Creating the Legal Framework for ICT Development: The Example of E-Signature Legislation in Emerging Market Economies

James X. Dempsey*

INTRODUCTION

Many developing and transitional countries are eager to participate in the global information-based economy. These countries recognize that law and government policy can play an important role in either hindering or fostering the development of information and communications technologies (ICT), the growth of the online economy, and the realization of e-government.

Conducting business and offering e-government services in the global digital environment present important questions of the legal validity of electronic documents and complex issues of trust and authentication. Governments and policy experts have grappled with ways to provide certainty and trust to businesses and citizens engaging in transactions online. One solution that has received considerable attention is the adoption of "electronic signature" or "digital signature" laws.[1] In many countries, policymakers seeking to promote e-commerce and e-government have given priority to enactment of laws intended to create a legal basis for the use and acceptance of electronic or digital signatures. Over the last five to seven years, approximately 50 countries have adopted laws or executive decrees on electronic or digital signatures, and others have them under consideration.[2] A number of these laws anticipate complicated systems of "public key infrastructures" and "certificate authorities" that are expected to manage the technology for creating cryptographically-based digital signatures. Some involve government licensing. Some provide that only signatures made with government-approved

---

* Executive Director, Center for Democracy and Technology, Washington, DC, http://www.cdt.org, and Policy Director, Global Internet Policy Initiative, http://www.internetpolicy,net.

[1] Following a widely accepted convention, this article uses the term "electronic signature" to mean any authentication made by electronic means. Under this definition, electronic signatures include digitized versions of handwritten signatures, biometric techniques, and the "From" line on an email. The term "digital signature" refers to a specific kind of electronic signature involving the use of asymmetric encryption, in which a user publishes a public cryptographic key and "signs" data messages with a private key, such that application of the public key will confirm that the data message was "signed" with the private key that is the unique pair of that public key.

[2] The e-commerce laws of many countries are compiled at http://rechten.kub.nl/simone/ds-lawsu.htm and at http://www.mbc.com/ecommerce/legislative.asp.

technology will be recognized as binding. The adoption of these laws has been accompanied by reports, journal articles and news stores predicting that e-signature legislation will revolutionize business practices and promote e-commerce.

One purpose of this article is to argue that the role of e-signature laws in practice is much less than the hype suggested.[3] This is not to say that trust and authentication are not important online. They are. Digital signature technology and other online authentication systems deserve the attention of developing as well as develop countries. My point is that the legal system can offer only limited certainty and cannot generate trust. The value of digital signatures and other authentication systems flows less from the legal rules than from the technology itself, the choices made by those who use the technology, and the way it is integrated by businesses into commerce as it is actually practiced online.

A second theme of this article is that the focus on electronic signatures in discussions of e-commerce and ICT development may have created misconceptions as to the priorities of legal reform necessary to support the Internet and e-commerce. This article argues that, at the least, an early focus on electronic signature laws can be a distraction from more important issues. Worse yet, a highly regulatory approach to electronic signatures can hinder the development of e-commerce.

The third purpose of this article is to outline an incremental approach for emerging economies to address the issues surrounding electronic documents and e-signatures. This approach emphasizes, first, ensuring that there is no legal bar to the acceptance of electronic documents and, second, allowing businesses to agree among themselves on their own technical standards for entering into contracts electronically. Thirdly, for e-government applications, governments may experiment with authentication systems (including possibly digital signatures). But governments should hesitate before setting up regulatory systems intended to approve technologies or service providers for e-commerce.

Finally, a consideration of the limitations of electronic signature legislation yields some broader lessons for those interested in legal reforms to support growth of the Internet as a component of development. First, it highlights the importance of basing legal reform efforts on a sensitive analysis of local needs and actual business practices, for it seems that electronic signature laws have sometimes been proposed without a realistic prior assessment of the legal and other barriers to development and use of ICT. Secondly, the experience with digital signature legislation reconfirms that legal reform efforts intended to foster ICT development should continue to give priority to the basics

---

[3] Others have begun to sound this theme. John Humphrey, et al., The Reality of E-Commerce with Developing Countries, Institute of Development Studies at the University of Sussex and Interdepartmental Programme in Media and Communication of the London School of Economics and Political Science (March 2003), http://www.gapresearch.org/production/Report.pdf; Jane K. Winn, The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce, 37 Idaho L. Rev. 353 (2001).

of telecommunications liberalization, removal of licensing burdens, support for entrepreneurship, transparency, banking and currency law, and the improvement of basic transportation infrastructures. If those issues are not resolved, e-commerce will not flourish no matter what law is adopted on e-signatures. Finally, the experience with electronic signature legislation in more developed as well as less developed and transitional countries shows that the law cannot produce what is beyond the state of the technology or the marketplace.

The Need for Certainty and Trust in E-Commerce and E-Government

It is understandable that questions have arisen about the legal acceptability of electronic documents and electronic signatures, for the laws of many countries, when referring to contracts or to information that must be submitted to the government, use words such as "writing" or "original" or "signed" – words that were intended for the age of paper. Businesses and individuals may be hesitant to use electronic means of communications to enter business transaction or to make filings with government agencies if they are not assured that electronic messages have binding legal effect. In order to facilitate e-commerce and e-government, it may be necessary to make it clear that the words "writing, "original" and "signature," when used in legislation or other normative acts regarding the making of contracts or compliance with the filing requirements of government agencies, do not exclude the use of electronic messages.[4]

However, there has been a disconnect between this need for certainty and the legislative solutions that have been proposed in many countries, in both the more developed and the less developed world. The problem begins with a failure to distinguish certainty from trust and to distinguish the legal aspects of trust from its non-legal aspects. At the simplest level, the question of certainty concerns whether an electronic message will satisfy the legal requirement that a document be "in writing?" Related questions include: What is the "original" of an electronic document, for example, for purposes of evidentiary laws requiring someone to present an "original" version of a document as evidence in court? These are purely legal questions.

A more difficult set of questions concerns what kind of electronic function can satisfy the legal requirement for a "signature." Here, the question of legal certainty has been blurred with the question of trust in the global marketplace. Addressing electronic signatures requires a full understanding of the various functions that have been served by the ink signature on paper.[5] The desire to promote e-commerce may also justify a re-examination of the role that signatures play on contracts and legal documents in general. The outcome of these inquiries may vary between countries operating under a common

---

[4] See *An Analysis of International Electronic Signature Implementation Initiatives,* A Study Prepared for the Internet Law and Policy Forum, September 2000 by Chris Kuner and Stewart Baker, published at http://www.ilpf.org/groups/analysis_IEDSII.htm.

[5] See Jane K. Winn, The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce, 37 Idaho L. Rev. 353 (2001).

law tradition and civil law countries. Nevertheless, in most legal systems the core legal function of a "signature" is to indicate an intent to be bound by that which is signed. Secondarily, signatures can be valuable in aiding the resolution of disputes if the contract is called into question. Thus, to the extent that signatures are unique and recognizable, they may serve to identify or authenticate the signer. The appearance of a unique signature on a piece of paper may make it difficult for the signer to repudiate the document.

However, in the policy discussions surrounding electronic signature laws, the question of legal certainty and the questions of trust have been conflated. To adopt legal reforms suited to actual practice, it is important to distinguish between the question of whether it is certain that an electronic document will be legally valid and enforceable and the separate questions of trust and authentication. Online communications can present especially acute questions of trust and authentication, but it is important to recognize that by and large these are not legal questions that can be solved by legislation. For example, how does the recipient of an electronic communication know with assurance that the person sending it is the person he claims to be? This is the question of "identity" or "authentication." Another issue is how can a recipient of a message, who has relied on it, avoid the apparent sender denying that he sent it? This is the question of "non-repudiation." Also, how does one ensure that a message will be read only by the intended recipient and not by someone who might intercept it? This is the problem of "confidentiality." Finally, how can it be proven that a message has not been altered or otherwise tampered with in transmission or storage? This is the problem of "integrity."

These questions are not unique to electronic transactions, although sometimes it is suggested that they are. However, confusion has arisen about this third set of issues in the e-commerce realm, in part because the modern cryptographic technology that can be used to create "digital signatures" can also be used to improve online trust in the face of these four concerns – identity or authentication, non-repudiation, confidentiality, and integrity. In fact, digital encryption technologies, properly applied, can provide a much greater degree of trust than pen-and-ink signatures on paper. (In practice, though, using encryption to solve these problems is not easy.) But the components of trust -- identity, non-repudiation, confidentiality and the integrity of communications -- are mainly not legal questions. For example, encryption is widely used for creating secure connections between a web server and a web client, such as a personal computer. This security protects the confidentiality of information (such as a credit card number) between the customer's computer and the business's computer. It involves the same technology that can be used for digital signatures, but the confidentiality of the data in transit has nothing to do with the legal validity of the transaction. Confidentiality simply is not a legal requirement for a contract. Similarly, it is not necessary from a legal standpoint that a person prove his identity to enter into a binding contract (although it may be very important from a practical standpoint). Non-repudiation also is not a legal element of a contract.[6] And while the integrity of a document may be called into question, integrity is largely a factual question and one that affects paper documents as well. This distinction -- between the functions of an electronic signature that are legally required to make a

[6] Id.

contract and those that build confidence independent of the legal framework – has too often been overlooked in discussions of e-commerce. Also overlooked has been the distinction between issues of confidence that can be solved by the adoption of a legal framework and the issues of trust that can be resolved by technology independent of the legal framework.

THE LEGAL CONTEXT FOR E-COMMERCE AND ICT DEVELOPMENT

Something else has also been overlooked in many discussions of e-commerce: that electronic signature legislation is not the most important policy reform needed to support e-commerce and ICT development.[7] The best electronic signature law in the world will not make e-commerce flourish, if other legal reforms have not been instituted. Conversely, e-commerce can flourish without an e-signature law, if other legal reforms are adopted. Indeed, it is probably no exaggeration to say that e-signature laws have proven to be largely irrelevant to the development of e-commerce.[8] In the most developed countries with the most robust e-commerce, e-commerce took off before e-signature laws were adopted.[9] E-signature laws have even proven largely irrelevant to the implementation of e-signatures, since most of the implementations of e-signatures that exist in the real world have been in closed systems where the laws are not applicable.

---

[7] A more realistic approach emerges, for example, in the E-commerce and Development Report 2001 of UNCTAD, which notes that restrictive regulations such as exchange controls, protection of telecommunication monopolies, restrictive trade practices, limits on encryption and prohibitions on Internet telephony are more of concern to enterprises in less developed countries than whether or not e-commerce laws are in place. P. 195.

[8] In the United States, for example, where contracts are largely governed by state law, the State of Utah was the first state to adopt an e-signature law. The Utah law gives legal force to signatures based upon an asymmetric cryptosystem utilizing private and public key pairs. The legislation, known as the Utah Digital Signature Act, was signed by the governor of Utah in March 1995 and was amended during the1996 Utah legislative session. There is no evidence that corporations or individuals in Utah adopted e-commerce sooner or at a higher rate than those in other states.

[9] For example, on the federal level, the U.S. adopted an e-signature law in 2000, but by then there were already $29 billion a year in retail e-commerce sales (a tiny fraction of overall retail sales in the US, but still significant evidence that consumers and merchants were going online without the need of an e-signature law). Amazon.com, the online bookseller, was founded in 1995, went public in 1997, and compiled $1.8 billion in sales in the first 9 months of 2000 before the US E-Sign Act took effect. For a perspective on the situation in the UK, see Ian Lynch, E-signature law labelled as 'red herring,' (July 25, 2000) http://www.vnunet.com/News/1107369.

Compared to electronic signature legislation, there are other reforms that are far more important in creating the legal and regulatory environment for e-commerce.[10] First and foremost among these is probably telecommunications reform. To conduct e-commerce requires access to the Internet, which, for most users in most contexts, requires access to telecommunications. It has been shown that the policies of "liberalization" (i.e., the introduction of competition, the privatization of state-owned telecommunications operators and the establishment of independent regulators capable of effectively managing spectrum and enforcing competition) will best foster investment, innovation and infrastructure development, leading to increased access at lower prices, and thus contributing to the growth of ICT.[11]

It is important to stress that liberalization does not mean non-regulation. Telecom liberalization requires the establishment of an independent regulator that can enforce competition.[12] Furthermore, liberalization is important but not sufficient to foster widespread diffusion of IT systems and the development of e-commerce. Studies on national systems of innovation and diffusion have shown that innovation and diffusion need more than a free market system; governments and other institutions play a significant role.

Also important is the elimination of unnecessary legal barriers to business start-up. Entrepreneurs online and offline should be able to form a business and begin operations without high barriers of licensing requirements. Government regulators are

---

[10] The choice between e-signature legislation and other legal reforms is not a trade-off or a zero-sum situation -- except in the sense that governments have to prioritize their legal reforms. Countries can certainly adopt e-signature laws and at the same time adopt the many other reforms necessary for ICT development. My point is that governments should not put e-signature laws ahead of other, more fundamental reforms and should not assume that they can consider the process of reforming the legal framework for ICT to be finished when they have adopted an e-signature law.

[11] OECD, Understanding the Digital Divide (2000), p. 9 ("Liberalisation of telecommunications services has been crucial to the growth of access lines (fixed and mobile), alternative access technologies, price reductions, Internet access and use."); Creating a Development Dynamic: Final Report of the Digital Opportunity Initiative (July 2001), p. 35; Scott Wallsten, Regulation and Internet Use in Developing Countries, AEI-Brookings Joint Center For Regulatory Studies, Related Publication 03-8 (May 2003).

[12] "Liberalization" or "deregulation" of telecoms refers to privatization and competition, it does not mean the elimination of regulation. To the contrary, telecom deregulation involves the enforcement of the rules of competition. Under "deregulation," telecoms are regulated, not as part of government, but as private entities. Deregulation means a shift in the focus of regulation. With privatization and its counterpart, competition, price regulation is less necessary, and even undesirable, but interconnection and non-discriminatory practices must be enforced.

poor judges of what will succeed or not in the marketplace. Regulation is valuable in protecting consumers but too often regulatory requirements left over from command and control economies do not protect consumers or investors but increase the cost of starting a new business. The streamlining of regulatory burdens is especially important to e-commerce, where speed, innovation and flexibility are often key determinants of market success.

Banking laws are also crucial. People who do not have credit cards or access to some other form of non-cash transfer of money cannot engage in e-commerce. Rules that limit liability of cardholders or account holders in the case of fraud contribute to trust online as well as off. In many developing countries, credit card fraud needs to be addressed by effective law enforcement. Merchant credit accounts are not available to entrepreneurs in many developing nations in large part because so much credit card fraud is committed by users in those countries.

In terms of trust, another key concern is redress. There must be an efficient means of enforcing contracts of any kind. In most legal systems, this depends on the judiciary, which must be independent and free from corruption and which must function without delay. Even a traditional handwritten signature on a paper contract is unreliable if the contract can be breached knowing that an effort to enforce it will be delayed in court for years. Similarly, the basic elements of consumer protection come not from the law of signatures, but from the procedures for redress. The same principles of consumer protection that are needed offline are also relevant online. For example, consumers will not buy something online unless they are confident that they can get their money back if it is not delivered.

Finally, a general observation: E-commerce may be more effectively fostered by the elimination of formalistic legal requirements, rather than their translation to the digital context. (The same is true of e-government.) Yet some e-signature legislative proposals in developing and transitional countries would establish rules for online transactions that are even stricter than those associated with offline transactions. Countries making the transition to a market economy should use the advent of e-commerce to generally re-examine the formalistic legal requirements that apply to commerce offline as well as online. Many of the more developed countries where e-commerce has flourished had already, before the Internet, eliminated some of the formalistic requirements for contracts and other legal interactions. (For example, in the US, for over a century, the legal requirement of a "signature" on a contract has not required a handwritten signature.[13]) Developing and transitional countries seeking to take advantage of the information economy might re-examine long-standing rules to see if they can be eliminated or simplified in the offline context as well, rather than merely trying to find for them an online equivalent. This is consistent with the principle of transaction neutrality: as much as possible, paper transactions and electronic ones should be treated the same.

---

[13] The same is true in the UK. Nicholas Bohm, Do we need new digital signature law? http://www.fipr.org/publications/newsig.html

Within this context, one can better approach the question of the need for and the content of e-signature legislation. E-signature legislation may have a special role in developing or transitional countries, where the judicial system cannot cope with new questions and where other forms of legal protection for means of conducting online transactions, such as credit card laws, are lacking. However, the process of adopting e-signature legislation should proceed only after there has been a complete assessment of current law – identifying what questions it answers and fails to answer -- and a clear understanding of what functions the e-signature is supposed to perform. And rather than setting up a complex system for acceptance of cryptographically-based digital signatures, developing and transitional countries might be better served by an incremental approach, outlined below.

THE VALUE AND LIMITS OF THE INTERNATIONAL MODELS

As suggested above, the legal and technical questions posed by e-commerce and e-government arise at several levels. The simple question of whether an electronic message can be denied legal effect as a "writing" can be simply answered. The separate question of what electronic techniques will be accepted as the legal equivalent of a pen and ink signature poses more difficult questions that turn to some extent on the requirements of the particular legal system (most notably, the difference between common law and civil law systems). The most difficult question in e-commerce or e-government from both a legal and a technical standpoint is how one proves identity online.

In an effort to answer some of these questions, including the most difficult question of how strangers can confidently establish identity online, international legal experts and institutions have developed model laws. One of these is the Model Law on Electronic Commerce developed in 1996 by the United Nations Commission on International Trade Law (UNCITRAL). It recommends legislative language to make it clear that a document cannot be denied legal effect as a "writing" or as an "original" solely because it is in electronic form. It also lays out the stages of making a contract electronically, addressing concepts such as offer and acceptance in the electronic context. UNCITRAL has also issued a separate model law addressing the more difficult question of what electronic function can satisfy the legal requirement of a signature: the UNCITRAL Model Law on Electronic Signatures of 2001 (the "UNCITRAL E-Signature Model"). In the same vein, in 1999, the European Union adopted a directive setting out a "community framework" for electronic signatures (the "EU E-Signature Directive").[14]

---

[14] UNCITRAL Model Law on Electronic Commerce (1996), Dec. 16, 1996, http://www.uncitral.org/en-index.htm; UNCITRAL Model Law on Electronic Signatures (2001), July 5, 2001, http://www.uncitral.org/en-index.htm; Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://europa.eu.int/ISPO/ecommerce/legal/digital.html.

These models are based on several principles of equal relevance both to more developed countries and to less developed and transitional economies. First, they reflect the premise that e-commerce will flourish best if the private sector is allowed to develop solutions driven by competition and market choice. Accordingly, the international models disfavor any government intervention that would limit the development of a market in electronic signature services. In particular, the models disfavor a system under which entities providing e-signature services for e-commerce must first obtain a government license. The EU directive specifically prohibits Member States from imposing a licensing requirement. Second, the models emphasize the principle of "technology neutrality" – that national e-signature laws should not exclusively recognize any specific technology for creating electronic signatures.[15]

However, for a variety of reasons, it is increasingly clear that the message of these international models has been misinterpreted by developing and transitional countries. Many developing and transitional countries have adopted or proposed e-signature laws that are too regulatory, denying potential companies the flexibility that e-commerce requires.[16] In part, this may be because the international models have been influenced by an unjustifiable marketing hype surrounding e-signatures. Also, it may be because their technology neutrality does not afford adequate certainty in developing and transitional countries, so those countries move toward a more regulatory system. The international models leave many questions to be resolved either by the judiciary or by regulatory agencies or self-regulatory industry bodies that will set standards. Yet many developing and transitional countries do not have a judiciary practically and legally able to interpret a

---

[15] For example, the EU Directive defines "electronic signature" without reference to a particular technology. It includes an express non-discrimination clause (Article 5, para 2) and general language emphasizing the importance of an open approach given "rapid technological development and the global character of the Internet."

[16] For example, the Russian Electronic Digital Signature Law that took effect in January 2002 establishes encryption as the only method whereby a valid electronic digital signature may be created under Russian law. The Law is drafted to intentionally omit other analogues of personal signatures and exclude the use of other technologies for electronic digital signature creation. Baker & MacKenzie, Legal Alert - Electronic Digital Signature Law, January 14, 2002, http://www.bmck.com/ecommerce/Russia-E-Signature-Alert.doc. The Argentine law provides for the creation of a Federal Digital Signature Infrastructure consisting of an Application Authority, which shall be the Chief of Cabinet and shall dictate regulations and implementing rules under the law: a Public Key Infrastructure Advisory Commission, located at the Chief of Cabinet, which must issue recommendations concerning technical aspects of the Digital Signature Infrastructure; a Digital Signature Administrator Institution, responsible for licensing the certification authorities and supervising their activities; Licensed Certification Authorities, which issue certificates and render other services related to digital signatures; and Registration Authorities, entities responsible for validating the identity and any other information concerning certificate holders, under delegation from the licensed certification authorities. See http://www.pki.gov.ar/English/index.html.

general law on a case-by-case basis, and do not yet have competent self-regulatory or regulatory institutions. Perhaps, part of the problem has also been inadequate guidance from donor organizations or international consultants. And there is also a tendency worldwide of policymakers to reach for the tool at hand: there is a model law on e-signatures but not on telecomm liberalization or consumer protection or credit cards, so policymakers start with e-signatures.

But perhaps the most significant reason why the UNCITRAL e-signature model law and the EU directive can be misleading for developing and transitional countries is this: while they allow for the use of any kind of e-signature technology, they give considerable attention to technology that can address the most difficult question in e-commerce – the entry into a contract between parties who are strangers to each other. They specify procedures for the most reliable form of e-signature, involving the establishment of certification service providers who vouch for the signature creation data of a person or entity, such that the signature creation data can be linked exclusively to one person and no other. However, the problem of electronic transactions between strangers is not one that can be solved by legislative fiat; the hurdles are largely technological and economic. More importantly, experience is now showing that most e-commerce is not between strangers who meet online for the first time, but rather is between trading partners who have first developed a relationship through traditional, face-to-face means.[17] Thus, a great deal of e-commerce can be supported without ever addressing the problem of stranger-to-stranger transactions. For developing and emerging economies, it is the wrong place to start in building the legal framework for e-commerce and ICT development.

A REALISTIC APPROACH TO E-COMMERCE

A more realistic approach to e-signatures would draw from the UNCITRAL and EU models, but with a different emphasis. First and foremost, a realistic legal framework would place its primary emphasis on the principle of "party autonomy," also referred to as "business choice" or "freedom of contract." This is the principle that laws on electronic signatures should permit businesses and individuals engaged in e-commerce to agree by traditional means on their own methods of entering into electronic contracts. Thus, for example, if a business sets up an online procurement system for its suppliers and provides to suppliers it deems qualified some form of authenticator – whether a simple identification number or cryptographic technology -- the law and the courts should enforce agreements made within that system, whether or not the technology meets specific technical standards.

Secondly, while the goal of e-commerce is best achieved through a competitive market, and government licensing for e-commerce applications should be avoided as a barrier to innovation, e-government should probably be treated separately. It is entirely

[17] "Our overall finding is that the main effect of B2B e-commerce is to enhance the relationships between existing trading partners." John Humphrey, et al., The Reality of E-Commerce with Developing Countries, supra, p. i.

appropriate and probably necessary for the government to set standards for identification technology to be used in interactions with the government. It is even appropriate for the government to set up its own e-signature system, and to issue the necessary technology (or contract with a private sector vendor to set it up.) But this too will normally involve face-to-face interaction, or traditional means of communication, to set the basis for subsequent online transaction, eliminating the need for the elaborate arrangements of a public key infrastructure.

These two elements alone – business choice for e-commerce and government requirements for e-government – should be sufficient to cover a large portion of the situations where electronic signatures might be valuable in developing and transitional countries. A third category of situations –transactions between strangers – are probably better addressed through the adoption of laws regulating credit cards, debit cards and pre-payment or "cybercash" schemes, where crucial verification functions are handled in large part between the merchant and the entity issuing the credit or debit card or providing the cybercash services, not between the merchant and the consumer.

The First Step – Recognition of Electronic Documents as "Writings" and Other Rules of Electronic Message Exchange

In many countries, the law requires that contracts or other documents must be in "writing" and/or "signed." Other laws require that a "record" be retained. Rules of evidence or other legal requirements may refer to the "original" of a document. Questions have been raised about whether electronic documents satisfy these requirements. To some extent, these concerns are overstated, since most legal systems have already dealt with telegrams, telexes, and faxes. But to remove these concerns, it is generally sensible for a nation to adopt a law providing, at the least, that "a signature, contract or other record may not be denied legal effect, validity or enforceability solely because it is in electronic form."[18] The UNCITRAL E-Commerce Model spells this out in detail in Articles 5 through 10. Such a law does not say that an electronic document is always binding or that an electronic signature is always valid – it merely says that the document or signature cannot be denied effect solely on the ground that it is electronic. The UNCITRAL E-Commerce Model also includes useful language on receipt and acknowledgement and other rules for the formation of contracts through the exchange of

[18] This is essentially the language of the US law, the Electronic Signatures in Global and National Commerce Act, section 101(a). Similar language appears in the EU E-Signature Directive, Article 5.2 of which states, "Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is … in electronic form." The EU Directive on E-commerce states, "Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

electronic messages. Any country would be well-advised to adopt these rules.[19] They entail no regulatory burden on e-commerce participants.

Second Step -- Endorsement of Business Choice in Transactions Based on Prior Agreement Entered into by Traditional Means

A harder question is what technology in an exchange of electronic messages should be accorded the presumption of reliability traditionally associated with an ink signature handwritten on a paper document. But in a large percentage of transactions, this question can be answered by giving legal recognition to the identification and reliability choices that the parties themselves have made. This is the principle of "business choice," "party autonomy," or "freedom of contract." It is much more important in practice than one would gather from studying the international e-signature models.

It turns out that in the business-to-business (B2B) context, the problem of creating trust between strangers in a purely online environment rarely arises, for most B2B commerce does not occur between strangers.[20] Most B2B commerce, even in the age of the Internet, relies on face-to-face interactions or other traditional means of credit and background checks ("due diligence") to verify identity and competency.[21] Only after identity and trust have been established by traditional means does online commerce take place. That online commerce may or may not entail cryptography-based e-signatures. If it does, however, it uses e-signature technology required by one of the parties, not by law.

An example of this might be an online procurement system that a business sets up for its suppliers.[22] Through traditional means, the business will inquire into the stability

---

[19] See the recommendations of the UK-based Foundation for Information Policy Research (FIPR), http://www.fipr.org/publications/sigdirecon.html.

[20] The Guide to Enactment of the UNCITRAL E-Signature Model recognizes this, stating in para. 111 that, "in practice, solutions to the legal difficulties raised by the use of modern means of communication are sought mostly within contracts."

[21] Humphrey and his colleagues found that in-person inquiries precede e-commerce. For example, in agriculture supply chains, large retailers do not source products without conducting extensive audits of the suppliers' premises. John Humphrey, et al., The Reality of E-Commerce with Developing Countries, supra, at p. 27. Once a relationship has been established by traditional means, companies rely heavily on the Internet, because it allows them to lower telecommunications costs. Ninety-five percent of firms in the garments sector surveyed were using e-mail to place or accept orders with existing international trading partners. Id. at p. 21. Many respondents to the survey indicated that Web-based relationships cannot substitute for face-to-face encounters. Id at p. 29.

[22] "Some types of Internet-based B2B e-commerce are developing, but these appear to be the private, exclusive models, where access is restricted to firms that are already

and professionalism of prospective suppliers. Once it is satisfied with the competency and reliability of a particular company, it will enter into an agreement with the supplier by traditional means (for example, a mailed or faxed contract with a handwritten signature). Among other things, the parties will agree on means to be used to identify those suppliers who are authorized to use the online system. The entity running the procurement system will provide qualified suppliers some form of authenticator – whether a simple password and identification number or cryptographic technology. In this situation, there is no need for government regulation of the making of online agreements – the private system can be set up in any way its owner chooses and agreements with suppliers granted access to the system should be fully enforceable.

Recognizing that this is how most B2B e-commerce is conducted, an e-commerce or e-signature law should make it clear that contracts subsequently made between parties to this kind of relationship are legally binding even though in electronic form, and a "signature" of whatever kind the parties have agreed to (including merely a typewritten name or the entry of a personal identification number) should be accepted as a valid "signature."

The business choice principle is not limited to B2B transactions. Some business to consumer (B2C) transactions are based on the same model. Take online banking, for example. Generally, online banking is available to customers who have established an account offline. The bank and the customer will already have confirmed each other's identity to the extent necessary through traditional means, and will have entered into an agreement with a handwritten signature in person at a bank office or with an exchange of paper documents in the mail. Even so-called "virtual banks," which have no bricks-and-mortar offices, will not establish an online account until a paper-based agreement is submitted by mail or fax to the system for online banking.[23] Thereafter, all online transactions between the bank and the customer using the system the bank has created and the customer has accepted should be recognized as legally binding.

Both the UNCITRAL E-Signature Model and the EU Directive incorporate the principle of business choice – but it is indirectly stated or buried. Article 5 of the UNCITRAL Model states that "The provisions of this law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law." The preamble to the EU Directive states that "a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; … the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognized." (Paragraph

---

integrated within their sector supply chains." John Humphrey, et al., The Reality of E-Commerce with Developing Countries, supra, p. 31.

[23] For example, one of the leading virtual banks in the US, the First Internet Bank, which has no offices or branches where customers can engage in face-to-face transactions, requires customers to submit a paper application by mail or fax. http://www.firstib.com/apply/personal.html

16.) Unfortunately, neither model offers recommended legislative language for actually giving legal effect to the choices that parties make for their online transactions.

It is important that the business choice principle apply to Internet-based systems. Some legislative proposals that have been put forth in developing or transitional countries have recognized the business choice principle only within a "private" system or a "corporate information system" or systems that do not interface with public networks. This is too narrow. The nature of the communications network is not the most relevant defining factor, since many "private" or "corporate" systems interface with or even operate entirely over the public network. The relevant consideration is whether the system for making transactions is limited to people bound to the rules of the system by a contractual agreement entered into by traditional means.

Third Step -- Government Authentication Standards for E-Government

There is one exception to the principle that the government should not regulate technologies used in online authentication, and that exception is in the area of e-government. For countries that normally require a high degree of proof of identity for those transacting business with the government, it is acceptable and probably desirable for the government to establish authentication standards for those wishing to submit documents electronically to the government. There is no reason, however, why these standards would have to meet the technical standards of the EU digital signature directive. The government itself can decide what level of authentication is appropriate for citizen-government interactions. As with e-commerce applications, the simplest approaches would use traditional face-to-face means to initially establish identity or to distribute electronic authenticators.[24]

There are several ways the government may do this: The government may establish its own system for online authentication in which it issues the authenticator (which may be no more than a password). Or the government may issue a contract to a private entity to do the same. Most desirable would be for the government to issue standards and approve any and all private sector service providers who meet those standards. This might encourage private enterprise to develop services that would also be available for commercial applications. And if the technology is to be used in private commerce, it might be more acceptable if the government were not controlling components of the system.

A good legislative model for this e-government application is found in the legislation adopted by the state of Illinois in the United States. The central language is this:

---

[24] For example, Denmark is planning to introduce a "public certificate for electronic services" with the government, but it will not live up to the requirements of the EU directive. In the judgment of the Danish government, however, it will provide sufficient security in most e-government transaction. eGovernment: The Danish Experience, by Poul Bernt Jensen, Senior Advisor, Ministry of Science, Technology and Innovation, Denmark, http://www.oio.dk/index.php?o=705d5300e9beb7aa5bdc69ffa88e190a

> "Whenever any rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any State agency, a filing made by an electronic record shall have the same force and effect as a filing made on paper in all cases where the State agency has authorized or agreed to such electronic filing and the filing is made in accordance with applicable rules or agreement.
>
> * * *
>
> "Each State agency shall have the authority to issue, or contract for the issuance of, certificates to (i) its employees and agents and (ii) persons conducting business or other transactions with such State agency and to take other actions consistent therewith, including the establishment of repositories and the suspension or revocation of certificates so issued, provided that the foregoing is conducted in accordance with all the rules, procedures, and policies specified by the Department of Central Management Services. The Department of Central Management Services shall have the authority to specify the rules, procedures, and policies whereby State agencies may issue or contract for the issuance of certificates."

It is probably a good idea to reject the assumption that there should be a single system for both e-commerce and e-government applications. There are many benefits to creating a government authentication system that is separate from the e-commerce authentication system. Privacy and security may be improved if individuals and organizations have several forms of online authentication, each of which authenticates the user in a different transaction space. This is analogous to having a keychain with multiple keys for different locks, or a wallet with multiple credit cards, a driver's license, and a passport, for example, each of which is tied to the same person but has validity in a specific environment.

Transactions with Strangers

An extension of the business choice principle – again combining traditional methods with online transactions -- serves to facilitate a wide range of e-commerce transactions between strangers. Sales of books from Amazon.com may be a familiar example. In this context, the e-commerce merchant may require from the customer no more than a name, address and credit card number to identify or "authenticate" the customer. The trust that allows this to happen is provided by a set of contractual relations entered into by traditional means and the law on credit cards, which define the responsibilities, liabilities and protections for all the parties. While the merchant and the customer are strangers to each other, both the consumer and the merchant have well-defined contractual relationships with the bank that issued the credit card to the consumer – contractual relationships most likely entered into by traditional means with a traditional signatures on paper contracts. Before accepting the transaction, the on-line merchant checks with the bank to ensure that the card is not stolen, and other anti-fraud inquiries

may be conducted (asking for a billing address (to ensure that it matches the address on record) or a code number on the back of the card (to ensure that the user physically has the card)). These measure give the merchant some assurance that the bank will pay for the transaction. Similarly, the bank that issued the credit card has a contractual relationship with the customer, also entered into by traditional means, giving the credit card issuer rights against the customer, including the right to collect on the credit card holder's bill. And the customer knows that if the merchant does not deliver the requested product or service, the customer will get his money back from the bank and the bank will have rights to get its money back from the merchant.

The point is this: the trust in the relationship does not come from an electronic "signature" – it comes from a web of other legal rules (rules applicable to the offline world as well) that define the relationships among credit card issuers, credit card holders and merchants. (The same is true of a legal system for debit cards or e-payments.) Fraud is a problem in the system, and its major participants are looking for better means of authentication, but even in developing countries cryptographic authentication has not been instituted for most "stranger" transactions and yet e-commerce flourishes in some of them.

Of course, many developing and transitional countries do not yet have laws and regulatory schemes for credit cards, debit cards or other similar payment schemes. And even if the legal framework exists, the problem of fraud poses a significant barrier in some developing or transitional countries to the widespread acceptance of credit cards. Online B2C transactions may be out of the reach of these countries. However, adopting laws to allow the online use of credit cards or some form of e-payment – and creating a law enforcement system that will be effective in suppressing fraud so that financial institutions will take the risk of accepting credit card transactions from a developing country – are steps far more likely to be effective in satisfying e-commerce's needs for reliability and trust than adopting an e-signature law would be. E-signatures may be part of the system for creating trust in credit cards or e-payment systems, but in that case, the principle of business choice again can apply: it should be the credit card issuers or the providers of e-payment services who determine what type of authenticating technology to use, and the credit card issuers will enter into contracts with their customers and merchants through traditional means that set the rules for acceptance of e-signatures. The law should enforce the resulting transactions under the principle of business choice, subject to legal rules that allocate the risk of fraud among the credit card issuer (or e-payment services provider), the customer, and the merchant, and subject, as well, to consumer protections rules.[25]

---

[25] In the name of business choice, businesses should not be allowed to avoid compliance with consumer protection rules. As noted above, developing and transitional countries seeking to support development of consumer e-commerce will need to adopt consumer protection laws, including laws protecting consumers in credit transactions. The e-signature law that recognizes B2C choice should include language prohibiting avoidance of consumer protection rules.

Purely Electronic Relationships - The Tension Between Certainty and Technology Neutrality

The two principles outlined above – business choice and e-government standards – provide an adequate basis for a wide range of e-commerce and e-government. If a country chooses to go further and legislate standards for acceptance of e-signatures in the absence of business choice, it must carefully strike a balance between the goal of certainty and the principle of technology neutrality. The creation of rigid bureaucratic systems could actually stifle the development of the market.

On the one hand, the need for certainty pushes policymakers to set up a regulatory system that will endorse particular technologies, which usually means in practice the version of digital signatures based on what is known as Public Key Infrastructure or PKI.[26] As of now, PKI, while not widely *deployed*, is widely available, and offers the highest form of assurance of authentication, non-repudiation, integrity and confidentiality. However, the evolution of electronic and digital signature technologies continues. Recognizing this, the international models embrace the principle of "technology neutrality" and make it clear that no technology should be endorsed as the only means of creating valid signatures.

In emerging and transitional market economies, strict technology neutrality can be confusing. If the legal system fails to identify in advance particular technologies that will definitely be accepted, the issue is left to case-by-case determination by courts, and potential market participants will not have the certainty they desire before entering into an online transaction. To try to mediate this tension, both the UNCITRAL E-Signature Model and the EU Directive recognize that the regulatory or self-regulatory system could give a preference to PKI technology. The EU Directive takes a "two tier" approach. It defines an "advanced" electronic signature to be automatically recognized if it is "based on a qualified certificate" and created by a "secure-signature creation device" (Article 5, para 1). Although other technologies could fit the UNCITRAL and EU criteria, there is no doubt that they were drafted with PKI technologies in mind.

Therefore, it is not an inappropriate policy choice for an emerging market economy to develop a system (either legislative standards or regulatory determination) that gives a presumption of legal recognition to electronic signatures based on PKI technologies. However, even developing and transitional countries should avoid legislation that makes PKI the only means of creating electronic signatures. Legislative or regulatory endorsement of PKI and only PKI would constrain the acceptance of other technologies and thereby hinder the growth of e-commerce. Any legislation that seeks to establish a framework for electronic signatures in e-commerce outside the scope of business choice should explicitly recognize the potential for technological change. The UNCITRAL Model states in Article 6, paragraph 4 that the establishment of statutory

---

[26] A description of PKI can be found in the Enactment Guide accompanying the UNCITRAL E-Signature Model.

criteria for signature technology that will be deemed reliable does not limit the ability of any person to establish in any other way the reliability of an electronic signature.[27]

Developing and transitional countries have an understandable interest in creating public trust in the businesses that provide electronic signature services, such as certificates for PKI-based signatures. Government licensing schemes are one way to provide this trust, especially if industry standards and case-by-case judicial determinations are not viable alternatives. But licensing schemes are subject to delay and favoritism. Government licensing requirements can interfere with the development of a competitive marketplace if the regulatory requirements or bureaucratic delays create barriers to market entry.

The EU Directive, under the two-tier approach, gives a higher presumption of validity to a certificate issued by a provider *accredited* in accordance with the requirements of the Directive. This scheme is not, however, mandatory nor need it be governmental: An accreditation issued by a recognized industry-based group makes it easier to prove the contractual validity or admissibility of a document, but a party that has relied upon an unlicensed provider may nevertheless prove that a document meets the standards set in annexes to the Directive. This may be an acceptable model for a developing or transitional economy.

If emerging market economies choose to require government licensing of entities providing electronic signature services for e-commerce, the regulatory requirements should be transparent, limited to those requirements necessary to protect the public, and harmonized within the region with appropriate reference to international standards. Local and international businesses as well as international standards groups can provide guidance and should be active participants in setting up those requirements. The key principle is this: any licensing scheme should recognize the principle of business choice. If parties agree by traditional means that they will enter into electronic contracts without using a licensed service provider, the law should recognize and enforce those contracts.

However, even a signature based on technology from a licensed service provider is entitled only to a rebuttable presumption of validity. No matter where a country falls on the spectrum between legislated standards and government licensing, a party always can seek to prove that a digital signature was not properly created.

---

[27] Singapore has established a two-tiered system. Under Singapore law, digital signatures generated from the certificates issued by a licensed certificate authority will enjoy the benefits of evidentiary presumption. Without such a presumption, a party that intends to rely on a digital signature must produce enough evidence to convince the court that the signature was created under conditions that will render it trustworthy. With the presumption, the party relying on the signature merely has to show that the signature has been correctly verified, and the onus is on the other party disputing the signature to prove otherwise. There is a very clear explanation of the Singapore law at http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/3d122fbf7d5ac170c82568390001fb31?OpenDocument.

Licensing is distinct from direct government participation in the e-signature process. Both of the international models clearly disfavor a role for governments in issuing, registering, keeping, or verifying signature components. Yet some transitional countries have given a direct, functional role to the government. Article 10 of the Russian Federation law, for example, gives an executive agency the role of receiving and verifying a certificate before the user may rely on that certificate and maintaining a unified central registry of verified certificates. This is almost certain to be counterproductive. Bureaucratic process may be the source of unnecessary delays. Second, and perhaps more important, government access to signature information raises privacy and security concerns, which will discourage the use of electronic signatures. The negative effects of such an approach are mitigated only by the fact that people will not use it.

CONCLUSION

In this article, I have sought to place the issue of electronic signatures in its proper context, outlining the broader legal reforms that developing and transitional economies should give priority attention if they wish to foster ICT growth, and to describe a realistic and incremental framework for the basic elements of a law recognizing electronic documents and electronic signatures.

For a variety of reasons, sound and not so sound, governments have put a high priority on the adoption of electronic signatures laws. I argue here that this priority is misplaced. I have tried to place in context the very genuine issues of certainty, trust and authentication online that are sometimes cited in justifying the adoption of e-signature laws. I have argued that there are other legal and institutional reforms that are a much higher priority. I have also argued that, with specific reference to the acceptance of electronic documents and the recognition of electronic contracts, relatively modest legal reforms will achieve the goals of fostering e-commerce and e-government.

Efforts to promote e-commerce and e-government through reform of the laws regarding the legal recognition of documents and signatures should begin with an assessment of what must be changed and why.[28] Laws intended to facilitate e-commerce should not place more burdens on e-commerce than exist in the paper world. An assessment of the legal environment should ask what exactly are the legal impediments to e-commerce. The model that developing and transitional countries should have in mind should not be the contract between strangers. Instead, developing and transitional countries should ensure that they facilitate online contracting between established trading partners. There are important issues of trust in an e-commerce environment that cannot be solved by the law. In fact, a highly regulatory legal approach may stifle rather than

---

[28] "'Top-down' government policies promoting 'e-readiness' will be unsuccessful unless much greater effort is given to examining how Internet applications are actually being used … . Policy makers … should support 'bottom-up' approaches that are based on realistic assessments of B2B e-commerce opportunities and obstacles … ." Humphrey, et al., The Reality of E-Commerce with Developing Countries, supra, p. ii.

promote the development of e-commerce. E-commerce is best fostered by the removal of barriers, not the creation of new ones.

Based on the international models, it is possible to outline an electronic document law for developing and transitional countries. First, when the existing law requires a writing, an original, or a signature, it should be made clear that a document cannot be denied legal effect solely on the ground that it is in electronic form. Second, the soundest reform that could be made in a nation's law to promote e-commerce law would be to give full legal effect to contracts entered into electronically between any actors who have agreed by traditional means to transact business electronically, regardless of the nature of the technology they agree upon to authenticate themselves in the online context.

Global companies need e-signature systems that they can count on globally. Typically, the fastest way to achieve global uniformity is through a web of contracts, entered into by traditional means. If a developing country adopts a law that seems to cast doubt on whether it will enforce e-signatures used in accordance with such contracts, the country creates a reason for global users of e-signatures to avoid conducting e-commerce in that country. In other words, an e-signature law that does not provide for business choice could actually hurt participation in the global digital economy more than no law at all.

To support e-government, it might be desirable to require those doing online business with the government or engaging in other e-government transactions to obtain an authenticator issued by the government or issued by a government-approved service provider.

Beyond that, it is very difficult for a government to use the law to create what the technology and the marketplace cannot currently offer. A regulatory system might give a presumption of validity to certain existing and recognized technologies, such as PKI. But if the law does give a presumption of validity to certain technologies, it should also establish the principle of technology neutral, permitting courts to accept any technology meeting objective criteria. Government licensing of service providers should be avoided. Overall, policy should encourage the development of a competitive marketplace in which there are many services providers and many types of technology in use.

Development of electronic signature technologies and processes will continue. Developing and transitional countries may play a role in ongoing research, experimentation, and innovation. In the meantime, however, the realistic model of electronic signature acceptance outlined here can facilitate most e-commerce and e-government applications with no regulatory intervention.