

# DRAFT

## Internet Policy Guidance for Iraq

June 2, 2003

This paper is meant to provide a framework for a discussion of policy with respect to the Internet, including aspects of policy with respect to telephone networks, in Iraq.

The paper is divided into three sections. The first section provides a moderately thorough conceptual framework for a discussion of national Internet policy in general. It motivates the second part, which consists of a discussion of problems facing present day Iraq and recommendations for short term actions that should provide an enabling environment for the growth of the Internet in the longer run. The third section is more comprehensive, and addresses the more detailed issues that are involved in establishing a comprehensive regulatory framework for e-commerce.

### I. Conceptual Framework

The Internet -- architecturally open and decentralized, abundant, inexpensive and user-controlled -- is a communications medium ideally suited for the promotion of open, democratic societies and is increasingly central to economic growth and human development worldwide. Yet, with growing concern, we see the emergence of a digital divide, as the Internet in too many developing countries remains out of reach of the vast majority of the population, its economic potential untapped.

There are many hurdles to be overcome in bridging this digital divide. But one crucial factor is policy. It turns out that the Internet is not independent of the legal and regulatory framework of individual countries. To the contrary, laws and public policies can hinder or promote the development of the Internet. Government regulation can quash Internet growth. On the other hand, the lack of clear laws can result in an environment where government officials arbitrarily and inconsistently decide what is permitted and what is forbidden, leaving Internet service providers, Web site operators and others subject to licensing and other controls with no hope of legal recourse. Sound Internet policy is a mix of regulation and non-regulation.

Nations around the world are revising their legal systems with a desire to make them "Internet ready." It is a time of great promise and great peril, as countries seek to reconcile their desire for the Internet's contribution to economic development with their fears of its destabilizing potential:

- **Misunderstandings abound.** Policymakers in many countries do not appreciate how the Internet is different from radio and TV. Nor do they appreciate the critical role of competition, especially in the telecommunications market, as well as governmental transparency and accountability

- **Regulatory controls are growing.** In a number of countries, governments are on the verge of moving from a posture of "benign neglect" toward the Internet to one of intervention and control.
- **On the ground, there is a policy vacuum.** Until now, no one has been working at the local level, country-by-country, to develop Internet policy reforms based on rule of law, transparency, democratic principles and market-based solutions.
- **Effective policies are generated through consensus-building, controlled and directed by local private sector and non-profit partners.** For any Internet policy to succeed internationally, it must have the support of local partners and must bring together participants from the Internet industry, content providers, NGOs and the government.
- **What is needed varies from country to country.** Strategies for Internet policy reform must be developed locally and must respond to local conditions.
- **European policy developments are influencing the rest of the world.** The US is by no means the only or most relevant reference point for Internet policy.

Not surprisingly, countries are at varying stages in their policy attitudes toward the Internet.

- In many countries, there is no law on the Internet per se; as of yet, the word "Internet" simply does not appear in most countries' legislation and regulation. This absence of law has different consequences and should prompt different responses from a policy project:
- In some countries, this absence of law has allowed the Internet to develop without government interference. Greater government funding for training and Internet access in schools and universities would boost Internet development, but what would be most dangerous now would be government efforts to assert control over the Internet.
- In other countries, the absence of Internet law creates an environment of discretion where government officials arbitrarily and inconsistently decide what is permitted and what is forbidden, with the result that ISPs, Web site operators and others are subject to licensing and other controls arbitrarily or corruptly imposed with no hope of legal recourse. In such countries, a law "regulating" the Internet could be an improvement, since the law could limit the power of the government.
- In some countries, the government is trying to fit the Internet within licensing schemes designed for the scarce, gatekeeper controlled media of radio and TV, without an appreciation for the uniquely decentralized, abundant, user-controlled nature of the Internet.
- In a few countries, the Internet is already subject to excessive government regulation and the goal of reform would be to free the Internet from these restrictions.

- In all countries, a great deal of the fate of the Internet depends on rules that do not directly concern the Internet; rather, the most important rules are those requiring governmental transparency, business laws affording certainty with flexibility, and the rule of law in general. In particular, a key precondition to Internet development is the establishment of laws promoting open access, non-discriminatory pricing and fair competition in the telephone market.

Internet policy needs to understand and take advantage of those attributes that make the Internet unique:

- It is a global medium; it does not necessarily respect national borders
- It flourishes in part because it is based upon open standards and open access
- It is decentralized; there are no gatekeepers
- It is abundant; the barriers to entry are low, and for most transmission methods, there is no scarce spectrum
- It is inexpensive; everyone can be a publisher of information and a provider of information services
- It is by and large user-controlled -- e.g., encryption, filtering
- It is interactive, and the interaction can be 1-to-1, 1-to-many, or many-to-many

One of the first questions to be asked in establishing Internet policy should be whether Internet regulation is needed. Does regulation or lack of regulation help or hinder the development of the Internet? We believe that the starting point should be that regulation should only be imposed if there is a clear reason for imposing it that is consistent with the development objectives of the network. It is worth noting that legislation in a number of countries has hindered the development of the Internet, and that in countries where the Internet has flourished most, there is no comprehensive "Law on the Internet." Is the purpose of any proposed regulation:

- To give the government control or to limit arbitrary government power?
- To preserve monopoly power or to promote competition?
- To enhance user control over content and privacy or to diminish user control?
- To preserve monopoly power or to promote competition?

Internet regulatory policy needs to contain a wise mix of regulation and non-regulation. We suggest as a start, that:

- No new laws are required for Internet content.
- Those who create the content should be responsible for it, not the ISPs that carry it.
- In most cases, user empowerment should be preferred over content regulation: Users, parents and schools can choose from among a variety of filtering and blocking software to protect children from harmful content.

One can ask what legal framework is needed for the Internet to flourish. Many of the legal principles favoring Internet development are principles of general application to business law and the field of telecommunications, and are not specific to the Internet. One such principle is transparency:

- Regulatory and legislative process should be transparent and open.
- Citizens should have access to all laws, decrees, regulations and judicial rulings including draft laws and regulations in print and through the Internet.
- No one should be subject to any rule that is not published.

In order to take advantage of the very substantial contribution that e-commerce can make to economic development, good Internet policy should include effective support for entrepreneurship:

- Business laws and financial systems should allow start-ups to achieve legal status and pursue business without delay.
- The law should reduce risk of arbitrary government action and provide certainty, while allowing flexibility.
- Regulatory bodies should be independent - there should be a clear separation between the (telecomm) regulator and companies (carriers).

The growth of the Internet depends critically upon having an efficient and effective classical telecommunications system. Good telecommunications policy is so much a prerequisite to effective Internet use that one should consider the two subjects together. Some of the principle underlying an effective telecommunications and Internet policy with respect to industry structure are:

- \* Privatization of governmental PTTs; internationally, telecomm policy favors such privatization actions
- Competition: Competition can drive down prices, promote investment and spur the deployment of affordable services. Existing networks should be open to competitors.

- International standard: full and fair competition in local exchange service, leased lines, long distance, and backbone; among wire line, wireless, and cable; and among ISPs.
- \* Non-discrimination: ISPs should have access to network facilities on same terms telecomm companies offer their own ISP affiliates.
- \* Goods and services should be open to foreign competition; trade barriers should be low. EU directives and WTO agreements support this principle.

Licensing requirements should be predictable and consistent and should not impede competition.

- There is no need for licensing of ISPs.
- Licensing should not be used as a means of restricting market entry.
- The marketplace and ordinary business law are sufficient to protect consumers.

Similarly, technical standards should be established in such a manner that competition is not impeded:

- There is no need for individual licensing or approval of equipment.
- Conformance to international standards, based on open standards, broad participation, and interoperability, will promote innovation, growth and expanded access.

Two of the most important determinants of Internet growth and usefulness are the availability of local voice telephone lines and the price associated with the use of those lines for dial-up access to the Internet. With regard to these determinants, we observe that:

- Telephone pricing policies, especially per minute metering for local calls, may inhibit the growth of the Internet.
- Flat rate pricing for local telephone calls can improve Internet affordability, as can flat rate pricing of Internet service.
- The principle of universal service for basic telecom access supporting voice and data is an international norm.
- Competitive pricing can lower prices and spur development, but should be balanced with protection for residential and rural customers.

There are other considerations that are perhaps more important for guiding policies in other areas that are useful to note:

- The government education system has an indispensable role in producing both technicians knowledgeable in telephony, networking, and programming, and a broader

population base that understands the Internet as a tool of commerce, government and human development.

- Public access at libraries and other public points are useful both for access to the Internet and to boost public awareness of it and what it can do..
- Industry, governments and NGOs all should support the creation of Web site content in local languages.
- Support should be given to the development of standards for browsers and other software that displays local alphabets.

Finally, in addition to the foregoing areas, issues specific to ICTs (Information and Communication Technologies) and the Internet must eventually be addressed:

- Intellectual property: there must be adequate protection for intellectual property so that content providers can earn a profit.
- Taxation: Internet tax policy should neither penalize e-commerce nor inhibit the offering of electronic services.
- Digital contracts: laws recognizing credit cards, cybercash and digital signatures need to be put into place as e-commerce begins to become important in a country's business
- Consumer protection:
- Privacy protection: OECD guidelines and the EU privacy directive have useful material for studying what needs to be put into place at the national level.
- Computer crime: effective measures to deal with online fraud, hacking while preserving anonymity and limiting government monitoring

## *II. Short Term Actions Considerations*

The agenda of policy considerations above has been provided to give a broad overview of what must eventually be considered to obtain a robust and empowering environment for the Internet, as well as other ICT media and services, to grow and prosper. All of the above points will eventually be important for an Iraq administration to consider.

However, the needs of Iraq with respect to Internet policy at the present time are considerably simpler, but no less important. The question resolves to the following: "What are the important actions to take now, and what are the important policies to put into place now, so that what is built in the future based upon them will produce the desired long run effect?" The current state of affairs in Iraq may well not permit any formal policies or regulations to be promulgated — indeed, it does not yet have the administrative or legislative apparatus to

construct or enforce them — so one must focus upon principles such as are contained in the above section and upon setting the right directions for the future.

In addition, it is premature for a country like Iraq, with scarce Internet deployment, deficient computer proliferation, destroyed PTT infrastructure and most importantly a vast majority of its population with meager buying power and no access to training and education facilities, to consider any comprehensive approach to Internet policy. Today Iraq needs computer and Internet literacy workshops to develop some capacity building expertise within the country as much as it needs policy attention. E-Commerce and e-Government will come later; they will grow in parallel with the natural build up of a critical mass of Internet users within Iraq. It may well take the Iraqi technology engaged and trained diaspora three to four years to venture back to Iraq and start making a difference, assuming that peace and some sort of a democracy would prevail.

It is very important that assistance to Iraq in the area of Internet also focus on capacity build up close to the community of Iraqi residents, as the Internet will provide them with a window to the world. The faster such an Internet-knowledgeable community can grow, the more rapidly the detailed policy issues become relevant.<sup>1</sup>

These considerations suggest that the enablement of the Internet in Iraq at this time is as much of a development issue as it is a policy issue. Initial policy guidance should set the basis for the evolution of a policy environment that will facilitate rapid growth and exploitation of the Internet. Subsequent to that, the growth of the Internet will be facilitated more by investment in physical infrastructure and multi-user access points, in generating useful local content and services using the web, and in investing both in the technical skills of Iraqis to extend the net and in Internet use skills of many more Iraqis so that they can exploit its content and services.

We suggest several issues that should be confronted at an early stage. While some of these issues are pure policy issues, others are either developmental or mixed.

1. The Internet still depends critically upon the use of the classical voice telephone system, especially the fixed line system. It is essential for this reason, and for others, that competitive principles be embodied in the reconstruction of the voice telephone industry. No actions should be taken, especially in terms of licenses or license terms granted, that would deny eventual competition at any level of the telephone system, fixed line or cellular, or would restrict it in any way unconnected with rational resource allocation. Exclusivity of service should be avoided. In almost all countries, low access prices have been achieved through the existence of competitive markets for ICT goods and services, and while it may not be possible to introduce competition now, no barriers should be erected to their introduction later. Given a chance, competitive services will soon emerge and play their part in making access affordable. No barriers should be placed in their way.
2. Make electronic infrastructure available on a non-discriminatory basis. ISPs ((Internet Service Providers) should be able to obtain circuits in the same manner as any other

---

<sup>1</sup> These observations were contributed by Dr. Nabil Bukhalid, Director of Information Technologies at the American University in Beirut, Lebanon.

consumer, especially higher speed leased lines that will be essentially for a robust Internet infrastructure as business and government begin to use the network heavily. If a voice carrier also offers network services, transactions between the parent and subsidiary of the voice carrier must be at arms length, and on a basis consistent with its dealings with competitive network services.

3. ISPs should be able to offer Internet services without prior approval. Licensing should be kept to an absolute minimum necessary for essential government operation, and the preferred position is that ISPs should be treated no differently than other businesses with regard to establishing a business. As noted above, one needs to ask the question "why license ISPs," and then only derive licensing requirements from applicable responses. We believe that the reasons for licensing are substantially outweighed by the reasons not to license. Licensing may confer rights, but it also is likely to confer obligations and delays that are barriers to entry. Using physical transmission media such as copper or fiber, there is no issue of colliding in the use of a scarce resource such as spread spectrum. Using popular wireless technologies such as those using the IEEE 802.11x protocols, all competing transmissions use the same spectrum (in the 2.4 and 5.5 Ghz range), and the spread spectrum technology that these protocols use has its own method of minimizing the effects of interference.
4. E-commerce should be anticipated by ensuring that the new civil code includes a statement that no document shall be denied legal effect solely because it is in electronic form. While the third section of this paper provides considerable detail about the legal and documentation issues involved in e-commerce, in the beginning it may be sufficient just to declare that there should be no legal prejudice against documents just because they are in electronic form. There are to be sure more complex issues, but in the beginning, such a statement legitimizes the use of e-documents, and paves the way for an expansion of their use, and consequently a deepening and refinement of the policy issues surrounding them.
5. In reconstructing the governmental structure, provision should be made at the outset for an independent regulatory authority. Such an authority will be needed more for broadcast media than for the Internet, but the principle of its early establishment and its independence is the key objective to be established as early as possible.
6. Helping an Iraqi Internet industry to emerge and be healthy is an important part of the reconstruction of the media environment in Iraq. In particular, the country will need an emerging set of entrepreneurs who will become Internet service providers (ISPs) as quickly as possible. ISPs serve as intermediary organizations between end users, both individuals and organizations, and the global Internet, and their success is essential to the success of the Internet in Iraq. Government policy needs to encourage these entrepreneurs by assisting them to start their business quickly and easily, and to offer service on a competitive basis to all potential subscribers.
7. The Internet industry in Iraq will also want to establish as early as possible an Internet exchange point (IXP). The purpose of an IXP is to allow traffic local to Iraq to stay in Iraq without having to enter the global Internet and be routed through another country, most often the United States or a country in Europe. In spite of the fact that this seems like a simple and



economical concept, IXPs have often materialized in developing countries later than one would expect. An IXP can be created by the set of ISPs in a country; it can also be an independent entity, and it can even be offered by a long haul Internet provider as a service at the point of termination of the international connection. Regardless of how it is implemented, an IXP should allow the interconnection of any ISP that wishes to connect to it, as well as any international Internet carrier that wishes to offer internal connectivity to Iraqi ISPs. There should be no barriers to entry to the IXP beyond technical competence, existence of the interface equipment, and the costs associated with providing the service.

8. The issue of content is a difficult one. In particular, there are three aspects to it that need to be considered in any policy discussion:
  - a. Internet legislation and policy needs to distinguish between carriage and content. In particular, ISPs should be regarded as providing carriage for information, and that function should incur no legal liability imposed by the content that is carried. Of course, an ISP may also be a supplier of content, and that content should be subject to policy regarding content. However, ISPs should not be liable for any aspect of the content which they transmit in their function of providing data carriage.
  - b. The Internet economy is increasingly an information economy. Forms of information that can be put into digital form and transmitted digitally over any data network including the Internet include texts, software, music, images, animation, and movies. Much of that information is protected by copyright, and has specific conditions attached to its reproduction, transmission, and distribution. National policy with respect to such material should definitively respect the rights of the copyright holder, while still allowing for some type of occasional use without permission for certain purposes. The latter type of use is sometimes referred to as "fair use." Given the ease with which digital materials can be copied and transmitted, this balance is a difficult one to obtain because of the difficulty of enforcement, and in fact such intellectual property issues are among the most important unsolved issues in the digital economy today. Nevertheless, the issue demands recognition and needs to be addressed.
  - c. The legality or illegality of specific content depends very much on national, cultural and religious views. Some content, such as child pornography, is illegal in almost all countries, while other content that may be viewed as offensive, may or may not be legislated as illegal. Indeed, some content may be legal if distributed in certain ways, and the same content may be considered illegal if distributed in other ways. With regard to content filtering, it should be noted that the Internet tends to work around such barriers, and that such content control is only possible at the enforcement stage rather than at the distribution stage. Therefore, if national policy bans specific content, it would be wise to consider the issue of enforcing laws based upon this policy and the secondary effects of the enforcement procedures that are adopted.

### *III. E-Commerce Regulatory Framework – International Legislative Practice*

At some time in the future, Iraq will be in the position of writing new laws that specifically address issues regarding the Internet and e-Commerce. At that time, it will be useful to use the framework suggested above, as well as to examine approaches taken by other countries in defining their laws with respect to cyberspace. This section raises some of the issues mentioned in section I of this paper in more detail, and provides pointers to resources that will help Iraq when it approaches being ready to take this step.

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 section 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 (wire line, 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](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](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](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 they 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 Nations 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. (Article 7.)
- **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 exceptions 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](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 identity 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 manage 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](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](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](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](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.<sup>2</sup> 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/cpspubl.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.
  - 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").

---

<sup>2</sup> 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, HCOFIL, ICC, Report of the Conference, the Hague, 11-12 December 2000.*



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](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](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, HCOPII, 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.<sup>3</sup> 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:
  - does not have actual knowledge that the activity is illegal;
  - is not aware of facts or circumstances from which illegal activity is apparent; and
  - 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.

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:**

---

<sup>3</sup> 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.

- 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>.