
- the characteristics of the goods or services and their price;
- the arrangements for payment, delivery or performance;
- the existence of a right of withdrawal.

Right of withdrawal: For major online transactions and other distance contracts, consumers should be afforded a right of withdrawal. The exercising of the right of withdrawal makes it possible to cancel credit agreements concluded in connection with a transaction.

Timeliness of performance: Unless otherwise agreed to, the supplier must perform a contract within thirty days. Where the supplier fails to perform his side of the contract, the consumer must be informed and any sums paid refunded, unless the consumer agrees to accept an equivalent good or service.

Protection against fraudulent charges: Consumers should not be held liable for amounts billed to them for "unauthorized transactions." In the event of fraudulent use of his payment card, the consumer may request cancellation of payment and reimbursement of the amounts paid. Vendors should promptly refund consumer payments for unauthorized transactions or sales transactions in which consumers did not receive what they paid for. Where unsolicited goods or services are supplied, the consumer's failure to reply does not constitute consent.

International Models:

- European Parliament and Council Directive 97/7/EC of 17 February 1997 on the protection of consumers in respect of distance contracts - http://europa.eu.int/information_society/topics/ebusiness/ecommerce/3information/law&ecommerce/legal/documents/31997L0007/31997L0007_en.html.
- European Parliament and Council Directive 2000/31/EC of 8 June 2000 on electronic commerce - available in PDF at http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf and in HTML at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett

Part IV. Electronic Funds Transfer and the Use of Debit/Credit Cards

Relevant banking laws must be amended to accommodate payment through credit/debit cards, for both domestic and international e-commerce. This is a complex area of the law, but an important one. There are many types of "e-payments" including automated clearing house (ACH) funds transfers (including electronic checks), credit card payments, and stored value or e-money payments. There are also high value payments made between banks and separate laws often cover these.

One of the challenges of establishing an effective e-commerce regime is identifying a payment mechanism that can be used effectively in an online environment. Developing a viable payment option will require resolving certain issues of security, liability and taxation. In addition, there may be a need to establish legal authorization to permit the use of new electronic currencies in some instances.

Credit cards and bank transfers are the most prevalent forms of online payments used in the US. Nonetheless, many consumers remain reluctant to use credit cards online due to concerns about maintaining the security of their credit card information. Furthermore, credit card usage is not common in many parts of the developing world. In part to address these

challenges and otherwise facilitate high volume and low value purchases over the Internet, a variety of alternate payment mechanisms, including smart cards, e-cash, digital cash and cybercash, also have been introduced. A variety of materials addressing the use of these payment systems are listed below.

It is also important to recognize the need to incorporate consumer protection components into any regulatory structure adopted for payment mechanisms. The European Union, for example, has announced the urgent need for Community level legislation establishing a right and basic conditions for refunds in the event of non-authorized transactions and non-delivery of merchandise.[1] Legislation already exists in the US establishing rules to protect consumers in the event there is unauthorized use of their credit cards.

International models and resources include:

A variety of international models may provide useful perspectives for analyzing the legal issues involved with online payment mechanisms:

1. The Bank for International Settlements has a Committee on Payment and Settlement Systems, which produces many reports including a "Survey of Electronic Money Developments" in 160 countries and also "Core Principles for Systematically Important Payment Systems:" http://www.bis.org/cpss/cpsspubl.htm

2. The European Union has a directive on electronic money institutions: DIRECTIVE 2000/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. PDF downloads of this are available here http://www.fs.dk/uk/acts/eu/epeng-uk.htm Other EU materials include:

- EU Recommendation 97/489/EC addresses transactions by electronic payment instruments and contains provisions governing liability for unauthorized transactions, and treatment of electronic transfer of funds, including home banking.

- EU Directive 87/102/EEC allows consumers to exercise claims against the grantor of credit under certain circumstances. This directive does not, however, apply to debit or charge cards.

- EU Directive 97/7/EC protects consumers and grants them the right to request cancellation of a transaction and to have their payments refunded where there has been fraudulent use of their credit cards.

[1] See also OECD, Working Party on Information Security and Privacy, *Building Trust in the Online Environment: Business to Consumer Dispute Resolution, Joint Conference of the OECD, HCOPIL, ICC, Report of the Conference, the Hague, 11-12 December 2000*.

· EU Directive 2000/28/EC deal with electronic money issues and, seek to ensure technical security, and provide that electronic money may be issued only by supervised institutions that meet certain legal and financial standards.

3. In the United States, there is a model uniform state law on money services including "stored value" services and providers of e-payments. The Act can be accessed online here: http://www.nccusl.org/nccusl/default.asp ("Money Services Act").

4. UNCITRAL has a model law on International Credit Transfers (i.e. wire transfers): http://www.uncitral.org/en-index.htm (choose "Adopted Texts," then click on "International Payments"). This Model Law, adopted in 1992, deals with operations that begin with an instruction to a bank to place at the disposal of a beneficiary a specified amount of money. It covers such matters as the obligations of a sender of the instruction and of the receiving bank, time of payment by a receiving bank, and liability of a bank when the transfer is delayed or other error occurs.

5. As for credit cards or ACH funds transfers, these are regulated by private agreement (between financial institutions, participating merchants, etc) and then through consumer protection laws. In the United States, the bank regulators have adopted a regulation called "Regulation E" which specifies the protections for consumers using credit cards (what happens if a card is stolen, what happens when a consumer says that a mistake was made or a product was returned).

Part V. Dispute Resolution

Disputes between buyers and sellers (e.g., failure to deliver the requested merchandise, disputes regarding payments, etc.) are inevitable in any commercial environment. However, concerns or uncertainty regarding how such disputes will be resolved in an online environment may make parties hesitant to purchase items electronically. In these e-commerce related disputes, where relatively small amounts of money are frequently at issue, recourse to the courts is often not a practical option for most consumers and small businesses. To help alleviate these concerns and instill consumer confidence in online systems, it is advisable to encourage the use of mechanisms that permit a fast, low-cost and easily accessible resolution of large numbers of low value transactions (i.e., disputes that are especially likely to result from business to consumer sales). Accordingly, governments that are interested in establishing effective e-commerce regimes should give thought to permitting and encouraging the use of electronic alternate dispute resolution ("ADR") mechanisms, in addition to providing recourse through the national court system.

The creation of these ADR mechanisms is especially important in markets where the courts are slow or ineffective, or in instances where several countries within a geographic region are seeking to develop a common market for cross border transactions.
For example, the EU Directive on E-Commerce requires Member States to amend any national legislation that is likely to restrict the use of such out of court settlement mechanisms. In addition, in May of 2000, the European Commission initiated a European Extra-Judicial Network for settling out of court consumer disputes (EEJ-NET). The EEJ-NET will establish a network

of national dispute resolution programs and link them to national bodies, thereby providing an EU-wide complaints network. This project will cover any consumer dispute over goods or services, and is expected to reduce costs, formalities, delays and obstacles in resolving cross-border disputes, thereby improving consumer confidence in electronic commerce.

It is important to note that the establishment of ADR mechanisms need not result from government initiatives. Instead, the private sector, local non-governmental organizations or other "neutral" entities may create and effectively administer these programs. Governments, however, should work with other interested stakeholders to develop and encourage these mechanisms. In addition, to the extent that existing legislation would hamper or prevent the establishment and use of ADR mechanisms, governmental reform of the legal regime may be necessary.

International Resources and Models:

- EU Directive on E-Commerce, Article 17. The E-Commerce Directive is available in PDF at http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf and in HTML at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett

- Council Resolution of April 13, 2000 on the creation of a Community network for out-of-court settlement of consumer disputes.

- See Organization for Economic Cooperation and Development, Building Trust in the Online Environment: Business to Consumer Dispute Resolution, Joint Conference of the OECD, HCOPIL, ICC, Report of the Conference, The Hague, 11-12 December 2000, DSTI/ICCP/REG/CP (2001).

- For examples of operating ADR programs in Chile, see Camara Nacional de Comercio Servicios y Turismo de Chile. Programa Singolpes. See http://www.singolpes.cl. (In Spanish.) See also a program established by the Santiago Chamber of Commerce at http://www.camsantiago.com.

Part VI. ISP Liability

Another important element of a successful e-commerce regime is providing mechanisms to limit the civil and criminal liability of Internet Service Providers ("ISPs") where these entities are acting as intermediaries who are merely providing backbone access to the Internet. This approach is needed to protect ISPs from a variety of potential claims, including copyright infringement, unfair competition, misleading advertising, defamation and trademark infringement, where the offending activities are conducted by third parties who are using an ISPs services.

This liability limitation for ISPs has been enshrined both in U.S. and E.U. laws. For example, the European Union E-Commerce Directive includes language that limits the liability of "intermediary Information Society service providers" (i.e., Internet Service providers and carriers that transmit or host information provided by third party users of the service). This directive limits liability for ISPs in three important instances:

- **Mere Conduit**. In instances where an ISP is merely providing Internet access or transmitting information provided by a third party via its communications network, the ISP is functioning as a "mere conduit." The EU Directive provides that the ISP will not be liable for the information transmitted provided that certain conditions are met (i.e., the ISP did not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission). See Article 12 of the EU E-Commerce Directive.

- **Caching**. An ISP that transmits information provided by a recipient (or user) in a communications network is not liable for the automatic, intermediate and temporary storage of that information. This limitation of liability applies only where these acts are performed for the sole purpose of making the information's subsequent transmission to other recipients more efficient.[2] Again, the ISP may lose this legal protection under certain defined conditions, such as if it modifies the information that is being transmitted. See Article 13 of the EU E-Commerce Directive.

- **Hosting**. An ISP that stores information provided by a recipient (or user) of the service is not be liable for information stored at the request of a recipient of the service. The limitation of liability applies where the service provider:
  - ß does not have actual knowledge that the activity is illegal;
  - ß is not aware of facts or circumstances from which illegal activity is apparent; and
  - ß if upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the system. See Article 14 of the EU E-Commerce Directive.

Furthermore, the E-Commerce Directive makes it clear that an ISP that is acting as a "mere conduit," or simply in a caching or hosting capacity has no duty either to monitor the information that it transmits or stores; or to actively seek facts or circumstances indicating the existence of illegal activity. See Article 15 of the E-Commerce Directive.

Part VII. Domain Names

The guidelines for management of country top level domain name do not need to be included in any e-commerce legislation that is adopted by a government. Nonetheless, this policy issue is an important one that can be integral to the development of e-commerce applications. Management of a country's domain name, therefore, should be considered as a part of the overall e-commerce strategy that is being developed by a government.

[2] Cache servers make complete copies of works in order to place them in physical locations that are closer to users. This practice improves the speed and efficiency of the network.

The creation and management of domain names also may be especially important to consider in regions that are seeking to develop common economic markets. For example, the European Union is pursuing an initiative to create ".eu", a new top-level domain name for European business. This approach is part of the eEurope Action Plan adopted by the European Council to promote e-commerce applications.

International resources or models:

· For recommended best practices for the management of ccTLDs see the ICANN website at: http://www.icann.org/cctlds/centr-2nd-best-practices-20may01.htm

Part VIII. Other Issues

We did not discuss here other issues often considered key to the enabling framework for Internet growth, such as intellectual property, privacy, and cybercrime. These and other issues are addressed in various materials found on the GIPI website, http://www.internetpolicy.net.

For further information: Paige Anderson, GIPI Counsel, panderson@cdt.org
Jim Dempsey, GIPI Policy Director, jdempsey@cdt.org