INTERNATIONAL LAW AND TECHNOLOGY

The Emerging Disharmony of Electronic Commerce Legislation in Latin America

Robert M. Kossick*

The Internet presents one of Latin America's most important developmental opportunities. Even at this early point in its evolution, the unique communication efficiencies associated with the worldwide Web have facilitated the integration of Latin America into the global economy, made regional businesses more competitive, increased popular awareness of and participation in the formation of governmental policy, injected an element of accountability into public thinking, and contributed to the preservation of the environment. If, going forward, the nations of Latin America are to exploit these and other developmental opportunities fully, it is imperative that the region's governments adapt the formalistic writing, signature, and authentication standards and procedures contained in outdated codes to the reality of the digital age. While it was initially hoped that Latin governments would introduce new laws based upon the principles, objectives, and model provisions of the MLEC, it is increasingly apparent that the disparate legislative examples of other nations and regions (for example, the United States and the European Union) are having an even more profound impact on national initiatives to modernize writing, signature and authentication requirements and procedures. This tendency has been exacerbated, moreover, by the promulgation of provisions designed to safeguard the monopoly positions enjoyed by Latin authentication professionals. Almost four years after the MLEC's completion, Latin America has not harmonized the set of provisions originally envisioned but, rather, created a patchwork of substantially divergent—and, in some cases, functionally incompatible—laws. The author argues that the absence of a uniform legislative framework with respect to data messages and electronic signatures will undermine legal certainty in electronic contracts and consumer confidence in contemporary security and authentication methods. These outcomes, the author further argues, have the potential to increase the cost and complexity of electronically realized international transactions and could impede the growth of electronic commerce and development in Latin America. The author concludes by advocating that the introduction and adoption of either a regional or supra-national level convention containing harmonized provisions would ameliorate the negative effects produced by the emergence of inconsistent e-commerce regulations in Latin America.

* Robert M. Kossick, Jr., Esq., U.S.C.B., earned his L.L.M. in Inter-American Law at the University of Miami. The author is associated with Aballi, Milne, Kalil & Garrigo, P.A., a Miami firm specializing in international transactions and international commercial litigation. The author dedicates this work to his mother.

"The Internet has become the most powerful force for change with which mankind has had to reckon in a very long time."[1]

I. INTRODUCTION

A. Electronic Commerce in Latin America

1. The Potential

a. The Market Place

i. General Overview

The Internet[2] has changed the course of business, as well as many other things, forever. As one commentator accurately observes, "the

1. Moises Naim, *Six Nail Biters for the Millennium*, MIAMI HERALD, Mar. 19, 2000, at L1.

2. The Internet is best understood not as "a thing; it is an interconnection of many things." A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 130 (Brian Kahin & Charles Nesson eds., 1997). Using the TCP/IP communications standard, a set of rules permitting computers communicating with the Internet to communicate with each other, independently managed computers around the world can be inter-

Internet is not only growing at a dizzying speed and invading every nook of human activity, it is also drastically transforming everything it touches."[3] Using Internet tools such as the Word Wide Web and e-mail, business people can continuously engage in the production, advertising, sale, and distribution of products via telecommunications networks around the world.[4] Speaking in a global context, the World Trade Organization (WTO) recently noted, "[E]lectronic commerce is burgeoning as a means of doing business and shows every sign of continuing to expand at a rapid rate."[5]

Nowhere in the world has demographic, commercial, and technological forces coalesced in favor of electronic commerce as they have in Latin America. In line with this perspective, *Time* magazine recently identified Latin America as the Internet world's "Next Big Thing."[6]

Collectively considered, Latin America's potential e-commerce market consists of 100 million people representing approximately 65% of the region's total purchasing power.[7] Within this pool of Latin consumers, Internet demand is growing five times faster than the rest of the world.[8] Based on this demand, the number of Latin American Internet users is projected to increase from 4.8 million (representing approximately three percent of the world total)[9] to 34 million over the next three years (representing a 4000% increase from 1998).[10] The region's rate of Internet connectivity is already one of the fastest growing in the world.[11]

---

connected. Widely known and relied upon functions include, *inter alia*, e-mail, Usenet, the World Wide Web (www), file transfer protocol (FTP), Gopher, Wide Area Information Server, Internet Relay Chat (IRC), Multiple User Dungeons/Domains (MUDs), and MUD Object Oriental (MOOs). *See id.* at 131.

3. Naim, *supra* note 1, at L1.

4. *See Study from WTO Secretariat Highlights Potential Trade Gains from Electronic Commerce*, *at* http://www.wto.org/wto/archives/press96.htm. (last visited Jan. 24, 2000) (on file with author).

5. LUDGER SCHUKNECHT & ROSA PEREZ-ESTEVE, WORLD TRADE ORGANIZATION, A QUANTITATIVE ASSESSMENT OF ECONOMIC COMMERCE 2 (1999). "Electronic commerce" encompasses transactions involving any combination of consumers, businesses, banks, and governments. *See id.*

6. Sandy Fernandez, *Latin America Gets Wired*, TIME LATIN AMERICA (Apr. 3, 2000) (on file with author).

7. *See Getting Up and Running*, LATIN FIN. Sept. 1999, at 34.

8. *See A Force for Change*, LATIN FIN., Sept. 1999, at 37.

9. *See* Onelia Collazo, *E-Tailing*, LATIN FIN., June 1999, at 48.

10. *See id.* Another study, conducted by Ovum, projects that between 1998 and 2005, Internet usage will increase from 144,000 to 2.3 million people in Argentina, 877,000 to 2.8 million people in Brazil, and 41,000 to 397,000 people in Chile. *See Force for Change*, *supra* note 8, at 37.

11. *See* Emily Little, *Virtual Enterprises*, LATIN FIN., Sept. 1999, at 35.

Consistent with its characterization as a "nascent, yet . . . vibrant market place" with an "exciting, multi-billion dollar future,"[12] revenues from online sales were projected to reach $160 Million in 1999 and to reach in excess of $8 billion by 2003,[13] representing a growth rate of approximately one hundred seventeen percent.[14]

To date, Brazil has been the regional leader in online commerce and accounting, according to the results of one study which accounted for eighty-eight percent of the total volume in 1998.[15] Much of Brazil's leadership is attributable to the strength of its consumer protection laws[16] and the fact that its people are accustomed to transacting business online using state of the art systems developed by banks. This transactional reality serves as a solid base for the development of e-commerce.[17]

Mexico, alternatively, is the region's second largest market with six percent of all online transactions. The huge gap which exists between Brazil and Mexico in terms of volume of Internet transactions has led some analysts to comment that Mexico has not yet reached the "critical mass" of Internet users capable of supporting domestic e-commerce.[18] This criticism aside, online sales in Mexico are projected to rise from $50 million in 1999 to $800 million by 2003.[19] A substantial part of this explosive growth is expected to derive from Mexico's proximity to the United States and NAFTA arrangements regarding the cross border shipment of goods.[20]

ii. Business to Business (B2B)

B2B[21] transactions have dominated e-commerce. This situation is predicated on the ongoing development of different models of B2B

---

12. Giraldo Gutierrez, *Real Electronic Commerce Coming Soon to Latin America*, LATIN FIN., Sept. 1998, at 38.

13. *See Foreword*, LATIN FIN., Sept. 1999, at 5.

14. *See id.*

15. *See* Collazo, *supra* note 9, at 5.

16. *See* Scott Weeks & Onelia Collazo, *E-Merchants Turn to Online Payment Alternatives*, *at* http://www.latamnetstrat.com/cgi. . ./index.cgi?view=current&art_id=15722335 &from=visualco (last visited June 5, 2000).

17. *See* William M. Landers & Mark Ribeiro de Sa, The Internet and Latin America 9, (Aug. 18, 1999) (unpublished Lehman Brothers Report, on file with author). Brazil represents an estimated forty-six percent of all Latin American Internet users. *See id.*

18. *See id.* at 31.

19. *See* Sam Quinones, *E-Commerce Clicks*, MEX. BUS., May 20, 2000, at 30.

20. *See* Landers & Ribeiro de Sa, *supra* note 17, at 31.

21. In the context of Latin America, B2B e-commerce has been described as "the culmination of all that the Internet promises: efficiency, global reach, and opportunity for increasing revenues." Onelia Collazo, *B2B: Changing the Landscape*, *at* http://www. latamnetstrat.com/cgi?. . ./index.cgi?view=current&art_id=10428288&from=visualco (last visited July 6, 2000).

interaction. The model which has been most commonly adopted to date involves electronic data interchange (EDI) pursuant to the terms of a prearranged "master" or "framework" agreement between companies within an industry (or parents and subsidiaries) over a secure, leased-line, closed-circuit, and high-speed proprietary network (i.e., a value added network, or "VAN"). Using an EDI/VAN B2B approach, trading partners with an existing relationship can electronically "transmit purchase orders, shipping notices, bills of lading, receipts, invoices, payments, and financial reports."[22] Companies which are set up for EDI/VAN transactions stand to profit in several ways: "they can act as brokers, nabbing a percentage of each on-line sale. They can help other companies set up web sites where goods can be sold. They can earn revenue by letting vendors advertise on web sites set up as central markets for a specific industry."[23] Examples of Latin American companies which have established profitable B2B operations include Argentina's Disco, Brazil's Companhia Brasileira de Distribuicao, Globex, and Grupo Acucar, and Mexico's Cifra.

Notwithstanding the various efficiencies and profit opportunities associated with an EDI/VAN B2B model, its rigid structure and closed nature do impose limitations. Leasing lines to create a proprietary network is not an inexpensive undertaking, nor are the services of lawyers needed to draft, to execute, and subsequently to update the framework agreement. Whereas larger corporations are able to absorb the membership and/or usage fees commonly encountered with an EDI/VAN trading agreement, smaller companies which are unable to make this kind of expenditure may find themselves precluded from competing effectively. In this connection, U.S. studies have estimated that EDI trading arrangements are beyond the financial capacity of ninety-eight percent of U.S. companies.[24] As long as high costs continue to limit access, EDI trading arrangements will have a difficult time gaining wider acceptance.

A recently developed alternative to EDI/VAN B2B trading arrangements involves the use of a VPI (virtual private Internet).[25]

---

22. David L. Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures*, 17 J. MARSHALL J. COMPUTER & INFO. L. 769, 786 (1999) (citing Johnny Long, *E-commerce: Doing What's Best for Business, Forget Bits and Bytes: Business Processes Drive the Most Successful Electronic-Commerce Implementations*, DATA COMM. 69, 77 (1997)).

23. Miriam Hill, *Latest Net Craze: B2Bs*, MIAMI HERALD, Feb. 6, 2000, at 3E.

24. *See* Gripman, *supra* note 22, at 787 (citing Jay Palmer, *Net Change: Though the Internet Has Disappointed Many an Investor, It's About to Take Off*, BARRONS, July 7, 1997, at 25).

25. VPIs are also known as "Web EDI." *See* Gripman, *supra* note 22, at 787.

Borne of the growing movement from closed to open architectures, VPIs provide a closed, private environment within the public Internet community. While VPIs, like VANs, are built around a security-oriented framework agreement, VPI agreements tend to have less complex structures, thereby reducing the overall costs of access. This benefit is compounded by the savings derived from being able to create and operate a VPI trading site on the Internet, as opposed to a proprietary network. Looking forward, the continued fusion of cutting edge security technology solutions with open commercial trading models will likely have the effect of making B2B transactions more accessible to a broader base of companies.

Examples of early B2B market entrants include durable goods manufacturers (particularly high-tech hardware and components) and wholesalers of office supplies, electronic goods, scientific equipment, and raw materials or commodities. With time, more professional services (e.g., consulting, engineering, medical, architectural, accounting, legal, and pharmaceutical) are expected to be provided over the Internet.[26] Of the total $70 billion projected for global e-commerce sales over the next three years, $60 billion is expected to flow from B2B activity.[27] Regionally, B2B deals are expected to account for $6.7 billion of the $8 billion in e-commerce sales forecast for Latin America by 2003.[28]

iii. Business to Consumer (B2C)

B2C electronic commerce, in contrast with the aforementioned B2B models, involves isolated, relatively unstructured transactions carried out between merchants and consumers on the Internet.[29] While the wide-open architecture of this environment does not afford the same security or management control as a proprietary VAN, it does significantly improve the access that merchants and consumers have to one another.[30]

Following current trends, B2C e-commerce is expected to remain niche-oriented pending the evolution of certain Latin American

---

26. *See* Robert D. Hof et al., *The "Click Here" Economy: How the Internet Changes (Almost) Everything*, BUS. WK., June 27, 1998, at 128.

27. *See* Gutierrez, *supra* note 12, at 38.

28. *See* George Haj, *Latin E-Commerce Expecting Major Growth*, MIAMI HERALD, Feb. 2, 2000, at 11C. Globally, Forester Research estimates that US$1.3 trillion worth of business goods will be sold online. *See* Hill, *supra* note 23, at 3E.

29. B2C payments are usually by credit card. This necessitates the use of a secure server and credit card processing software.

30. *See Responding to the Legal Obstacles to Electronic Commerce in Latin America*, 17 ARIZ J. INT'L & COMP. L. 5, 9 (1999) [hereinafter *Issues Paper*].

purchasing habits,[31] improved access to an ever-broadening array of hardware,[32] the expansion of middle-class purchasing power (through

31. While credit card payments have been the "lubricant" of the Internet economy in the United States, their comparatively low penetration in Latin America may pose a barrier to the growth of e-commerce. As one author notes, "[c]redit is not widely available, or is more expensive, while the legal protection surrounding the use of credit cards and the purchase of products is not well developed or enforced." *See* Andre Vanyi-Robin, *Untapped Potential*, LATIN FIN., Dec. 1998, at 57. Consider, for example, the situation in Brazil, where fewer credit cards are issued than in Mexico, a country whose population is 60% smaller than that of Brazil's. *See* Landers & Ribeiro de Sa, *supra* note 17, at 31. This potential barrier may, however, be leapfrogged by the future introduction of electronic cash. "Electronic cash, broadly defined, includes both smart-card based tokens of value and digital coins or other digital tokens of value." *See* A. Michael Froomkin, *The Unintended Consequences of E-Cash*, Mar. 12, 1997 (unpublished paper presented at conference on *Computers, Freedom, and Privacy*, *available at* http://www.law.miami.edu/~froomkin/articles/efp97.htm). Some professionals are skeptical, however, about the immediate utility of e-cash, noting that until e-cash can offer the same degree of legal protection as that associated with credit and debit cards, these new payment media will be used primarily for "small and micro-payments." *Id.* Whatever the payment method ultimately used, it must be capable of resolving transactions instantly and securely. A promising step in this direction is the Secure Electronic Transaction, or "SET" standard for realizing electronic transactions. Representing the initiative of a consortium of credit card and technology companies (i.e., Visa, Master Card, Microsoft, IBM, Netscape, GTE, RSA, and Verisign), SET offers a more sophisticated and secure alternative to proprietary security systems such as Secure Socket Layers (SSL). Importantly, where SSL merely encrypts data being sent without validating the identity of the party at the other end, SET both encrypts and validates. *See* Weeks & Collazo, *supra* note 16. Moreover, the encryption technology underlying SET is significantly stronger (128 bit) than that used by SSL (40 bit). *See* Gripman, *supra* note 22, at 791. Many technology observers speculate that SET will be adopted as the leading industry standard for e-commerce security, in spite of the heavy demands it places on credit card transaction processing infrastructures and end user system processing capacities. *See* Jane Kaufman Winn, *The Emerging Law of Electronic Commerce*, *at* http://www.smu.edu/~jwinn/mbachapter.htm (last visited Jan. 24, 2000). Widespread recognition of SET would be a boon for e-commerce insofar as it would harmonize transactional technology and procedures. Another purchasing habit that needs to be overcome before B2C e-commerce catches on is the generalized Latin preference for physical shopping environments and actual human service over unknown and electronic facades. Finally, some commercial services that have become available through the Internet in the United States may simply be incompatible with Latin America's current social, cultural, and economic reality. For example, the recent popularity of online grocery shopping may not catch on quickly in those Latin nations where this activity is commonly the responsibility of domestic help.

32. PC penetration in Latin America ranges between five and ten percent. This low penetration rate is partly explained by the fact that an Internet capable computer can cost up to half a Latin wage earner's annual salary. *See* Collazo, *supra* note 9, at 50. To stimulate sales, some companies have taken the innovative step of bundling hardware and Internet access into an affordable package (e.g., TELMEX's Prodigy package). Other companies have begun to lease computers or to sell second-hand equipment, thereby making technology more affordable. *See* Paul Day, *Dot-Com or Dot-Gone?*, MEX. BUS., June 2000, at 60. In Argentina, one wealthy individual has even gone as far as to donate the needed equipment as an investment in his country's future. Not to be outdone, regional governments are also taking steps to make computer hardware and Internet access available to its citizens. *See Getting Up and Running*, *supra* note 7, at 31. The issue even found its way into Mexico's presidential campaign, when PRI candidate Francisco Labastida promised to put computers in every classroom, should he be elected. As a result of this tendency, electronic content is reaching places not previously anticipated. *See E-Commerce Grows Roots*, LATIN FIN., Sept. 1999, at 44. The Latin American information technology market is seen as the "greatest growth opportunity" in the world. *See*

increased per capita income levels and credit),[33] and the resolution of physical delivery obstacles.[34] Most recently,[35] the downturn in the U.S. Internet market has produced considerable consolidation (or strategic alliance formation) in the Latin American Internet world, as well as a stronger emphasis on revenue-generating business plans.[36] Emblematic of this new efficiency and discipline is the latest Internet catchphrase to hit the street, "P2P," standing, appropriately enough, for "path to profitability."

Markets which have been amenable to the B2C commercial model include, *inter alia*, travel, computer hardware and software, books, music, entertainment, wine, and flowers. Examples of early Latin B2C leaders are Argentina's Libreriras Yenny, Brazil's Submarino, and Mexico's Liverpool. The housing, food and beverage, and services sectors of Latin America are expected to enter the region's still incipient B2C market in the future. As computer-based shopping becomes more familiar, the average amount of money spent online by Latin American consumers is expected to increase from the 1998 average of $280 to $750 by 2003.[37]

Foreward, *supra* note 13, at 5. Supporting this observation is the fact that growth in server sales, PC penetration, and Internet access in Latin America is projected to surpass all other regions in the world. *Id.*

33. *See* Landers & Ribeiro de Sa, *supra* note 17, at 9.

34. In their attempts to overcome what has been characterized as the "last mile" of e-commerce, different companies have set out to provide better home delivery systems. Central to these new systems is wireless technology which permits parties to be paged or notified of deliveries via e-mail. *See* Eric Young, *No More "Sorry We Missed You"*, INDUSTRY STANDARD, June 12, 2000, at 96. This concern is also articulated in a Lehman Brothers report describing distribution systems as a "weak link" in the overall process of Latin e-commerce. That report relates how "post offices and private couriers are slowly developing capabilities to meet the needs of e-commerce." Landers & Ribeiro de Sa, *supra* note 17, at 9.

35. In hindsight it appears that many U.S. Internet "pure plays" (i.e., commercial entities that operate exclusively online) were guinea pigs for "brick and mortar retailers waiting to let someone else figure out online selling." Matt Krantz & Adam Shell, *Amazon Dive Deepens Dot-Com Gloom*, USA TODAY, June 26, 2000, at 1B. It is now thought that retailers which combine both a Web site and a physical storefront (a so-called "bricks and clicks" operation) stand the best chances of long term success. *Id.*

36. Early Latin American Internet pure plays which were not focused on profitability are also now struggling for survival. As in the United States, some Latin American B2C pure plays will likely "give way to their clicks and mortar counterparts that can leverage their less glamorous, but difficult to replicate, capabilities such as fulfillment and customer management." Karchi Lukac et al., *The Empire Strikes Back in Latin America*, *at* http://www.latamnetstrat.com/cgi. . ./index.cgi?view=current&art_id=18716989&from=visualco (last visited July 6, 2000).

37. *See* Collazo, *supra* note 9, at 50. Continued free Internet access as well as tax and duty free treatment of online purchases will no doubt be important drivers of these numbers.

b. Four Growth Drivers

i. Relaxed Export Restrictions

Underlying Latin America's substantial e-commerce growth potential are four key developments. First, the recent loosening of export and re-export restrictions by the U.S. Commerce Department on retail encryption commodities and software has had the effect of making encryption technology more readily available, thereby enabling greater levels of Internet activity.[38] The Clinton administration announced it would permit U.S. software companies to sell their most sophisticated encryption systems to twenty-three "friendly" nations, without having to obtain an export license.[39]

An important corollary to relaxed export controls has been the introduction of new methods of securing electronically transmitted data. By making it even easier to establish a secure transaction environment, products such as "chaffing and winnowing" (which uses electronic

38. *See* Edward J. Radlo, *U.S. Encryption Export Regulations Enter the 21st Century*, Spring 2000, *at* http://www.fenwick.com/pub/ip_pubs/u_s_encryption/u_s_encryption.htm (last visited Feb. 28, 2000) (on file with author). Important considerations in the lifting of export restrictions have been money laundering and terrorism. Initial export authorizations and licensing exemptions coincide with nations that are signatories to international agreements regarding money laundering and/or are not linked with terrorist activity. *See Is Security "SET" for E-Commerce?*, LATIN FIN., Sept. 1998, at 24. At the heart of the issue is the government's concern that the use of strong encryption technology by criminals would leave authorities powerless to counter threats to law and/or national security. Using this technology, cybercriminals that commit online frauds could, without additional control, conceal their identity. *See* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207, 221 (1997). In this connection, the U.S. government has attempted to establish a means of accessing the encrypted contents of electronic messages (referred to as "key escrow"). One early method called the "clipper chip" was abandoned after coming under attack from civil liberties groups. Most recently, the Clinton administration has proposed new legislation permitting the interception of electronic communications in connection with a list of approximately one hundred federal crimes (for which telephone wire taps pursuant to valid judicial orders have already been authorized). The legislation encompassing this so called "carnivore" system may be tacked on to privacy measures currently pending in Congress. *See White House Plan Would Bolster E-Mail Privacy*, MIAMI HERALD, July 18, 2000, at 1. Additionally, the U.S. government participates in Echelon, a global electronic surveillance project. *See* Elinor Abreu, *Keep Your Hands Off My Data*, INDUSTRY STANDARD, May 15, 2000, at 65.

39. As a "dual use" technology (i.e., military/civilian), an export license is required under the Arms Export Control Act and the Export Administration Act. Nations which are exempt from this requirement are the fifteen members of the European Union as well as Australia, Norway, Hungary, Poland, Japan, New Zealand, Switzerland, and the Czech Republic. Sales to other countries, including those of Latin America, continue to be subject to prior licensing and inspection by the Department of Commerce's Office of Strategic Trade. *See* Lenny Savino, *U.S. Relaxes Rules on Encryption Software*, MIAMI HERALD, July 18, 2000, at 4C. One example is the Internet Security Systems (ISS) which recently had to obtain government approval prior to furnishing strong encryption products for corporate networks and the Internet in Latin America. *See EUA Autorizam Exportacao de Sistema com Criptografia*, *at* http://www.globo.com/infotech/arquivo/tecnologia/20000627/4lpsy8.htm (last visited June 30, 2000) (on file with author).

authentication rather than encryption to provide security and maintain confidentiality) will further accelerate the growth of Internet based e-commerce.[40]

ii. New Network Access Points NAPs

The second development supporting Latin American e-commerce is the recent completion of the Latin Internet Exchange (LIX), the first NAP designed to switch South American Internet traffic via a Dominican Republic-based giga switch. To the extent it reduces delays, packet loss, and network failures, the operation of the LIX will make Latin American e-commerce transactions more reliable.[41] In this same connection, another Latin American-oriented NAP is currently being developed in Miami. Dubbed the "Gateway to Connectivity,"[42] this NAP will facilitate the flow of data, voice, and video to and from Latin America "where Internet usage and e-commerce are expected to explode in coming years."[43]

iii. Convergence

The last technological issue bearing on the e-commerce potential of Latin America involves developments within the cable and wireless phone industries. Notwithstanding Latin America's low PC penetration rates, cable television penetration rates throughout the region are generally high.[44] Recognizing a unique opportunity to benefit from the Internet boom, cable providers in Latin American nations have begun to offer either telephone services and/or Internet access using set-top box technology at rates significantly below the cost of a computer.[45] The expanding trend toward web/TV-like systems will greatly increase the

---

40. *See* Kurt M. Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 947 (1999) (citing Roland L. Rivest, *Chaffing and Winnowing: Confidentiality Without Encryption*, *at* http://theory.lcs.mit.edu/rivest/chaffing.txt (last visited Nov. 11, 1998).

41. *See Force for Charge*, *supra* note 8, at 37.

42. *Major International Technology Center to Rise in Downtown Miami's Park West/Overtown Area*, *at* http://www.biz.yahoo.com/bw/000517/fl-terrema.html (last visited June 29, 2000) (on file with author).

43. Beatrice E. Garcia & Jack Rejtman, *Bell South, EPIK Spearhead Network Access Point Movement*, MIAMI HERALD, Apr. 21, 2000, at 1C. Since the Internet's transformation from government-financed, commercially operated networks, NAPs have been established in New York; Washington, D.C.; Chicago; San Francisco; Atlanta; and San Jose, California.

44. Argentine cable television penetration rates, for example, are amongst the highest in the world. *See Force for Change*, *supra* note 8, at 37.

45. *See id.* Cable companies in Chile and Brazil are able to offer these services. *Id.*

base of Internet users and strengthen the potential for e-commerce in Latin America.[46]

A related development involves wireless platforms.[47] Using wireless application protocol (WAP), Latin America's cellular phone and PDA users are able to connect to the web without the use of a computer. This capability, considered in conjunction with the region's already high level of wireless device ownership and/or service subscription, translates directly into increased Internet penetration.[48] An executive with T1msn, the newly created joint venture between Telmex and Microsoft, states that, "Internet access will not always be through the PC. We will be seeing a lot of interactive devices coming onto the market such as cell phones, pagers, and in the end there will be a lot of devices we don't yet know of that will provide access."[49] Once connected, consumers can, *inter alia*, send and receive e-mails, access and maintain their agenda, track weather, monitor and trade stocks, order supplies, obtain customer service, and even (at least in Helsinki) purchase a Coca-Cola from a vending machine with embedded cellular technology.[50] Significantly, the cost of access a wireless device is well below that associated with a PC.

iv. Favorable Demographics

Independent of the aforementioned initial experiences and developments, current demographic trends suggest that Internet based e-commerce has a bright future in Latin America. According to market research, the key age range for Internet usage is currently fifteen to

---

46. The convergence of the web and pay TV has also occurred in the United States. Entities spawned through this process have, moreover, become leaders in the movement towards broadband technology (i.e., the delivery of data over high speed digital networks). Broadband barely exists in Latin America at present. By the year 2009, however, studies estimate that 10% of Brazilian households will use broadband Internet connections. *See* Chris Hussey et al., *Media: Pay TV in Brazil*, June 20, 2000, at 22. Even without convergence, the number of Latin American Internet users increased by eighty-five percent between 1998 and 1999. *See* Landers & Ribeiro de Sa, *supra* note 17, at 4.

47. *See* Jonathan Bokor, *Drafting Content License Agreements*, *in* FOURTH ANNUAL INTERNET LAW INSTITUTE 265, 275 (Ian C. Ballon et al. eds., 2000).

48. According to a study by Merrill Lynch, Latin America will have nearly as many wireless phones (fifty-three million) as it does fixed line phones (fifty-six million) by year's end. The demand for wireless service, and by extension, Internet access, is projected to increase sharply. *See* Beatrice Garcia, *The Wireless Invasion*, MIAMI HERALD, June 25, 2000, at 1E.

49. Day, *supra* note 32, at 60.

50. *See* Janet Guyon, *The World is Your Office*, FORTUNE, June 12, 2000, at 277. WAP-based communication is limited, however, by slow transmission speeds and difficulty in downloading or receiving graphics and video. These limitations may soon be moot, however, given recent advances in voice recognition technology. *See The Power of Speech*, ECONOMIST, May 13, 2000, at 60. Bluetooth, the short range wireless networking standard, holds great promise for the development of truly inter-operable platforms.

thirty-four years old.[51] With approximately 75% of Latin America's population falling within this range, continued growth of regional Internet usage seems assured.[52] The existence of such a large group of young and technologically savvy people significantly strengthens the foundation of Latin American e-commerce.

2. The Benefits

Latin American nations, corporations, and consumers will derive significant benefits from the realization of the region's Internet and e-commerce potential. Properly channeled, this potential can contribute to the development and integration of the whole hemisphere.[53]

a. Competitive Telecom Markets

The increasing linkage between commerce and the Internet has forced Latin telecommunications providers to improve networks and services so as to be Internet and e-commerce ready. While these advances may occur in real time, they frequently leverage prior global experience and leapfrog directly to proven state-of-the-art technology and implementation practices.[54] Should a local telecommunications company be unable to deliver the technological infrastructure and services required by modern business practices, Latin America's liberalized foreign investment laws have produced a large number of alternative technology and service providers that are capable of satisfying commercial demand (e.g., cable and satellite). To assure the continued operation of this performance incentive, it is important that national legislatures keep telecommunications and related media markets open to competition, foreign or otherwise.[55]

---

51. *See Getting Up and Running*, *supra* note 7, at 31.

52. *See id.*

53. *See* DALE MARSHALL & RUBEN MORALES, FTAA JOINT GOVERNMENT—PRIVATE SECTOR COMMITTEE OF EXPERTS ON ELECTRONIC COMMERCE, REPORT WITH RECOMMENDATIONS TO MINISTERS 4 (1999) [hereinafter FTAA REPORT].

54. An example of this phenomenon is Internet access. In the United States, free Internet access took almost two years to develop and implement, whereas its introduction in Latin America has virtually been overnight. *See E-commerce Grows Roots*, *supra* note 32, at 44; *see also* Luis Esnal, *El crecimiento de la Red en America latina: En Brasil, el acceso gratuito desatò la fiebre virtual*, LA NACION, Feb. 20, 2000 (on file with author).

55. Latin Ameriacan nations have taken different approaches to the issue of network architecture and the end-to-end (E2E) design principle (which advocates keeping networks simple and building intelligence in end applications). This principle operates in the United States with respect to telephone service and Internet access insofar as telephone companies have not been able to discriminate against ISPs, thereby assuring consumers choice. It has not been upheld, however, in the arena of cable. Under present law, cable companies are able to discriminate against and block certain ISPs, business concepts, services, and uses. *See* Lawrence Lessig, *Will AOL Own Everything?*, TIME, June 19, 2000, at 68. Brazil has adopted the E2E

b. Enhanced Commercial Operations

Improved telecommunications infrastructures, coupled with new modes of accessing the Internet, open the door to an increased volume of e-business. Using these increasingly efficient networks and technologies, corporations can disseminate more information regarding their requirements, products or services, overcome the comparative disadvantage of long distance to access new markets, improve performance throughout the supply chain, simplify order taking procedures, compress sales cycles, reduce administrative and transportation costs, and earn substantial customer loyalty dividends. Because the Internet is a nonstop world, corporations need not be constrained by time zone differences. It is estimated that by 2002, corporations will save up to US$1.25 trillion in costs by doing business over the Internet.[56]

The Internet is also proving beneficial in the way it "levels the playing field" and enables small- and medium-sized companies to compete head-to-head with large, established monoliths.[57] Therefore, the Internet poses a meritocratic alternative to Latin America's rigid business culture. For example, in Mexico, a country dominated for generations by powerful families and business groups with privileged access to credit and lawmakers and steady flows of U.S. venture capital have enabled young executives without strong political connections to create their own businesses.[58] Just a few years ago, such an outcome would have been much less likely. Similarly, the operation of Compranet, a government sponsored contract bidding site, enables businesses of all sizes to compete for lucrative public sector projects in a more even-handed way.[59]

---

design principle with respect to both telephone and cable service. By not allowing the privatized subsidiaries of Telebras to offer ISP services, the Brazilian government succeeded in creating a robust and dynamic market of private sector ISPs. More recently, ANANTEL, the agency which regulates cable TV services in Brazil, has been tasked with the responsibility of upholding an "open access" law requiring cable companies to allow any ISP to use their networks. Hussey et al., *supra* note 46, at 3. Mexico supports the design principle of E2E in theory, permitting private sector ISPs to operate. In terms of execution, however, Mexico has a highly concentrated ISP market that is unattractive to start-up service providers. *Id.*

56. *Foreward*, *supra* note 13, at 5.

57. An example of this leveling effect is the way in which Librerias Yenny, an Argentine book chain, can now compete with larger book chains such as Amazon in markets as distant as Norway, China, Australia, and the United States. *See* Collazo, *supra* note 9, at 48.

58. *See* Quinones, *supra* note 19, at 32.

59. Also, strong Internet connectivity may help governments operate more efficiently in extra-procurement contexts. For example, the creation of an online National Crime Data Bank has improved Mexican law enforcement capabilities. In Brazil, citizens can vote online and lawyers can file papers and pleadings with certain courts. Likewise, the Internet has made government-supplied legal, economic, financial, and trade information more readily available to

c. Empowered Consumers

Consumers also will experience new and enhanced forms of commercial power as a result of the Internet. Internet-based direct-to-consumer marketing, for example, enables consumers to browse for and purchase exactly what they want or need, without having to contend with the potentially limited selection or costly services of a middleman.[60]

> The Internet has changed the traditional model where manufacturers push things to distributors, then distributors market them to retailers, then retailers market them to consumers in a physical manner. In electronic commerce, it is the consumer who dictates terms, saying 'this is what I want, this is when I want it, and this how much I want to pay for it.' Before consumers got what those in the channel wanted. Now, a consumer can go right to the source . . . compare . . . and in the end, buy from whom he wants.[61]

Ultimately, electronic commerce will result in broader product choices, more streamlined ordering processes, and lower prices for consumers.

d. Energy Savings Benefit the Environment

Finally, to the extent that e-commerce reduces the amount of energy and materials consumed by businesses, the growth of the Internet can benefit the environment. Recent statistics best speak to the scope and nature of this potential benefit:

> a. The ratio of energy consumed per book sold in a traditional (brick and mortar) bookstore as opposed to one published on-line is 16:1.
> b. Reflecting increased levels of Internet usage, energy demand was flat in the United States during 1997 and 1998, despite economic growth of 9%.

---

private foreign investors. Developments such as these have led to the postulation of a correlation between the "continuing internationalization of the Internet" and the promotion of "liberal democratic values of openness and freedom." Froomkin, *supra* note 2, at 155. Professor Froomkin notes the existence of "empirical evidence" that "information connectivity is a powerful predictor of democracy." *Id.* (citing Christopher Kedzie, *International Implications for Global Democratization*, *in* ROBERT H. ANDERSON ET AL., UNIVERSAL ACCESS TO E-MAIL: FEASIBILITY AND SOCIETAL IMPLICATIONS (1995), *at* http://www.rand.org/publications/MR/MR650/mr650.ch6/ch6.html. Illustrations of this point are found in the experience of Mexico (where, by being in continuous communication with the outside world via the Internet, the Mexican army was forced to adopt a radically different, more humanitarian response to the Zapatista guerrilla uprising in Chiapas) and Cuba (where the government restricts Internet "surfing").

60. Examples of companies with successful direct-to-consumer marketing strategies are Dell, Gateway, and Compaq. In Mexico, sixty-five percent of Compaq's sales are transacted online, as opposed to traditional distribution channels. *See Non Stop E- Business*, LATIN FIN., Sept. 1999, at 42.

61. *The Ups and Downs of Cyber Business*, LATIN FIN., June 1999, at 51-52.

> c. The Internet may eliminate the need for 5% of total commercial building space, including 1.5 billion square feet of retail space, 1 billion square feet of warehouse feet, and 2 billion square feet of office space.
> d. The aforementioned space reductions would result in an estimated savings of 53 billion kilowatt hours of electricity and 67 billion cubic feet of natural gas per year.
> e. The Internet could save 2.7 million tons of paper each year, regardless of the increase in the use of paper.[62]

The foregoing statistics directly support the claim that "the Internet can turn buildings into web sites, replace warehouses with supply chain software, . . . transform paper and cds into electrons, and replace trucks with fiber optic cables."[63] Considering the extensive degree of environmental degradation and natural resource depletion that has already occurred in Latin America, e-commerce represents a valuable opportunity for these nations to simultaneously enjoy the benefits of commerce and preserve the region's remaining environmental patrimony.

B. The Requisites of Electronic Commerce and Latin America's Tradition of Legal Formalism

To realize fully the benefits associated with Latin America's "multi-billion dollar" e-commerce potential, there must exist a transactional environment characterized by certainty of electronic contract and security of information.[64] Certainty of electronic contract implies, minimally, that: (1) electronically transmitted data messages will be given legal effect; (2) electronically generated data messages can satisfy writing requirements and form the basis of a contract; (3) electronically created "signatures" will be recognized and given effect by courts; and (4) there be a clear expression of the interrelationship between electronic signatures and additional writing and/or signature formalities. Security of information, in turn, enables parties to an electronic contract to identify each other with certainty and verify that the content of a data message has not been altered in transmission.[65] At the risk of over-simplifying the foregoing concepts, business and consumers must be confident that e-commerce practices and procedures are both legally valid and trustworthy.

---

62. *See* Beth Cox, *E-Commerce Said to be Eco-Friendly*, Jan. 11, 2000, *at* http://www.ecommerce.Internet.com/opinions/article/0,1281,3551_27901,00.html (last visited Jan. 24, 2000) (on file with author).

63. *Id.*

64. This is consistent with Professor Lessig's observation that the needs of commerce have "pushed for changes in the architectures of the Net to enable more secure and safer commerce." LAWRENCE LESSIG, CODE & OTHER LAWS OF CYBERSPACE 39 (1999).

65. *See* FTAA REPORT, *supra* note 53, at 11.

Certainty of electronic contract and security of information have not, to date, been widely available in Latin America. More critically stated, "Latin American law, especially that found in its nineteenth century civil and commercial codes, is unfriendly to e-commerce."[66] This fact can be largely, but not totally, attributed to the traditional formalism with which the region's codes are interpreted. As Latin American practitioners relate, the region's "legal frameworks were created to deal with physical transactions and may be insufficient to secure the enforcement of electronic contracts and ensure the validity of electronic signatures."[67]

Latin American judges are often unwilling to expand the meaning or applicability of commercial code provisions beyond the limits of a statute's text. True to the civil heritage, Latin American judges mechanically apply the law. It is not part of their job to "find" or interpret the law. For a Latin American judge to recognize and give effect to electronic data messages or signatures, it is necessary to have written statutes.[68]

Similarly, express statutory guidance is necessary if a Latin American judge is to know how to receive and evaluate the evidentiary value of an electronically generated data message. This need becomes more acute where additional levels of authentication or attestation are required (e.g., a notarization) and/or the judge is unfamiliar with the fundamental strengths and weaknesses of the technologies and procedures underlying electronic communication and interaction.

Inadequate statutory guidance, compounded by a preference on the part of the Latin American bench for paper-based contracts and signatures, results in parties being unable to predict with confidence the interpretation Latin courts will give to electronic instruments, documents, and signatures. Moreover, the continued absence of effective statutory guidance impedes the development of important supplementary sources of interpretation such as "jurisprudencia" or the "sumula."[69] These outcomes could lead many merchants within the international and Latin American business communities to resist the replacement of paper-based forms of doing business, thereby perpetuating inefficient traditional commercial practices.

---

66. *Issue Paper*, *supra* note 30, at 13.

67. *Id.*

68. Scott Weeks, *Experts Meet on Legal Obstacles to E-Commerce*, LATIN AM. INTERNET STRATEGIES NEWSL., Oct. 1999, at 2.

69. *Sumula* is a Portuguese term conceptually akin to jurisprudence. It does not have a binding, *stare decisis* effect, but rather is persuasive authority.

Left unaddressed, low levels of certainty of contract and security of information could negate the region's bright potential with regard to electronic commerce and "raises the specter of non-compliance, breach of obligations, and costly lawsuits."[70] Absent the existence of a legal, technological, and cultural infrastructure capable of promoting its growth in Latin America, regional demand for electronically negotiated and procured goods and services may continue to be satisfied offshore, exacerbating the effect of the financial outflows that have characterized the early development of global electronic commerce. Studies indicate that 74% of Latin America's estimated US$170 million in online transactions for 1998 entailed capital outflows from the region.[71] Failure in this regard could also contribute to the creation of a "digital divide" between Latin America and an otherwise rapidly developing world.[72] Such a development would, in turn, undermine the positive effects associated with the balance of forward-looking and integration-oriented policies pursued by the nations of Latin America in the recent past.

C. The Model Law on Electronic Commerce: A Supposed Panacea

In their attempts to overcome the obstacles posed by the formalistic interpretation of antiquated codes and doctrines, many Latin American nations have begun to revise and update their commercial laws using the UNCITRAL's Model Law on Electronic Commerce (MLEC)[73] as a point of reference.[74] This evolutionary step is squarely in line with the increasingly accepted view that commercial law statutes should be "reformed in response to significant changes in business practices to reduce uncertainty that can arise under existing law."[75]

Adopted in 1996, the MLEC is a framework of model principles and provisions designed to facilitate legal certainty with regard to

---

70. Daniela Ivascanu, *Legal Issues in Electronic Commerce in the Western Hemisphere*, 17 ARIZ J. INT'L & COMP. L. 219, 221 (2000).

71. *See* Daniel Pruzin, *Open Telecom Markets Said to Be Key to E-Commerce for Developing Nations*, 16 INT'L TRADE REP. (BNA) 844 (May 19, 1999). In contrast, only ten percent of United States online purchases were made abroad. *Id.*

72. *See WTO Urged to Study Developing Nations' Participation in E-Commerce*, 15 INT'L TRADE REP. (BNA) 409 (Mar. 11, 1998).

73. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, G.A. Res. 51/162 U.N. GAOR, (1996) [hereinafter MLEC], *available at* http://www.un.org.at.uncitral/english/electcom/ml-ec.html (last visited Jan. 20, 2000).

74. *See Issue Paper*, *supra* note 30, at 7. In keeping with historic experience, Latin American e-commerce initiatives and policies have largely come directly from the government, without significant private sector input. This centralized approach to legislation stands in sharp contrast to U.S. experience where, until now, the private sector has taken an active role in the regulation of the Internet and the formulation of e-commerce policy.

75. Weeks, *supra* note 68, at 3.

electronic contracting, as well as the creation of uniform security infrastructure standards.[76] The preamble states that its principles are intended to "assist states in enhancing their legislation governing the use of alternatives to paper based methods of communication and storage of information and in formulating such legislation where none currently exists."[77] To the extent that it contributes to the establishment of a predictable, minimalist, and simple legal environment within which private electronic enterprise and free markets can flourish, the UNCITRAL's MLEC is generally not viewed as a form of heavy-handed or unnecessary regulation.[78]

---

76. According to the Global Information Infrastructure (GII) report prepared by the White House, the MLEC

> establishes rules and norms that validate and recognize contracts formed through electronic means, sets default rules for contract formation and governance of electronic contract provisions, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings.

Global Information Infrastructure Framework, *at* http://www.whitehouse.gov/wh/new/commerce/read/html [hereinafter *GII*] (last visited Jan. 24, 2000) (on file with author).

77. MLEC, *supra* note 73, pmbl.

78. Much debate has occurred with respect to the regulation of the Internet. At one end of the debate spectrum are the advocates of a liberal, self-regulatory approach where parties are free to make and enter into their own agreements within the limits of the law. Pointing to the fact that the design concept of cyberspace itself is premised on the "displacement of a certain architecture of control" (i.e., the replacement of single purpose telephone networks with a multipurpose network of packet switched data), this group envisions a space characterized by "freedom without anarchy, control without government, consensus without power." Lessig, *supra* note 64, at 4. The manifesto of this group has been described in the following terms: "We reject: kings, presidents and voting. We believe in: rough consensus and running code." *Id.* U.S. examples of self-regulation include the voluntary posting of privacy policies, the grass roots development of nongovernmental monitoring organizations, and the independent formulation of and adherence to industry-specific guidelines and standards. On the other side of the continuum are those individuals and groups which propose a rigid, highly regulated approach to every aspect of the Internet. They argue that legislative uncertainty "increases costs and discourages transactions." A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49, 108 (1996). An absolute version of this approach is undesirable insofar as the resulting proliferation of discordant national and international regulation (referred to as "crazy quilt") would likely inhibit the growth of e-commerce. In the worst case scenario, moreover, some regulation-oriented nations may be tempted to structure legislation in such a way as to secure competitive advantages over other states. *See* Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reforms*, 72 Tul. L. Rev. 1931, 1946 (1998). Notwithstanding the certainty and clarity entailed in an absolute approach, competing considerations of uniformity and competition/protectionism make it tantamount to taking "one step forward and two steps back." Thomas J. Smedinghoff & Ruth Hill Bro, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advanced E-Commerce*, 17 J. Computer & Info. L. 723, 753 (1999). The best approach is that which strikes a balance. Regulation in and of itself is not a bad thing, and ours is an "age of statutes." *Id.* at 763. History is full of examples of legislation stimulating the growth of industries. Given the many unique issues raised by the Internet, e-commerce, electronic signatures, and online security generally, "it may be appropriate to address these issues legislatively, so long as it is done in a

As a model law,[79] the principles and procedures contained within the MLEC technically represent what has been described as a "statutory ideal" for enacting member states characterized by different legal, political, and economic systems.[80] According to the guide accompanying the MLEC, it neither attempts to set forth all the rules and regulations necessary to implement the model law's principles and procedures in an enacting state, nor purports to cover every aspect of electronic commerce.[81] In fact, the guide specifically contemplates the possibility of a state issuing regulations to "fill in procedural details for procedures authorized by the MLEC" in accordance with the "specific, possibly changing circumstances at play" in an enacting state.[82]

Given the general consensus that has arisen regarding the "correctness" of the MLEC's principles and provisions, it has been generally hoped that its provisions would be adopted by enacting states without significant modification,[83] thereby establishing uniformity with regard to the law applicable to alternatives to paper-based methods of communication and storage of information.[84] For the UNCITRAL, numerous departures from the core provisions of the MLEC are to be avoided so as to not raise needless obstacles to the development of the

---

way that does not unfairly favor one technology over another." *Id.* at 762. In this equation, freedom of contract should be balanced against "statutes that promote predictability, reduce uncertainty, and provide default rules to fill in gaps in contractual coverage or to minimize the need (and attendant cost) of contracting to anticipate every possible eventuality." *Id.* at 763. These statutes should be viewed not as contractual "straightjackets," but rather as a "welcome guide through unexplored Internet territory." *Id.* This perspective is also adopted by the White House, which notes, in principle, that "governments should avoid undue restrictions on electronic commerce" and "refrain from imposing new and unnecessary" statutory regimes. *GII*, *supra* note 76. Recent federal electronic signature and privacy legislation clearly contradicts the position espoused by the GII. *See* Lawrence L. Knotson, *Clinton Ushers in New Era*, Miami Herald, July 1, 2000, at 22A. The U.S. government's regulation of specific sectors of the Internet (e.g., cybercrimes, e-signatures, intellectual property, and advertising) is expected to increase in the future. Latin America can boast of a few instances of self-regulation. For example, Brazilian ISPs recently organized to combat pedophilia on the web, while in Mexico Internet-oriented dispute resolution services have been launched by the private sector. For the most part, however, the nations of Latin America have, true to their continental European heritage, closely followed the path of regulation.

79. *See* Boss, *supra* note 78, at 1953. "Model laws" are uniform legal rules designed to serve as models for legislation by states. In contrast, treaties and conventions bind party nations to their terms.

80. Paul J. Keenan, Jr., *A Case Study of the Approaches to Digital Signature Legislation: The Argentine Digital Signature Law Under the UNCITRAL Model Law 1* (1999) (unpublished manuscript on file with author).

81. *See* MLEC, *supra* note 73, ¶ 13.

82. *Id.*

83. Weeks, *supra* note 68, at 2.

84. *See* MLEC, *supra* note 73, pmbls. This expectation stems from the consensus that has arisen regarding the correctness of the model law's principles. *See* Boss, *supra* note 78, at 1953.

modern communication techniques underlying e-commerce.[85] This point is also emphasized by the Free Trade Area of the Americas (FTAA), which calls for international cooperation and coordination as a means of avoiding national approaches to e-commerce that "fragment regional and global markets and unduly restrict trade."[86] The essential challenge is to "take countries of divergent economic capabilities, legal heritage, telecommunications infrastructures, and needs and bring them together to develop common analyses of and approaches to problems never encountered previously."[87] Considered from this perspective, the desirability of the MLEC is enhanced because "the only way that countries throughout the region will be able to understand each other [is] by adopting measures that are similar in scope."[88]

D. The Emerging Framework of Disharmony

Responding to the aforementioned pressures to adapt traditional doctrines to contemporary business practices and technologies, many nations, including many in Latin America, have enacted or are in the process of enacting domestic legislation inspired either in totality or in part by the MLEC.[89] While this domestic legislation succeeds, to varying degrees, in providing a framework of certainty and security within which e-commerce can grow, it cannot be presently said that the regulation of e-commerce has been "harmonized under the umbrella of the MLEC."[90] As a member of the ICC's delegation to the UNCITRAL's working group on electronic commerce explains, "[T]he sovereignty of each jurisdiction and the rush to promote electronic commerce has created differences in legislation and legislative proposals."[91] Instead of facilitating a coordinated and unified legislative approach to e-commerce, the MLEC appears to have been used primarily as the springboard for a "proliferation of competing and contradictory" national and international legal schemes.[92] The findings of the National Law

85. *See* MLEC, *supra* note 73, ¶ 69.

86. FTAA Report, *supra* note 53, at 5.

87. *See* Boss, *supra* note 78, at 1945.

88. Lola L. Grabb, *Panel II: Issues of Formalities: The Formation and Validity of Electronic Agreements*, 17 Ariz. J. Int'l & Comp. L. 119, 122 (2000).

89. *See Issue Paper*, *supra* note 30, at 7. Latin American nations which have undertaken to bring their legislation into line with the reality posed by the Internet and e-commerce include: Brazil, Mexico, Colombia, Argentina, Chile, Peru, Paraguay, and Ecuador. *See* Weeks, *supra* note 68, at 3.

90. Weeks, *supra* note 68, at 3.

91. John Andres Avellan V., *John Hancock in Borderless Cyberspace: The Cross-Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts*, 38 Jurimetrics J. 301, 302 (1998).

92. Boss, *supra* note 78, at 1946.

Center for Inter-American Free Trade, OAS, and the Business Software Alliance touch on this development by noting "unfortunately, not all . . . rules are consistent and conflicts abound."[93] These groups conclude that "no effort has been made to harmonize the key principles, let alone rules."[94] To the extent that the MLEC has served as the impetus for legislation that is, inconsistent, it may have spawned more problems than it resolved.

Using the MLEC and contemporary scholarship as a benchmark, this paper examines the extent to which implemented and forthcoming legislation from Brazil, Mexico, and Colombia differ with respect to threshold contracting issues likely to pose obstacles to the growth of e-commerce in light of Latin America's antiquated codes and formalistic legal tradition. This focus essentially coincides with Chapters I (General Provisions) and II (Application of Legal Requirements to Data Messages) of the MLEC, although the "Signature" discussion does expand to consider fundamental aspects of Brazilian, Colombian, and Mexican public key infrastructure (PKI) provisions, as well as the interrelationship between electronic signatures and the Latin American notary. Where possible, the practical commercial and policy implications associated with specific principles, procedures, and technologies are identified and analyzed in relation to the reality of Latin America. It should be noted that there are many other fundamental issues raised by doing business over the Internet which remain almost totally outside the scope of this paper, including, *inter alia*, the communication of data messages (i.e., contract formation and establishing time and place of dispatch), the protection of intellectual property rights (for example, the registration and use of domain names), the protection of consumers, the assessment and collection of taxes and duties for online transactions, questions of jurisdiction, choice of law, and dispute resolution. Already, significant differences in approach to many of these issues have been noted among Latin American nations.

Having demonstrated the failure of the MLEC to engender substantial uniformity in domestic e-commerce legislation, this paper concludes by arguing that the emergence of disharmonious rules, standards, and procedures constitutes a new and different obstacle to the continued growth of electronic commerce in Latin America. The final part of the conclusion offers recommendations, the implementation of which would help Latin American nations overcome the negative effects

93. *Issue Paper*, *supra* note 30, at 13.
94. *Id.*

of divergent legislation and secure the benefit of the region's e-commerce potential.

II. RECENT AND FORTHCOMING ELECTRONIC COMMERCE LEGISLATION FROM BRAZIL, MEXICO, AND COLOMBIA: CREATING AN ARCHITECTURE OF UNCERTAINTY AND INSECURITY

Brazil, Mexico, and Colombia have been selected to be the focus of this comparative analysis for several reasons. As the nations with the largest and most powerful economies in Latin America, it is important to understand the ways in which Brazil and Mexico are approaching the subject of e-commerce. Even at this early stage, differences in terms of legislative inspiration and approach are apparent.

Underscoring its strong historical ties with Portugal (and the rest of the European Union), Brazil's draft e-commerce legislation[95] has, at times, more in common with European Union directives on the subject than with the UNCITRAL's MLEC.[96] Considered in the context of Brazil's reluctance to embrace the Convention for the International Sale of Goods (CISG), another UNCITRAL initiative, this orientation is not entirely surprising. While it is impossible to know how the final version of Brazil's e-commerce legislation will appear, the approach of the current bill strikes an excellent balance between legal certainty and commercial flexibility.

Mexico's e-commerce initiative,[97] on the other hand, incorporates only those points of the MLEC which are not inconsistent with its minimalist and technologically neutral orientation. Reflecting strong U.S. influence in its self-regulatory spirit, Mexico's e-commerce reforms provide maximum commercial flexibility, but *de minimis* legal certainty. The wisdom of this United States-style approach may eventually come into question given the very different ways U.S. and Mexican judges

---

95. *Projeto de Lei* [hereinafter *Projeto*] No. 1.589, de 31 de agosto de 1999, *at* http://www.natlaw.com/ecommerce/docs/e-commercebill-brazil.htm (last visited Mar. 6, 2000) (on file with author). The Sao Paulo Division of the Brazilian Legal Association contributed to this bill. It was presented to the *Camara dos Deputados* as an appendage to Dr. Helio's Bill No. 1.483 of 1999.

96. *See* Weeks, *supra* note 68, at 3.

97. *"Decreto por el que se Reforman y Adicionan Diversas Disposiciones del Codigo Civil para el Distrito Federal en Materia Comun y para Toda la Republica en Materia Federal, del Codigo Federal de Procedimientos Civiles, del Codigo de Comercio, y de la Ley Federal de Proteccion al Consumidor"* [hereinafter *Decreto*]; approved by the *Comision de Comercio de la Camara de Diputados* Apr. 6, 2000; approved by the *Pleno de la LVII Legislatura de la Camara de Diputados* on Apr. 26, 2000; approved by the Mexican Senate on May 3, 2000, *at* http://www.natlaw.com/ecommerce/docs/e-commerce-iniciative-mexico.htm (last visited May 12, 2000) (on file with author).

respond to situations where the legislature has not yet "occupied the field" with respect to an issue.[98]

Colombia is included in this analysis not so much for its size or the power it commands in the global market but because its e-commerce legislation was the first in Latin America to be enacted into law. Of the three pieces of national legislation considered, Colombia's is most consistent with the spirit and substance of the MLEC.[99] The principal exception to the foregoing statement involves the technology-specific approach Law 527 takes to signatures. As shall be discussed in greater detail infra, the de facto requirement of digital signatures and public key infrastructures gives merchants and/or subscribers considerable legal certainty, but no flexibility.

The other important reason for including Colombia is that Latin America's first formal challenge to e-commerce legislation has been filed in its Constitutional Court. This challenge is significant in that its outcome may influence the future development of e-commerce regulations in Latin America.

Regardless of the inspirations underlying Brazil, Mexico, and Colombia's e-commerce legislation, each initiative is geared towards the same basic goal: creating the principles and procedures by which e-commerce transactions can be realized with legal certainty and technological security. The substantive ways in which the e-commerce legislation of these nations have diverged, as well as the legal certainty and commercial flexibility trade-offs implicit in each approach, are considered in the following Parts.

A. General Provisions

1. Sphere of Application

Article 1 of the MLEC states that the terms of the Model Law are applicable to any kind of information in the form of a data message used

---

98. As recently as April 2000, Mexico had considered a package of legislative reforms which balanced significant provisions of the MLEC with the needs and abilities of local commerce and infrastructure. Another group within Mexico had advocated the outright adoption of the MLEC. *See* Jose Maria Abascal Zamora, *Debe Mexico Adoptar la Ley Modelo de la CNUDMI sobre el Comercio Electronico?*, El Mundo de Abogado, Mar. 2000, at 53.

99. *Ley 527, Por Medio de la cual se Define y Reglamenta el Acceso y Uso de los Mensajes de Datos, del Comercio Electronico y de las Firmas Digitales, y se Establecen las Entidades de Certificacion y se Dictan Otras Disposiciones* [hereinafter *Law 527*], D.O., Aug. 21, 1999, *at* http://www.natlaw.com/colombia/topical/ec/stcoec/stcoec1.htm (last visited Mar. 14, 2000) (on file with author). Colombia's near total adoption of the MLEC may reflect the tendency of smaller nations with emerging economies to look to international instruments as a means of filling gaps in their domestic laws. *See* Boss, *supra* note 78, at 1940.

in the context of commercial activities.[100] This is not to say that the MLEC is intended to be inapplicable to civil transactions. The accompanying guide clarifies that "nothing . . . should prevent an enacting state from extending the scope . . . to cover uses . . . outside the commercial sphere."[101]

E-commerce legislation from both Mexico and Colombia departs from the suggested approach of the MLEC. Mexico's reforms expressly encompass, *inter alia*, the Federal Civil Code[102] and the Code of Commerce.[103] Colombia's Law 527, on the other hand, is applicable to all types of information in data message form, without regard to the civil or commercial nature of the underlying transaction.[104] These approaches are progressive in that they effectively overcome the well established civil law tradition of formally characterizing contracts as either civil or commercial. Having made their e-commerce laws applicable to all transactions, Mexico and Colombia can offer legal certainty to the broadest possible range of electronic transactions. These expansive orientations may prove beneficial to the extent that an increased level of trade-in services (e.g., law, accounting, engineering, and medicine) entails a corresponding increase in the electronic exchange of documents.

The sphere of application of Brazil's e-commerce legislation differs from Mexico's and Colombia's in that Law No. 1589 does not expressly indicate whether its application is either commercial or civil, or both commercial and civil. Article 1 indicates, *inter alia*, that the law applies to "electronic commerce," but does not otherwise preclude a civil application.[105] Given the way free standing legislation in Brazil tends to be applicable to both civil and commercial actions, it is probable that Law No. 1589 will have the same comprehensive effects as Mexican and Colombian legislation.

2. Interpretation

Article 3 of the MLEC provides that the Law 527's interpretation shall have regard for its international origin and need to promote

100. *See* MLEC, *supra* note 73, art. 1.

101. *Id.* ¶ 26.

102. *See* Código Civil [C.C.D.F.] (Mex.) (as reformed with respect to articles 1803, 1805, and 1811).

103. *See* Código de Comercio [Cód.Com.] (Mex.) (as reformed with respect to articles 80, 89, and 93). These provisions represent an important improvement over the original draft version of Mexico's draft e-commerce law which applied only to commercial transactions.

104. *See Law 527*, *supra* note 99, art. 1.

105. *Projeto*, *supra* note 95, art. 1.

uniformity and good faith.[106] In addition to advancing the interpretational objectives of article 7 of the UNCITRAL's CISG, this provision is designed to facilitate the harmonious international development of e-commerce law by ensuring that MLEC inspired domestic legislation is not interpreted primarily with reference to concepts of local law.[107] Given the existence of an interpretational standard which transcends the potential pitfalls and biases of national law, parties should be more confident about entering international electronic transactions.

Colombia's Law 527 tracks the elements of MLEC Article 3 regarding interpretation exactly.[108] Article 2 of Brazil's draft legislation substantially follows the MLEC model, with the exception that its article 2 emphasizes the dynamic progress of technological instruments, as opposed to the need for international uniformity.[109]

Mexico's e-commerce legislative reform package, in contrast, contains no express clause offering interpretational guidance. This does not mean, however, that Mexico's draft legislation can be interpreted arbitrarily. By virtue of the legislation's applicability to the Federal Civil Code and Code of Commerce, its contents are subject to being interpreted, respectively, in accordance with (1) the usage and customs of different countries, the general principles of contract law, and the stipulations of parties[110] and (2) the common customs of merchants.[111] Moreover, as a party to the CISG, Mexico's law pertaining to the international sale of goods mandates interpretations which have regard for a transaction's international origin and the need to promote uniformity and good faith.[112] From the foregoing, it is apparent that both domestic law and international treaty obligations require Mexico's e-commerce legislation to be interpreted in a way harmonious with international practice.

---

106. *See* MLEC, *supra* note 73, art. 3. Matters governed, but not expressly settled by, the MLEC are to be resolved in conformity with the general principles on which the MLEC is based. *See id.* art. 3(2). The MLEC guide identifies five principles which nations can look to in interpreting e-commerce legislation: "1) to further e-commerce among and within nations; 2) to validate transactions entered into using new technologies; 3) to promote and encourage the introduction of new information technologies; 4) to promote uniformity of law; and 5) to support commercial practices."

107. *See id.* ¶ 41.

108. *See Law 527*, *supra* note 99, art. 3.

109. *See Projeto*, *supra* note 95, art. 1.

110. *See* C.C.D.F., *supra* note 102, arts. 1856 and 1858.

111. *See* Cód.Com., *supra* note 103, art. 2.

112. Recent Mexican (*tesis* a form of jurisprudence) jurisprudence establishes the superior position of international treaties relative to federal laws. *Tratados Intenacionales. Se Ubican Jerarquicaments por Encima de las Leyes Federales y en Segundo Plano Respecto de la Constitucion Federal*, 10 J.S.C. 46, 46 (9a època 1999).

B. Application of Legal Requirements of Data Messages

1. Legal Recognition of Data Messages

Article 5 of the MLEC establishes an important foundation for e-commerce by articulating the minimum requirement that information not be denied legal effect, validity, or enforceability solely because it is in the form of a data message.[113] This provision is designed to prevent discrimination against electronically generated and communicated exchanges. It is not intended, however, to ensure the general legal validity of data messages.[114]

Article 5 of Colombia's Law 527 clearly follows the MLEC provision. One deviation is Law 527's reference to "all information," as opposed to simply "information."[115] This expansion reflects the fact that Law 527 has a broader sphere of application than the MLEC. As a result of this provision, a Colombian judge can not deny legal effect or validity to information simply because it is in the form of a data message.

While it is both explicitly and implicitly clear from Brazil's and Mexico's e-commerce legislation[116] that information in the form of a data message can be accorded recognition, neither Brazil's nor Mexico's legislation make an unequivocal statement affirming the principle of nondiscrimination. Lacking clear guidance of the type proposed by the MLEC, it will be easier for Mexican and Brazilian judges to decline recognition of a data message merely because of its electronic form. Mexican and Brazilian lawmakers could strengthen e-commerce's legislative foundation by rectifying this shortcoming.

2. Writing Requirements

Article 6 of the MLEC provides that where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is "accessible so as to be usable for subsequent reference."[117] This provision is premised on the principle that data messages which meet certain legal/technological requirements

---

113. *See* MLEC, *supra* note 73, art. 5.

114. *See id.* ¶ 46.

115. *See* Law 527, *supra* note 99, art. 5.

116. Código Federal de Procedimientos Civiles [C.F.P.C.] (Mex.), art. 210-A; Cód.Com., *supra* note 103, arts. 1205 and 1298-A. Brazil's article 3, in turn, does not expressly recognize the legal effect, validity, or enforceability of information contained in data messages. Rather, it implicitly recognizes a party's ability to use electronic means in contractual contexts. *See Projeto*, *supra* note 95, art. 3. Article 6 supports this interpretation by noting that nonface-to-face offers (i.e., electronically communicated) are permissible, provided certain requirements are met. *See id.* art. 6.

117. MLEC, *supra* note 73, art. 6.

are the "functional equivalent" of a paper document.[118] This provision represents an important building block for e-commerce by neutralizing the traditional, formalistic insistence of Latin American courts on paper-based writings.

Noting that a writing requirement is the "lowest layer in a hierarchy of form requirements" designed to provide distinct levels of reliability, traceability, and inalterability, the guide explains that more "stringent" authentication requirements (e.g., those associated with signatures, originals, and authentications) are excluded from the scope of its terms.[119] In taking this approach, the MLEC leaves it to enacting nations to identify those transactions which, for reasons related to underlying authentication requirements, cannot be realized by electronic means.

Article 6 of Colombia's Law 527 tracks MLEC article 6 verbatim, holding that data messages satisfy the requirement of a writing where the data message is accessible for subsequent reference.[120] Through this provision, judges are given the express guidance and authority needed to overcome civil and commercial laws requiring written (i.e., paper-based) contracts in certain circumstances.[121] Sub-parts (a) and (b) of article 1 of Law 527 enhance this clarity by unambiguously stating that the terms of this provision do not apply to consumer protection laws and international

---

118. *See id.* ¶ 16. Although the MLEC Guide specifically notes the functions served by traditional, paper-based writing (i.e., creating tangible evidence of the intent of parties to bind themselves; ensuring that parties are aware of the consequences of their acts/words; providing legibility; protecting against alteration over time; providing a permanent record of the transaction; allow for reproduction; allowing for authentication by means of a signature; and ensuring the acceptability of the document's form for public authorities and courts), it carefully notes that for the purposes of electronic communication, it would be inappropriate to adopt an overly comprehensive notion of a writing's function. *See id.* ¶ 48. As the Guide further elaborates, the purpose of article 6 is not to establish a requirement that, in all instances, data messages should fulfill all conceivable functions of a writing. *See id.* ¶ 49.

119. *See id.* ¶ 49. Consistent with this approach, MLEC article 6 contains an optional clause whereby an enacting state can preclude the application of its provisions from "certain types of situations, depending on the purpose of the final requirement in question." *Id.* ¶ 51. Specific examples of situations in which states may wish to maintain special writing requirements include: (1) the providing of notice or warning of factual risk (for example, with regard to products) and (2) international treaty obligations (the guide points out, by way of example, the requirement that a cheque be in writing, pursuant to the Uniform Law for Cheques, Geneva, 1931). *See id.*

120. *See Law 527*, *supra* note 99, art. 6.

121. Colombian law requires the following transactions to be in writing: (1) promises to enter a contract (article 89 of Law 153/1987); (2) conveyances of intellectual property rights (article 119 of Law 23/1989); (3) transfers of certain credits and rights (articles 1959 and 1961 of the civil code); (4) the incorporation of businesses (article 1`00 of the commercial code); (5) pledges of goods (article 1209 of the commercial code); and (6) insurance contracts (article 1046 of the commercial code). *See* Francisco Reyes Villamizar, *Electronic Commerce: Recent Developments in Colombia* 17 (Sept. 1999) (unpublished paper presented at the OAS conference on "Responding to the Legal Obstacles of Electronic Commerce in Latin America").

treaty obligations.[122] These express statements of limitation are beneficial in that they provide an absolute measure of certainty to parties considering whether to realize a transaction electronically.

Mexico's e-commerce legislation similarly provides for the electronic satisfaction of writing requirements, although the exact approaches taken by its commercial and civil codes differ. Mexico's commercial code, as reformed, expressly states that when contracts must be written, this requirement is satisfied by a data message which is attributable to the obligated person and accessible for subsequent reference.[123] This provision is consistent with MLEC principles insofar as both sources of law emphasize that for the purpose of writings, data messages remain accessible for subsequent reference. Mexico's writings provision exceeds the MLEC, however, by adding the element of "attributability." Given the fact that Mexico's commercial code has long taken a liberal, form-free view of documents and agreements, the impact of this provision is relatively minimal. As articles 78 and 79 establish, the validity of a commercial transaction depends neither on compliance with formalities nor on specific requirements,[124] except as required by other domestic or foreign laws.[125]

Mexico's civil code, in contrast, provides that when the law requires a writing, this requirement can be satisfied via electronic means (*medios electronicos*), provided such means are attributable to the obligated person and accessible for subsequent reference.[126] While essentially similar to the approach of the commercial code, Mexico's civil code uses the term "electronic means" in lieu of "data message." Notwithstanding the difference of language, this reform represents an important development relative to the large number of civil code contracts whose validity is premised on a writing. As a result of this legislation, Mexican judges will be better prepared to uphold the validity of civil contracts formed by electronic means.

Mexico's e-commerce reforms do not expressly identify which transactions fall outside its scope. Lacking the simple clarity and certainty associated with Colombia's approach to exclusions, parties interested in transacting electronically will be forced to consult, on a case

---

122. According to Professor Reyes, legal restrictions to e-commerce include public deeds, public registries, and negotiable instruments. *See* Grabb, *supra* note 88, at 123.

123. *See* CÓD.COM., *supra* note 103, art. 93.

124. *See id.* art. 78.

125. *See id.* art. 79. This broad approach is consistent with its obligations under the CISG. Exceptions to the foregoing include: (1) a factor's authority to incur obligations and (2) overland mercantile carrier contracts. *See id.* arts. 310, 581.

126. *See* C.C.D.F., *supra* note 102, art. 1834 bis. As was the case with Mexico's commercial code, this standard both satisfies and exceeds the standard set forth in the MLEC.

by case basis, with a local lawyer to determine whether their contemplated deal satisfies Mexican writing requirements, thereby adding to the general cost and complexity of doing business online.

Brazil's e-commerce legislation sharply departs from that of Colombia and Mexico by remaining silent on the subjects of writings and exclusions. To the extent that Brazil's civil and commercial codes generally advocate a free form of contracting, this silence is not detrimental to the growth of e-commerce. A writings recognition problem is presented, however, by the large number of commercial code statutes which either require a writing or otherwise indicate that the subject matter at issue can only be proved by a writing (effectively amounting to a writing requirement).[127]

The implications of this situation for e-commerce are negative. Absent express legislative guidance and authority, it will be hard for a Brazilian judge to find that electronically generated data messages are "writings." Concluding, in turn, that a contract does not observe the solemnities and formalities required by the commercial code, it then becomes impossible for that contract to form the object of any commercial action.[128] Lingering questions about the validity of electronically manifested documents and agreements will have the undesirable effect of being a drag on the development of e-commerce in Brazil and perpetuating the gap between cautious judges wielding old laws and the communications needs of modern business practices.

3. Signatures

a. General Standards

Article 7 of the MLEC establishes that a data message will satisfy signature requirements where: (1) a method is used to identify that person and indicate his or her approval, and (2) such method is reliable as appropriate for the purpose for which it was generated or communicated in light of all circumstances, including any relevant agreement.[129] Assuming the satisfaction of these standards, a data message is deemed to be the functional equivalent of a traditional, paper-based hand-written signature. The accompanying guide carefully points out, however, that the mere signing of a data message by means of an

127. Examples of Brazilian commercial code transactions that either expressly require or can only be proved by a writing are the *mandato* (article 140), *fiancas* (article 257), the *penhor mercantil* (article 271), the *deposito mercantil* (article 281), the formation of *sociedades comercais* (article 300), and the *contrato de fretamento* (article 566). *See* Código Comercial (C. Co.) (Braz.), arts. 140, 257, 271, 281, 300, 566.

128. *See id.* art. 124. This statute does not prevent a party from pursuing a civil action.

129. *See* MLEC, *supra* note 73, art. 7.

electronic signature does not automatically confer legal validity on the data message.[130] Moreover, as was the case with writings, the MLEC does not endeavor to override other reliability-geared requirements imposed by local law.

Significantly, neither the MLEC nor the accompanying guide offer specific guidance on what constitutes a reliable method of identifying an author and confirming that person's approval. The accompanying guide does, however, identify fourteen factors which enacting nations can consider in determining the appropriateness of the methods they adopt.[131] Within this broad-ranging and generally defined framework, enacting states are free to promulgate specific e-signature regulations.

Colombia's Law 527 follows the suggested approach of the MLEC regarding signatures almost exactly, establishing in article 7 the ability of a data message to satisfy legal signature requirements where: (1) a method is used to identify that person and indicate his or her approval, and (2) said method is reliable as appropriate for the purpose for which it was generated or communicated. Colombia breaks with the MLEC, however, by not including a provision which permits parties to independently reach agreements regarding signatures. This omission was likely designed to prevent the dilution or circumvention of Colombia's digital signature provisions.

Mexico's e-commerce legislation conforms to Colombia's Law 527 by expressly acknowledging that a data message[132] (or, in the case of the civil code, an electronic means)[133] can satisfy signature requirements, provided that the data message (or electronic means) is attributable to the

---

130. *See id.* ¶ 61.

131. *See id.* ¶ 58. In determining the appropriateness of the method used to assess the identification of parties and indication of approval, the MLEC sets out the following factors: (1) the sophistication of the equipment used by parties, (2) the nature of their trade activity, (3) the frequency with which transactions take place, (4) the kind and size of transactions, (5) the function of signature requirements, (6) the capability of communications systems, (7) compliance with authentication procedures set forth by an intermediary, (8) the range of authentication procedures made available by any intermediary, (9) compliance with trade custom and practice, (10) the existence of insurance coverage mechanisms against unauthorized messages, (11) the importance and value of information contained in the data message, (12) the availability of alternative methods of identifying and the cost of implementation, (13) the degree of acceptance of the method of identity in the relevant industry or field at the time it was created and communicated, and (14) any other relevant factor. *See id.* The UNCITRAL's Draft Uniform Rules on Electronic Signatures (DURES) incorporates many of these factors at the same time it further develops model electronic signature provisions. This set of model rules is expected to be finalized and presented to the Commission in Vienna by the summer of 2001. *See* UNCITRAL Working Group on Electronic Commerce, Draft Uniform Rules on Electronic Signatures, A/CN.9WG.IV/WP.84 (Dec. 8, 1999) [hereinafter DURES], *at* http://www.uncitral.org/english/sessions/wg_ec/wp-84.pdf (last visited Nov. 5, 2000) (on file with author).

132. *See* CÓD.COM., *supra* note 103, art. 93.

133. *See* C.C.D.F., *supra* note 102, art. 1834 bis.

person obligated and accessible for subsequent reference. While these qualifications are in line with MLEC standards regarding identity and approval,[134] Mexico's reforms depart from the MLEC's suggested approach by making reliability an express condition for satisfaction and by declining to recognize relevant inter-party agreements. With respect to the former issue, it may prove possible to imply a standard of reliability in the attributability and accessibility requirements. The Mexican legislature's absolute failure to develop these concepts does not help, however. This lack of guidance may ultimately result in considerable divergence both in terms of business practice and judicial interpretation, thereby diminishing the stability of Mexico's e-commerce framework.

Brazil's draft law, in contrast to both the MLEC and legislation from Colombia and Mexico, contains no express provision regarding the ability of a data message to satisfy signature requirements. This deficiency aside, however, it is abundantly clear that when utilized in accordance with regulations pertaining to party identity and approval, parties to e-commerce transactions can rely on electronic signatures.[135] Such regulations do depart from the suggested approach of the MLEC, however, by not making the acceptability of signatures expressly contingent on the use of a "reliable" method. As was the case with Mexico, it may nonetheless be possible to imply the satisfaction of the MLEC's reliability requirement from Brazil's promulgation of clear and detailed regulations with respect to digital signatures.

b. Electronic Signatures and Technological Neutrality

It is currently possible to "sign" electronically created data messages by a variety of methods.[136] For example, a sender can be identified by a name typed at the end of an e-mail, a digitalized image of a hand-written signature, a secret code or PIN,[137] a digital signature

134. That is, where the establishment of identity and approval is implied in the broadly stated, and unelaborated, notion of being "attributable to the person obligated." *See* CÓD.COM., *supra* note 103, art. 93; C.C.D.F., *supra* note 102, art. 1834 bis.

135. *See Projeto*, *supra* note 95, arts. 14-15.

136. "Electronic signature" is the generic, technologically neutral term that refers to the "universe of various methods by which one can sign an electronic record." *See* Smedinghoff & Bro, *supra* note 78, at 730.

137. These are examples of what is known as "private key" or "symmetric encryption." This type of encryption "relies on the same key (or stream of bits of a specified key length randomly created by a computer) to encrypt a message from plaintext into ciphertext, and to decrypt the ciphertext back into plain text again." *See* Gripman, *supra* note 22, at 775. Private key encryption is more limited than public key cryptography insofar as it (1) requires parties to share key information (thereby increasing the risk of key compromise) and (2) uses a more inefficient key distribution system (involving "snail mail" or face-to-face meetings). *Id.*

based on public key cryptography,[138] or a unique biometric identifier.[139] The diversity of methods, coupled with the likelihood of new methodologies based on future innovations, has led many scholars, practitioners, government actors, and the UNCITRAL to advocate the adoption of "technology neutral" electronic signature legislation which neither requires nor assumes a particular technology.[140] Through this means, legislatures can reduce the risk that new innovations will make older, technology specific legislation obsolete. To this end, legislation should not "preclude other methods of authentication that might also be appropriate, and thus inhibit the development of other technologies."[141]

Notwithstanding the broad support which exists for the adoption of technology neutral approaches to electronic signatures, emerging e-commerce legislation is characterized by a considerable divergence of approaches. According to one scholar, a quick survey of electronic signature legislation reveals that despite "agreement on where we ultimately want to go (facilitating e-commerce), there is little agreement on how to get there."[142] One state may broadly establish that all e-signatures satisfy legal signature requirements, while another narrowly legislates that only certain types of e-signatures are acceptable. Still other states may take an intermediate approach, establishing that only e-signatures possessing certain security attributes can satisfy legal signature requirements.[143] This diversity of approaches is manifest in the signature provisions of Mexico, Colombia, and Brazil's e-commerce legislation.

Mexico's e-commerce legislation accomplishes true technological neutrality by not setting forth elaborate regulations and guidelines in furtherance of one specific type of signature.[144] While this MLEC-

---

138. The term "digital signature" refers to one "technology specific type of electronic signature." Smedinghoff & Bro, *supra* note 78, at 730. As shall be discussed in greater detail, *infra*, a digital signature is a "sequence of bits . . . created by running an electronic message through a one way hash function to create a unique digest (or "fingerprint") of the message and then using public key encryption to encrypt the resulting message digest with the sender's private key." *Id.* at 731.

139. *See id.*

140. *See id.* at 761.

141. *Id.* Having said this, however, the authors note the possibility of creating legislation that simultaneously assures the principle of technological neutrality and addresses the "unique and legitimate legal issues" raised by technology specific authentication forms such as digital signatures (as well as their supporting public key infrastructures).

142. *Id.* at 727.

143. *See id.* at 738.

144. The closest Mexico's legislation comes to advocating a specific type of signature is article 90 of the Commercial Code which makes an indirect and vague reference to "keys" (*claves*) in the course of providing an example of a form of identification capable of supporting a

compatible approach is positive in that it creates maximum signature method flexibility at the same time it protects against legislative obsolescence, the lack of statutory guidance on the subject may leave parties uncertain as to the way a court will receive and value different types of electronically realized signatures. Such uncertainty could, in turn, make parties less willing to adopt electronic forms of doing business, thereby slowing the growth of e-commerce.

Given the tremendous level of legal uncertainty engendered by this approach, it is hard not to wonder whether the principle of technological neutrality has been used by Mexico as a pretext for not addressing tough issues raised by new technology. A review of the legislative history behind Mexico's e-commerce reforms reveals lobbying activity by groups with opposed interests (e.g., the *Associacion de Estandares Para el Comercio Electronico, AC*, the *Associacion Mexicana de la Industria de Tecnologia de Informacion, AC*, the *Associacion de Banqueros de Mexico, AC*, the *Associacion del Notoriado Mexicano*, and *Grupo EDI*). While one version did ultimately prevail, it is possible that insufficient legislative consensus precluded the promulgation of more detailed provisions.[145] Whatever the actual explanation, it is unlikely that e-commerce will reach its full potential in Mexico as long as parties continue to be exposed to the possibility of litigation over electronic signatures.

Colombia's Law 527 and Brazil's draft law, in contrast, address digital signatures to the exclusion of all other types of authentication. Irrespective of the neutral phrasing of article 7 of Colombia's Law 527,[146] only digital signatures which are unique to the user, susceptible of being verified, under the exclusive control of the user, linked to the information or message in such a way that subsequent changes invalidate the signature, and otherwise conform to regulations adopted by the national government are accorded the same force and effect as a manual signature.[147] In similar fashion, article 14 of Brazil's draft law establishes that only digitally signed electronic documents will be

---

presumption about the origin of a data message. *See* CÓD.COM., *supra* note 103, art. 90. Mexico's Civil Code contains no such provision.

145. The PRI's ongoing fall from power has provided opposition parties with an opportunity to play a more meaningful role in state and federal government. Because, after nearly seventy years of one party rule, Mexico's politicians are not accustomed to "building consensus," many legislative issues have been recently paralyzed in a political gridlock reminiscent of Washington, D.C.

146. Article 7 of Law 527 adopts the exact signature language of MLEC article 7. *See Law 527*, *supra* note 99, art. 7.

147. *See id.* art. 28. The promulgation of such clear guidelines regarding the establishment of a reliable method of realizing electronic signatures is wholly in line with the principles and factors set forth in the MLEC.

considered originals.[148] This article must be read in conjunction with article 15, which creates a presumption of truth regarding declarations contained within digitally signed electronic documents, provided that the digital signature is unique and exclusive to the signed document capable of being verified, generated under the exclusive control of the signatory, linked to the electronic document in such a way that any subsequent change invalidates the signature, and not generated after the expiration, revocation, or suspension of the keys.[149]

While these approaches provide parties to Colombian and Brazilian electronic transactions maximum certainty regarding the validity of their digital signatures, the technology-specific nature of these laws has the undesirable effect of foreclosing all electronic interaction based on simpler, yet still encountered, electronic signatures. This observation bears out Internet practitioners' criticism that technology specific statutes are problematic because they inhibit e-commerce.[150]

c. Digital Signatures, Public Key Cryptography, and Public Key Infrastructures

Colombia and Brazil's adoption of technology specific digital signature legislation is not surprising. According to Smedinghoff and Bro, the digital signature is the "one type of electronic signature that has generated the most business and technical efforts, as well as legislative responses."[151] To their credit, digital signatures based on the use of

148. *See Projeto*, *supra* note 95, art. 14. Although not an express and formal declaration regarding the exclusivity of digital signatures in Brazil, this article has the *de facto* effect of rendering nondigital signatures legally undesirable.

149. *See id.* art. 15. As is the case with Colombia, the enumeration of standards and guidelines with respect to the establishment of a reliable method of realizing electronic signatures is in line with the principles and factors of the MLEC.

150. *See id.*

151. Smedinghoff & Bro, *supra* note 78, at 731.

asymmetric or public key cryptography[152] can "contribute greatly" to transactional security on the Internet.[153]

The use of digital signatures alone, however, does not resolve all of the problems encountered by parties to e-transactions. Because of the Internet's open[154] architecture and highly scaleable communications protocols, e-mails and other communications can easily be intercepted by third parties such as hackers or outlaws, be made to appear as if they were sent by someone other than the true sender, or be misaddressed.[155]

---

152. Public key (also known as asymmetric) cryptography "employs an algorithm using two different but mathematically related cryptographic keys. One key is for creating a digital signature, or transforming data into a seemingly unintelligible form, and the other key is for verifying a digital signature or refining the message to its original form." *Id.* "The strength of a cryptographic key is measured by how hard it would be for an outsider to guess the key term from the ciphertext. The longer the mathematical key used, in general, the more secure the encryption system will be from attack by outsiders." *See* Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1198 (1998). One of the strongest and most broadly utilized public key systems is based on the RSA algorithm. One criticism of public key systems stems from the fact it is "more computationally intensive because of the complex mathematical algorithms necessary to produce asymmetric keys." *Id.* at 1200. As a result, public key cryptography is "not well-suited for encrypting large messages." *Id.* It is, however, well suited for smaller size messages. *See id.*

153. *See* Froomkin, *supra* note 78, at 49. In line with this thought, there is consensus that an encrypted data message and associated hash function-created message digest supported by a certificate-backed digital signature issued in accordance with strict PKI procedures provides sufficient authentication certainty.

This thought is echoed by the American Bar Association (ABA) Digital Signature Guidelines which note that given the appropriate legal and institutional infrastructure, "cryptographic technology can authenticate a message by assuredly linking it to an identified person and guarding the message integrity." *Digital Signature Guidelines*, A.B.A. SEC. SCIENCE & TECH. 19 (1996) [hereinafter *Guidelines*], *available at* www.abanet.org (last visited Apr. 8, 2001). The MLEC obliquely touches on this potential by noting the supplemental nature of electronic certificates intended to attest to the originality of a data message. *See* MLEC, *supra* note 73, ¶ 67.

154. The Internet is "open" because it: (1) "does not force users into closed groups or deny access to any sectors of society," (2) provides an "accessible environment for competing commercial and intellectual interests," and (3) remains open to changes associated with the introduction of new applications and services. *See* Winn, *supra* note 152, at 1190.

155. Anecdotes, statistical surveys, and reports regarding Internet security abound. A July 1997 "test of one computer system linked to the Internet by a security expert inadvertently revealed thousands of unprotected passwords." *Id.* at 1190. Around the same time, thousands of consumers who had made purchases from the NBA.com Web site "received anonymous e-mails reporting back to them the information they had transmitted to a supposedly secure Web site." *Id.* A 1996 survey of CIOs, in turn, revealed that fifty-four percent of the respondents "said that their company suffered a loss related to information security," and that figure jumps to seventy-eight percent when looses due to computer viruses are included. *Id.* at 1192 (citing Bob Violino, *The Security Facade*, INFO. WK., Oct. 21, 1996, at 36). Lastly, a report by the National Research Council warns that "much of this country's communications infrastructure is vulnerable to foreign and domestic hackers and saboteurs." *See* A. Michael Froomkin, *Encrypted Messages Ensure Privacy*, MIAMI HERALD, June 12, 1998, at 23A. At least one practitioner, however, takes a contrary position. According to Ian C. Ballon, concerns about the security of e-mails sent over the Internet are exaggerated. Ian C. Ballon, *E-Commerce and Internet Law: A Primer*, *in* 1 FOURTH ANNUAL INTERNET LAW INSTITUTE 9, 134 (Ian C. Ballon et al. eds., 2000). Ongoing

While public key cryptography can help establish a "secure line of communication" between a sender and "anyone . . . using a compatible decryption program," the technology guarantees nothing with respect to the identity of an actor in the material world.[156] As Professor Froomkin explains, "[T]here is no more reason to trust an e-mail message purporting to be from [person x] that says here is my public key than there is to trust any other e-mail message purporting to be from [person x]."[157] Touching on the same issue, another practitioner notes that "on the Internet, no one knows you're a dog."[158] If merchants are, consequently, insecure about their ability to verify the real world identities of the parties with whom they deal, they may likely be less willing to engage in online commerce.

The simplest way of resolving this problem is for parties to meet, face-to-face.[159] At such a meeting, parties could simultaneously exchange necessary key information and independently confirm identities. As well suited as this practice may be for trading partner agreements performed over proprietary networks, it is essentially incompatible with those transactional benefits uniquely associated with the Internet's open nature (e.g., increased exposure and access, expedited negotiations and ordering, and cost savings).

Absent a face-to-face meeting, the only realistic alternative currently available is to establish functional PKIs consisting of trusted third parties (e.g., a certifying authority, bank, and postal service, etc.) with the authority to issue certificates of identity. Assuming a trusted third party uses a reliable method to identify a subscriber and confirm the non-compromise of his or her private key for signing messages, then a party relying on the subscriber's public key "can have confidence that the signature is what it appears to be."[160] Internet practitioners note that digital signatures based on public key cryptography and that are supported by a properly functioning PKI can result in "extremely reliable" document certification.[161]

---

concerns regarding the security of communications carried over open networks has led the ABA to conclude that secure e-commerce increasingly depends upon securing the information itself, rather than relying upon the security of the channel. *See Guidelines*, *supra* note 153, at 19.

156. Froomkin, *supra* note 78, at 51.

157. *Id.*

158. Susan-Jacqueline Butler, *Panel IV: Certification, Authentication, and Electronic Signatures*, 17 ARIZ. J. INT'L & COMP. L. 149, 150 (2000).

159. *See* Winn, *supra* note 31.

160. *Id.*

161. *See* Gripman, *supra* note 22, at 771.

Notwithstanding significant growth in PKI deployment over the last two years,[162] the technology can, depending on the way it is implemented and regulated, have certain drawbacks. For example, critics point out the danger of promoting the adoption of "complex and risky technology by relatively unsophisticated parties before adequate safeguards have been established."[163] Others contend that many small-to-medium sized merchants and consumers lack the technological capability to implement and run security systems similar to those used by the military or sophisticated corporate entities.[164]

The other drawback experts commonly note involves PKI legislation which either under or over regulates Certifying Authorities (CAs) and certificates. Given the potentially broad impact of such imbalances on the growth of e-commerce, governments must guard against creating the legislative preconditions to their development.

Under-regulation occurs when a government declines to promulgate legislation in response to the introduction of new electronic communications and authentication technologies and procedures. Lacking a clear statement of duties, responsibilities, and standards, parties will neither know what steps to take in order to protect themselves nor will they be able to predict the outcome of a lawsuit. Without legal certainty of this type, moreover, companies with deep pockets that might have been interested in functioning as CAs will not take the risk.[165] The basic shortage of digital signatures and certificates that would result from the unwillingness of companies to enter the CA business might, in turn, produce stagnation in the e-commerce market.

---

162. In the United States, where large parts of the Internet are still subject to self-regulation, proprietary PKI systems are seen as the "most promising solution" to overcoming increased security risks encountered by commercial entities in an online business environment. *See* Diane E. Levine, *Public Key Infrastructure Adds Security to E-business*, INFO. WK., May 22, 2000, at 94. Using these systems, companies can give authorized outsiders access to resources and applications such as online payment systems, inventory data, or contract forms. *See id.* On a global level, a recent InformationWeek survey of 2700 executives, security professionals, and technology experts indicated that PKI use more than doubled from six percent to thirteen percent between 1998 and 1999. *See id.* PKI deployment rates are expected to keep rising due to the fact that Windows 2000 has built in PKI applications. *See id.*

163. Winn, *supra* note 152, at 1182.

164. *Id.* While conceding the "somewhat complex" nature of electronic document certification, other practitioners respond by noting that the software employed typically automates the whole process. *See* Gripman, *supra* note 22, at 784. This fact, taken together with the increased availability of training courses, undermines much of the argument that document certification using PKI is too complicated.

165. *See* Stewart A. Baker, *Law and the Net*, *at* http://www.stept. . ./International+ Development+Affecting+Digital+Signatures?OpenDocument (last visited Mar. 21, 2000) (on file with author).

An over-regulated approach to PKI, on the other hand, may inhibit e-commerce by producing legislative incompatibilities in terms of certificate requirements between jurisdictions and imposing "significant costs and operational constraints upon CAs and trading partners."[166] Legislation which creates elaborate financing, licensing, and technical requirements for CAs may drive up the cost of certificates to prohibitive levels at the same time it undermines established, cost-sensitive,[167] consensual trading systems.[168] The failure to provide a "savings clause" (exempting established trading partners from mandatory participation in elaborate public key infrastructures) can, moreover, threaten the operation of functional commercial arrangements premised on the use of cheap or closed-system certificates. Those parties which are able to manage the increased costs of certificates will do so, while those that cannot will be forced to either "find weaker, less regulated alternatives" or do without altogether.[169] The development of such a situation could be particularly detrimental to parties and/or protocols (e.g., the SET protocol for secure electronic payments) whose successful operations depend on the use of cheap or closed-system certificates. As one industry practitioner relates: "[B]urgeoning regulations that are not tailored to their private certificate systems will create disincentives for credit card companies to use digital signatures. In short, this outbreak of regulatory enthusiasm is likely to make digital signatures much rarer and riskier for prospective certificate authorities."[170]

Of the national legislation presently considered, Colombia's Law 527 lays out the clearest and most rigorous public key infrastructure. Article 29 of Law 527 broadly specifies that the functions of a CA can be fulfilled by public or private juridical persons of either natural or foreign origin. Significantly, CAs must meet minimum financial, technical, and background standards, in addition to obtaining a license from the *Superintendencia de Industria y Comercio* (SIC).[171] This governmental

166. Smedinghoff & Bro, *supra* note 78, at 753.

167. Cheap certificates can be used in "a lot of situations where even a no-liability signature is better than no signature at all." Baker, *supra* note 165. "Millions" of cheap, liability-free certificates are currently used in support of technologies such as SSL and "Active X." *Id.* Their broad disclaimers of liability make them unsuitable, however, for high value transactions. *See id.*

168. *See id.* Closed-systems certificates are those issued and utilized in connection with a preestablished trading or commercial agreement which promulgates relationship-specific rules regarding digital signatures, liability, etc. The SET protocol uses this type of certificate. *See id.*

169. *See id.*

170. *Id.*

171. *See Law 527*, *supra* note 99, art. 29.

organization, in turn, serves as the root certificate in the overall hierarchy of trust.[172]

Through this highly regulated approach, Colombia successfully establishes a PKI which offers maximum legal certainty and confidence to subscribers and relying parties.[173] Although Law 527 provides no express savings clause or exemption for parties with operations that depend on cheap or closed-system certificates, an alternative to expensive certificates may exist in the technological neutrality of article 7's signature provision. By specifically not referring to digital signatures using public key cryptography, the use of other types of electronic signatures can be reasonably inferred. On the basis of this interpretation, parties which seek to avoid the expensive certificates associated with a highly regulated PKI can do so.[174] Given the near absolute lack of "party autonomy" established by Law 527 in this connection, this clause is critical to the optimum development of e-commerce in Colombia.[175]

Brazil's approach to PKI is generally similar to Colombia's, although there are points of divergence with respect to legislative clarity. Pursuant to draft articles 24 and 25, Brazilian certifying authorities can either be public or private entities.[176] Departing from Colombia's approach, Brazil's draft law does not set forth an express requirement that certifying entities obtain a "license."[177] Notwithstanding this fact, however, Brazil's e-commerce legislation establishes that public certifying entities are not permitted to operate without having first secured a favorable technical opinion (*paracer tecnico*) from the *Ministerio da Ciencia e Tecnologia* (MCT).[178] This endorsement, in turn, is premised on the positive evaluation of a prospective certifying entity's knowledge of the technical conditions necessary to exercise the

---

172. *Id.* art. 41.

173. This is true provided the Colombian government controls its national territory and remains in power.

174. This alternative may be attractive considering that in addition to the inclusion of price-increasing PKI attributes, article 31 of Law 527 leaves local CAs free to set their own rates, thereby opening up the possibility of even higher service charges. *See Law 527*, *supra* note 99, art. 31.

175. Pursuant to article 4 of Law 527, parties are free to modify only the provisions of chapter III (the communication of data messages). By eliminating the right of parties to make relevant agreements regarding signatures, Colombia shuts down an important alternative means of avoiding expensive certificates. *Id.* art. 4.

176. *See Projeto*, *supra* note 95, arts. 24-25.

177. In what appears to be the product of unclear drafting, Brazil's proposed e-commerce legislation does specifically refer to a license for public certifying entities in its provision on administrative sanctions. *Id.* art. 41(v). As one isolated reference without a base context, however, it is impossible to state for a fact that Brazil's public certifying entities are subject to a licensing requirement.

178. *See id.* art. 37.

activity and plan for security.[179] The same ministry is charged with the responsibility of serving as a root certificate for public certifying entities. It is evident that even absent an express licensing requirement, public certifying entities are the subject of oversight. Subject to the criticisms discussed-*infra*, this fact may enhance the general public's perception of the trustworthiness of public certifying entities. Brazil's draft law additionally departs from Colombia's approach to PKI by not requiring CAs to meet certain financial standards. The lack of certainty with respect to a CA's financial condition may make certain subscribers less willing to put their faith in CAs.

Brazil's private certifying entities, in contrast, are under no equivalent type of regulation. This fact reflects the inferior legal quality of the certificates they issue relative to those of public certifying entities. As article 24 of Brazil's draft law states, the effects of services provided by private CAs are not to be confused with those associated with electronic certification services provided by notaries. The creation of classes of CAs authorized to issue certificates of disparate effect may result in an uneven development of Brazil's CA market.

Having established a system that expressly creates both a regulated, confidence-inspiring public CA and an unregulated, reduced-price private CA, Brazil's draft law reasonably balances the interrelated PKI considerations of legal certainty and transactional flexibility.[180] Equipped with legislation capable of accommodating the fullest possible range of transactional needs, Brazil is well positioned to reap the benefits of electronic commerce.

A potential criticism applicable to the legislation from both Colombia and Brazil is the establishment of governmental agencies as root CAs. Some commentators have suggested that the involvement of the government in a root CA capacity could hinder the establishment of a private CA marketplace. According to this view, such a development would be unfair to the extent that the doctrine of sovereign immunity put government CAs on a different liability footing than private sector CAs.[181] Proponents of government CAs respond to these arguments by pointing out the identification and binding efficiencies to be had by virtue of the government's special, preexisting relationship with all

179. *See id.* art. 38.

180. It accomplishes this, moreover, in a way consistent with the MLEC's principles and factors regarding electronic document certification.

181. Brad Biddle, *Public Key Infrastructures and Digital Signature Legislation: 10 Public Policy Questions*, *at* http://www.magnet.state.ma.us/itd/legal/biddle1 (last visited Jan. 15, 2000) (on file with author).

citizens.[182] It is too early to determine whether government involvement will have a positive or negative impact on the development of private CA markets in Colombia and Brazil.

Mexico's e-commerce legislation contrasts sharply with Colombia and Brazil's by declining to establish a PKI consisting of rules and standards to govern the interaction among CAs, subscribers, and relying parties. The adoption of this unregulated approach logically follows Mexico's decision to take a technologically neutral position on electronic signatures.

The upside to Mexico's approach is that by permitting parties to make their own rules and arrangements on the subject of signatures, a broader range of electronic transactions can be accommodated. Depending on their needs, subscribers can obtain either a custom-made, high inquiry, high cost certificate or a low inquiry, cheap certificate. Alternatively, Mexico's legislation is also capable of supporting transactional structures which use closed certificate systems (e.g., of the type used by the SET protocol).

The primary downside to Mexico's unregulated approach involves the uncertainty parties may experience as to the way courts, lacking both legislative guidance and/or understanding of the relevant technology, will interpret and rule on matters relating to the public key infrastructure. The adoption of such an approach is also problematic insofar as it provides little incentive for the subsequent development of any kind of PKI by either the public or private sector. Given the current state of Mexico's PKI legislation, answers to many basic e-contracting questions are unpredictable. For example, will Mexican courts make a legal distinction between electronic signatures generally and digital signatures backed by a CA issued certificate? Or, in the event a substantial CA practice were to emerge in Mexico, what duties would CAs have to subscribers and vice versa? It does not take a great degree of foresight to recognize the potential these issues have, individually and in combination, to diminish party confidence with respect to the realization of e-commerce in Mexico.

i. Reliable Methods of Establishing Identity

As noted, the major challenge confronting a system of public key cryptography-based digital signatures is the difficulty of assuring the identity of parties to the transaction and guarding against fraudulent misrepresentation. In a predominantly nonface-to-face business and communications environment, certificates issued by CAs in support of

182. *See id.*

digital signatures are only as reliable as the methods or procedures employed by the CA to corroborate the identity of a subscriber. Therefore, digital signature experts advocate that CAs have a valid method of inquiry capable of linking or "binding" subscribers and public keys.[183] As one scholar on the subject notes, "while a zero-inquiry certificate issued by 'Certificates-R-Us' is, in a sense, a real certificate, its attestational value is low."[184]

Responding to the interrelated considerations of attestational value and cost of service, some CAs offer certificates characterized by different grades of reliability, based on the quality and nature of the underlying identification inquiry. For example, Verisign, one of the top private sector certificate services in the United States, provides four certificate classes distinguishable both in terms of price and degree of inquiry.[185] These developments are fully compatible with MLEC article 7's provision that the acceptability of electronically created signatures be conditioned on the use of a reliable method of identifying the identity and approval of a signer.[186]

Irrespective of the fact that Brazil's draft legislation contains no equivalent to MLEC article 7, it does address the issue of binding with uncharacteristic clarity (at least with respect to public certifying entities). Representing an example of active regulation, draft article 25 specifies that a public certifying entity must certify the authenticity of public keys which, in turn, must be personally delivered by the duly identified subscriber.[187] Requests for certificates are similarly required to be made on paper, by a subscriber.[188] Assuming the proper implementation of these measures, parties that subsequently rely on certificates of identity issued by Brazil's public certifying entities can be reasonably confident about the identity of the individual or entity purporting to be the digital signer of a data message. Brazil's draft law does not, however, expressly distinguish between certificate classes. The nonexistence of qualitatively distinct classes of certificates does not preclude their future introduction.

No comparable standards or procedures are set forth with respect to the method by which a private Brazilian certifying entity binds subscribers and public keys. This fact further underscores the qualitative

---

183. *See* Gripman, *supra* note 22, at 779.

184. Froomkin, *supra* note 78, at 58.

185. Verisign Homepage, *at* http://www.verisign.com (last visited Mar. 22, 2000). Verisign offers its services in Brazil, too, under the name Certisign. It does not yet operate in Colombia or Mexico.

186. *See* MLEC, *supra* note 73, art. 7.

187. *See Projeto*, *supra* note 95, art. 25.

188. *See id.*

differences implicit in the certificates issued by Brazil's private and public certifying entities.

Colombia's legislation, on the other hand, identifies the basic issue, but declines to establish specific methodologies. Article 32 of Law 527 obligates CAs to elaborate "those rules that define the relationship with the subscriber and the form in which services are to be provided."[189] Additionally, article 35 requires that certificates issued by CAs indicate the methodology used by the CA to verify the subscriber's digital signature.[190] While these provisions generally identify the result that should be reached, they do not indicate how Colombian CAs will accomplish this objective (e.g., via a face-to-face meeting, or through the services of a notary). This failure to promulgate specific binding procedures may operate to reduce public confidence in certificates issued by Colombian CAs. As was the case with Brazil, Colombia's Law 527 neither creates classes of certificates with varying degrees of reliability nor proscribes their introduction.

Mexico's e-commerce legislation differs from that of Colombia, Brazil, and the MLEC in that it does not expressly link the acceptability of signatures to any notion of "reliability."[191] In keeping with this looser signature standard, Mexico's e-commerce reforms do not mandate exact methods by which the identity of subscribers can be bound with certainty to public keys.

Considered in the specific context of digital signatures based on public key cryptography, this approach may make Mexican CAs less inclined to undertake rigorous inquiries which at the same time leaving subscribers more willing to accept certificates of low attestational value. This result could facilitate an increase in identity-related fraud which might, in turn, diminish relying parties' confidence in the certificates supporting digitally signed electronic transactions.

ii. Reliable Methods of Establishing Approval

While a system of digital signatures backed by certificates premised on prior inquiry produces a reasonable degree of certainty regarding the identity of the sender and the integrity of the message, methods of establishing a party's approval are less forthcoming. The issue can become important in connection with a party's attempt to repudiate a

189. *Law 527*, *supra* note 99, art. 32.

190. *See id.*

191. *See* C.C.D.F., *supra* note 102, art. 1134; CÓD.COM., *supra* note 103, art. 93. These articles require that a signature be "attributable" to the person obligated. While an element of identity can be implied in this requirement, Mexico's legislation does not indicate the actual ways in which signatures are to be attributed.

transaction by claiming that he or she never actually approved (or possibly never sent) the underlying electronic communication or data message.

"Approval" may be inferred, to an extent, in the act of creating and transmitting a data message (i.e., where it is known that the identity of the creator and sender of a data message coincide). Outside of this possibility, there is no method for reliably establishing approval per se. Lacking guidance from the MLEC, parties may implement their own method utilizing any available technology. For example, a party to an electronic transaction may include in the overall set of data messages a "statement of approval" supported by a properly bound "transactional certificate."[192]

None of the legislation presently considered directly addresses the specific ways approval can be established. While article 7 of Colombia's Law 527 faithfully tracks MLEC article 7 on signatures (requiring the utilization of a method indicating approval of the contents of a data message), the law does not elaborate what the "method" should entail. This said, however, it may be possible to make a limited inference regarding approval via the requirement that digital signatures be under the exclusive control of those individuals that use them.[193]

Draft e-commerce legislation from Brazil differs from both the MLEC and Colombia's Law 527 in that it does not expressly condition the acceptability of data message-related signatures on the use of reliable methodologies. As was the case with article 28 of Colombia's e-commerce law, it may nonetheless be possible to infer a party's approval via draft article 15's requirement that digital signatures be generated under the exclusive control of the signer.[194]

Mexico's e-commerce legislation, like that of Colombia and Brazil, breaks from the MLEC by not expressly addressing the subject of party approval of data messages. Mexico's total lack of digital signature provisions, moreover, makes Colombian and Brazilian-type inferences impossible.

One possible solution to this shortcoming is to "read" approval into civil[195] and commercial code[196] requirements that signatures be

---

192. A transactional certificate can attest that "some fact or formality was witnessed by an observer." Froomkin, *supra* note 78, at 63. It has been suggested that the proposed "cybernotary" could issue such certificates. Theodore Sedgwick Barassi, *The Cybernotary: Public Key Registration & Certification of International Legal Transactions*, *at* http://www.abanet.org/scitech/ec/cn/cybernote.html (last visited Apr. 9, 2001).

193. *See Law 527*, *supra* note 99, art. 28.

194. *See Projeto*, *supra* note 95, art. 15.

195. *See* C.C.D.F., *supra* note 102, art. 1134.

196. *See* CÓD.COM., *supra* note 103, art. 93.

"attributable" to the person obligated. That is, a signer's approval would be implicit in the attribution of a signature. The inevitability of judicial interpretation which arises from the lack of legislative guidance on this point again underscores the uncertainty engendered by Mexico's adoption of a loose electronic signature standard.

iii. Other Methods of Establishing Reliability

Independent of the technological features and legal procedures that make digital signatures using public key cryptography reliable, certainty regarding a sender's identity and message integrity can be enhanced by presumptions regarding the attribution of data messages. Without assigning responsibility, MLEC article 13 sets forth provisions specifying when and under what circumstances a data message is that of an originator, deemed to be that of an originator, and when an addressee is entitled to regard a data message as being that of the originator.[197] This article is intended to help resolve questions as to whether a data message was really sent by the person indicated as being the originator.[198] Backed by the knowledge that the operation of presumptions can make it easier to enforce a transaction in court, should it become necessary, relying parties have more reason to be confident about engaging in online commercial activities.

Notwithstanding the positive role presumptions can play in assuring signer identity and message integrity, their use is opposed by those who think they might work to the detriment of certain e-commerce participants. In this view, the inadvertent acts of technologically unsophisticated consumers and small to medium sized businesses may result in key compromise and subsequent liability for transactions performed by unauthorized parties.[199] This is the so-called "grandma loses her key (or picks a bad password) and loses her house or life savings" argument.[200] Paragraphs 4 through 6 of MLEC article 13 afford parties a valuable measure of protection against this outcome by

197. *See* MLEC, *supra* note 73, art. 13. This article establishes that a data message is that of an originator if it was sent by an originator; a data message is deemed to be that of an originator if it was sent by a person with authority to act on behalf of the originator or an information system programmed by or on behalf of the originator to operate automatically; an addressee is entitled to regard a data message as that of an originator (and to act on that assumption) if the addressee properly applied a previously agreed upon procedure for ascertaining whether a data message was sent by the originator or, the data message resulted from the actions of a person whose relationship with the originator (or the originator's agent) enabled that person to gain access to a method used by the originator to identify data messages as its own.

198. *See id.* ¶ 83.

199. *See* Smedinghoff & Bro, *supra* note 78, at 752.

200. *See id.*

invalidating presumptions in connection with circumstances involving actual or constructive knowledge of timely notice, error, or duplicates.[201] These provisions do not, however, expressly contemplate a situation of fraud.

Articles 16 through 18 of Colombia's Law 527 contain most of the data message presumptions and entitlements found in MLEC article 13, although not in verbatim form.[202] One important deviation from the MLEC is Law 527's failure to foreclose the application of any presumption in a situation where the addressee both receives notice from the originator that a data message is not his or hers, and has a reasonable time to act accordingly. This omission is contrary to the best interests of technologically unsophisticated consumers and small merchants insofar as it deprives them of an important means of shielding themselves from liability for the unauthorized acts of others.

Mexico's presumption provisions are less extensive than Colombia's. Article 90 of the Commercial Code somewhat tracks article 13 of the MLEC by establishing, absent an agreement to the contrary, a presumption as to the originator of a data message, provided it was sent using a means of identification, such as keys or passwords (*contrasenas*), or by an information system programmed by, or on behalf of, the originator to operate automatically.[203] Beyond this partial concordance with the MLEC, however, Mexico's e-commerce reforms establish none of the other presumptions suggested by the MLEC. Nor does Mexico's legislation identify which specific circumstances, if any, operate to foreclose the use of attribution presumptions. Given the general lack of Mexican legislation dealing with the subject of electronic signatures, the components of this provision may be helpful to Mexican judges in their assessments of data message reliability. Lastly, it should be noted that the foregoing presumption discussion applies exclusively to transactions arising under Mexico's commercial code. Mexico's Civil Code, in comparison, is altogether silent on the subject.

Brazil, in contrast to Colombia and Mexico, has no provision on presumptions pertaining to the attribution of data messages. The detrimental consequences of this departure from the MLEC's suggested approach may nonetheless be mitigated to the extent that the detailed identification and binding regulations discussed *supra*, bespeak an advanced degree of reliability. The major shortcoming in this analysis, of course, is the fact that these regulations are only applicable to digital

201. *See* MLEC, *supra* note 73, art. 13(4)-(6).
202. *See Law 527*, *supra* note 98, art. 16-18.
203. *See* CÓD.COM., *supra* note 103, art. 90.

signatures based on public key cryptography. Accordingly, the reliability imputed to identifications made in conjunction with digitally signed data messages would not be available to data messages signed by non-digital means.

iv. The Issuance of Certificates of Identification

Having taken reasonable steps to assure subscriber identity, Brazilian and Colombian legislation provides for the issuance of certificates of identification by CAs. Although this step has no specific foundation in the MLEC, it does enhance the reliability of digital signatures in a way consistent with the general principles of MLEC article 7.[204] Through these certificates, relying parties can be reasonably certain that a public key downloaded[205] from a CA (or other repository) is actually associated with a specific subscriber. Moreover, assuming that the hash function associated with the message digest function in tandem, parties to an electronic transaction have strong grounds for believing that an original message has not been intercepted or altered in transmission.[206] Certificates issued in accordance with a properly managed public key infrastructure enhance parties' faith in the binding quality of an e-contract, strengthen a data message's probatory value, and discourage claims of repudiation.

Article 35 of Colombia's Law 527 mandates that the digitally signed certificates of authorized CAs contain: (1) the name, address, and domicile of the subscriber, (2) the identification of the subscriber named on the certificate, (3) the name, address, and place where the CA realizes its activities; (4) the public key of the user, (5) the methodology used to verify the digital signature of the subscriber found on a data message, (6) the number and series of the certificate, and (7) the date of issuance and expiration of the certificate.[207] Reviewing the date of issue and

---

204. UNCITRAL's DURES contains provisions that expressly address the issuance of certificates. *See* DURES, *supra* note 131.

205. The originator of the message could, alternatively, have attached his or her public key to the data message, thereby sparing the receiver the trouble of having to download same. *See* Gripman, *supra* note 22, at 778.

206. *See id.* at 779. According to Professor Froomkin, however, even verified certificates issued by reputable certifying entities are not "iron clad" proof of identity. Examples of situations which could give rise to the issuance of certificates based on fraudulent identity include the imprudent sharing of a subscriber's passphrase and the selection of a passphrase that is easily cracked. Froomkin, *supra* note 78, at 61.

207. *See Law 527*, *supra* note 99, art. 35. It is again pointed out that Colombia has yet to proscribe a method by which CAs can verify subscribers' digital signatures. One possible explanation of this fact is that the Colombian government intends to foster U.S. style self-regulation amongst CAs. Alternatively, the Colombian government may just be slow in drafting the necessary provisions.

expiration is one of several steps that can be taken by parties to guard against the risk of relying on outdated certificates.[208]

The digitally signed certificates issued by a Brazilian public certifying entity require more detail than Colombian certificates. In addition to presenting basic information about the date of issue and identification of the public key and user, Brazilian public certifying entities must also indicate the system of cryptography used and, in the case of a juridical person, the name of the party which solicits a certificate, as well as the holder's power of representation.[209] Absent a clause to the contrary, and, in contrast to Colombian practice, certificates are good for two years from the date of issuance.[210] Although requiring parties to renew certificates every two years may appear, at first glance, to be inefficient and costly, the aspect of regular review implicit in this requirement can help assure the up-to-date quality of Brazilian certificates. Furthermore, the greater degree of detail set forth in certificates issued by Brazil's public certifying entities enables relying parties to better assess the trustworthiness of digital signatures.

Encompassing, as it does, certificates pertaining to the authenticity of public keys, Brazil's draft article 26 does not appear to extend to private certifying entities. This observation stems from the fact that draft article 24 does not authorize private Brazilian certifying entities to work with public key cryptography.[211]

Mexico's e-commerce legislation departs from the regulated approaches of Colombia and Brazil by not setting forth any provision regarding certificate contents. Regardless of the technological neutrality of Mexico's e-commerce law, the government's current failure to provide guidance with respect to certificates may result in divergent judicial interpretations and a slower than necessary rate of e-commerce growth.[212]

---

208. *See* Froomkin, *supra* note 78, at 61.

209. *See Projeto*, *supra* note 95, art. 26.

210. *See id.* art. 26. In this age of instantaneous information and imperfect security, however, certificates that have been in use for up to two years may not be viewed as being sufficiently current. Relying parties may seek to reduce the risk of misplaced reliance by accepting only recently issued certificates. Professor Froomkin suggests these certificates can be issued in time intervals as precise as days, minutes, or even micro-seconds. *See* Froomkin, *supra* note 78, at 61.

211. *See Projeto*, *supra* note 95, art. 24.

212. In October 2000, SECOFI (an executive branch secretariat) entered into collaboration agreements with the National Association of Public Brokers and the National Association of Public Notaries to establish rules for the issuance and management of digital certificates capable of supporting commercial transactions. While these agreements are independent of the Mexican e-commerce legislation currently considered, it is apparent that Mexico's public brokers and notaries are positioning themselves to dominate, in conjunction with federal authorities, the certificate business. Said agreements were recently published in the National Official Gazette.

v. The Possibility of Other Certificates

The basic certificate associated with a digitally-signed data message is an identifying certificate. While this situation is expected to persist over the short term, CAs may eventually begin to certify attributes other than identity. For example, a CA may issue an "authorizing certificate" binding an individual with the authority or standing to engage in or commit an act that would otherwise have geographic, age, educational, or registration restrictions.[213] Such certificates could prove especially useful in overcoming obstacles associated with the establishment of party capacity in conjunction with the use of public key cryptography.[214]

Neither the MLEC nor the e-commerce legislation of Brazil, Mexico, and Colombia address this type of certificate. Seizing on its nonprohibition, one may be inclined to infer that to the extent it is not contrary to the law, the issuance of an authorizing certificate is permissible. Although intuitively compelling, this reasoning does not overcome the possibility of a formalistic Latin American judge declining to recognize (or otherwise give effect to) an "authorizing certificate" on the grounds that this instrument, besides being unknown to the judge, is not specifically provided for in local law.

Other certificates that may be encountered in the future are transactional and time stamp certificates. These are taken up in greater detail *infra*.

vi. Certificate Revocation Lists (CRLs)

The establishment and responsible maintenance of a CRL system simultaneously enhances the relying party's confidence and reduces the CA's liability exposure by listing public keys that have been revoked prior to their expiration date (if such a date is specified).[215] Possible reasons for wanting to revoke a validly issued certificate with a stated future expiration date include: (1) a breach or "compromise" in the confidentiality of a private key; (2) the death of a subscriber; (3) the closing of a business; and (4) the release of an employee whose authority to perform specific functions had been previously established by certificate (e.g., in the context of a trustworthy or closed trading agreement). By checking the CRL, a relying party will be alerted to

---

See Digital Certificates for Commercial Agreements, *at* http://www.bmck.com/elaw/current.asp?submitbtn+Show+Alert&area=calert (last visited Oct. 20, 2000).

213. *See* Froomkin, *supra* note 78, at 62.

214. *See* Winn, *supra* note 31.

215. *See* Gripman, *supra* note 22, at 782.

changes in the status of a certificate before detrimentally relying on the original status.

As is the case with other public key-related issues, the MLEC is silent on the topic of CRLs. The security and confidence enhancing functions they perform is, however, entirely consistent with MLEC article 7's emphasis on the reliability of the methodology used in connection with digital signatures.[216]

Brazil's legislation most clearly addresses the issue by mandating that the notary responsible for public electronic certificates maintain a publicly accessible, real-time, electronic information service which identifies revoked certificates.[217] No corresponding requirement is imposed on Brazil's private certifying entities.

Colombia's Law 527 appears to reach the same result, although the legislation's language is more ambiguous. Article 32(j) obligates Colombian CAs to maintain a "registry" of certificates, although it is not specified whether this means certificates issued, expired, revoked, or all of the above.[218] Article 37 adds to the confusion by setting forth the circumstances under which a subscriber must effect a revocation, without establishing any follow-up procedure regarding the notification of relying parties (e.g., via a CRL).[219] It appears that the Colombian legislature included the obligation of maintaining a registry with an intent to provide an electronic forum which relying parties could use to check the status of certificates issued by CAs. It is possible, however, that this provision will be interpreted as requiring nothing more than a registry of certificates issued, leaving parties with no indica of a certificate's reliability other than its stated date of expiration.

In line with its decision to forego detailed electronic signature regulations in the name of preserving technological neutrality, Mexico's e-commerce reforms contain no CRL requirements. The opportunity cost of this decision may be high insofar as relying parties which are unable to independently obtain real-time verification of the status of a certificate may be less willing to conduct business electronically with Mexican commercial entities.[220]

---

216. While a little late relative to the legislative activities of Brazil, Colombia, and Mexico, it should be noted that the pending final version of UNCITRAL's DURES contains a provision which permits a relying party to ascertain whether a signature device is valid and has not been compromised. *See* DURES, *supra* note 131.

217. *See Projeto*, *supra* note 95, art. 29.

218. *See Law 527*, *supra* note 99, art. 32(j).

219. *See id.* art. 37.

220. A Mexican business could avoid this problem by obtaining a certificate of identity from a CA that does maintain a CRL, notwithstanding the lack of legislative obligation. It is

vii. Cross-Jurisdictional Recognition of Certificates

To realize the maximum benefits of international electronic commerce, it is essential that certificates issued in support of digital signatures are capable of being recognized in foreign jurisdictions. Notwithstanding the MLEC's silence on the subject, a broad variety of approaches have already been adopted within the United States and abroad.[221] For example, a state may implement an "open" or "minimalist" cross-jurisdictional certificate recognition policy not focused on any specific technology or licensing requirements.[222] Alternatively, a state may adopt a highly restrictive approach, recognizing only those digital signatures backed by valid certificates issued by locally licensed certification authorities.[223] Reflecting this general diversity, the legislative approaches embraced by Colombia, Brazil, and Mexico demonstrate little, if any, uniformity.

Characterized as "reciprocal certifications," article 43 of Colombia's Law 527 establishes that certificates issued by foreign CAs may be recognized under the same terms and conditions demanded of national CAs, provided the foreign certificate is recognized by an authorized foreign CA whose issuance procedures are on par with Colombia's.[224] While not extreme in the sense of either of the possible approaches identified, *supra*, Colombia's policy may hinder international e-commerce to the extent that certificates relied on by commercial parties in nations with more liberal certificate issuance rules and procedures will not be accepted in Colombia.[225] The commercial effect of this limitation is compounded by the fact that the cross-jurisdictional certificate recognition provision of Law 527 applies exclusively to digital signatures. This disposition precludes recognition of certificates or other

---

possible that the collaboration agreements SECOFI has entered into with Mexico's broker and notary associations may ultimately result in guidance on this issue.

221. *See* Avellan, *supra* note 91, at 302. The UNCITRAL's pending DURES establishes that certificates issued by foreign certification services are recognized as legally equivalent to nationally issued certificates if the practices of the foreign certificate supplier provide a level of reliability at least equivalent to that required of national issuers under the law of the enacting state. In addition to tying recognition to those practices and standards set forth in the laws of the enacting state, the pending DURES notes that recognition may be made through a published determination of the state or through bilateral or multilateral agreements. The pending URES also identifies eight factors which states may take into consideration in assessing equivalence, and establishes the autonomy of parties to make their own agreements with respect to certificate recognition. *See* DURES, *supra* note 131.

222. *See id.* at 307. The state of Massachusetts has adopted such an approach.

223. *See id.* This approach has been followed by Hawaii and Mississippi.

224. *See Law 527*, *supra* note 99, art. 43.

225. This requirement will have a negative impact on United States-Colombian commerce insofar as U.S. certificates are largely left to the discretion of private sector CAs and subscribers.

indica of reliability associated with both contemporary and future nondigital signature methods.

Brazil's draft e-commerce law is similarly restrictive with respect to foreign certificates, although its specific requirements have little in common with Colombia's law. Under article 50 of Brazil's draft law, certificates issued by foreign CAs will have the same juridical value as those issued by a national certifying entity, provided that the nation of the foreign CA and Brazil are signatories to the same international accord relative to the judicial recognition of certificates.[226] The names of foreign CAs that meet this requirement will be published by the Ministry of Science of Technology.[227]

Irrespective of this article's clear expression of intent, its execution is problematic given the nonexistence of the referenced accord. This fact neutralizes the impact of Brazil's draft law, leaving parties uncertain as to the way foreign certificates will actually be received. Considering the lengthy periods of time usually required to draft, approve, and ratify treaties, it is unlikely this situation will be clarified in the immediate future.

The other shortcoming of Brazil's cross-jurisdictional certificate recognition policy involves draft article 50's nontechnological neutrality. Even though Brazil's draft law does not prohibit the use of nondigital signatures, article 50's exclusive application to digital signatures will, like Colombia's Law 527, not accommodate contemporary and future nondigital signatures alternatives. This internal inconsistency in the draft law may, in time, become an obstacle to international parties seeking to utilize nondigital signatures in Brazilian electronic commerce transactions.

Mexico's "open" and "minimalist"[228] approach to the subject of cross-jurisdictional recognition of certificates stands in sharp contrast to the approaches of Colombia and Brazil. Having not articulated a technology specific signature standard, Mexican e-commerce transactions should proceed without certificate-related obstacles. This approach may present a problem, however, for Mexican parties that wish to engage in electronic transactions with business partners in countries which impose reciprocal certificate standards on international

---

226. *See Projeto*, *supra* note 95, art. 50.

227. This approach is most likely inspired by the approach taken by California. *See* Avellan, *supra* note 91, at 306.

228. Mexico's e-commerce legislation is open and minimalist in the sense that it is silent as to recognition requirements for foreign certificates. Mexico's adoption of this approach may have been inspired, in part, by Massachusetts' policy regarding electronic records and signatures. *See id.* at 307.

transactions (e.g., Colombia). The existence of this legislative inconsistency in international electronic business practices poses a serious obstacle to the regional growth of e-commerce.

viii. CA and Subscriber Confidentiality Obligations and the Functionality of Authentication Systems Based on Public Key Cryptography

The proper functioning of authentication systems based on public key cryptography and digital signatures can be enhanced by the creation and maintenance of strict and clear standards of privacy between CAs and subscribers. That is, the protection of key privacy strengthens associated authentication procedures. Unlike the United States, where the federal government has generally permitted a policy of industry self-regulation,[229] most Latin American nations have elected, in varying degrees, to follow the continental European model and legislate on the subject.[230]

Different provisions of Colombia's Law 527 unambiguously obligate CAs to protect the confidentiality and use of information[231] and subscribers to maintain control of digital signatures.[232] Breaches of this duty by CAs can result in a fine, suspension of activities, or revocation of

---

229. Under this approach, a site may post a privacy policy stating which information is collected and how it is used (for example, information collected may be sold to companies specializing in "clickstream analysis"). Failure to observe a posted privacy policy is an offense actionable under the "Consumer Fraud and Abuse Act, as well as various common law and state consumer protection statutes." *See* Daniel Tynan, *Privacy 2000: In Web We Trust?*, PC WORLD, June 2000, at 112. In furtherance of self-regulation, independent nongovernmental organizations have been created to oversee privacy policies (e.g., Truste). Citing continued consumer concerns over the privacy of their information, the Clinton administration proposed legislation to protect financial, medical, and other personal data stored or collected online. *See* Abrea, *supra* note 38, at 65. As currently structured, consumers would be able to "opt in" or "opt out" of its protective scope. *See id.* It should be recognized that independent of the federal government's hands off approach to regulating privacy, some states have enacted their own standards. Moreover, some parties may be inclined to negotiate and incorporate terms of privacy and liability into their contracts and framework agreements, regardless of the law's requirements. *See* Froomkin, *supra* note 78, at 105.

230. This approach is more in keeping with that of the European Union, which issued a policy directive on the subject in 1998. *See* EUR. PARL. DEB. (Oct. 25, 1998). Commission Directive 95/46, 1995 J.O. (281) 31. Responding to these developments, the U.S. Department of Commerce created safe harbor principles which, if complied with, create a presumption as to the adequacy of privacy protections. Fledgling Latin American privacy provisions have not provoked a similar response from the United States. Independent of Latin American governments' tendencies to legislate on the issue, some private sector commercial entities in the region nonetheless publish privacy policies explaining what information is collected and disseminated. For example, see Patagon.com homepage, *at* http://www.patagon.com.br/all/disclaimer/disclaim.asp?DISCLE=1 (last visited Aug. 7, 2000).

231. *See Law 527*, *supra* note 99, art. 32(c).

232. *See id.* art. 39(3).

operating authority at the discretion of the *Superintendencia de Industria y Comercio*.[233] Subscribers, in turn, are made expressly responsible for noncompliance with their duties, although Law 527 does not specify the nature or extent of that responsibility.[234]

Brazil's draft law is significantly less clear on the issue of privacy. Neither public nor private certifying entities are expressly obligated to assure the confidentiality of information entrusted to them.[235] Although relieved of privacy-related responsibility, a Brazilian certifying entity may nonetheless be subject to administrative, civil, or criminal action for, respectively, failing to obtain the necessary operating authorization, negligence in revoking certificates, or falsification of certain electronic documents.[236] This attachment of legal consequences to the incompetent or fraudulent provision of services should inspire Brazilian CAs to do their job well, to the benefit of their clients. Brazilian subscribers, in contrast, are put under an express duty to adopt measures necessary to maintain the confidentiality of information.[237] The draft law does not, however, establish consequences for subscriber noncompliance.

All matters involving certifying entities and subscribers are heard by the Brazilian judicial power (*poder judicial*). Given the slow speed at which actions progress through Brazil's judicial system, it can be expected that Brazilian certifying entity-subscriber disputes will take longer to resolve than equivalent controversies in Colombia (which are brought before and resolved by an executive branch agency). This fact, when combined with the perception that Brazil's e-commerce law contains no incentive to respect party privacy, may have the undesirable effect of making parties less inclined to realize transactions involving the services of a CA.[238]

---

233. *See Law 527*, *supra* note 99, art. 42(1)-(5).

234. *See id.* art. 40.

235. Article 12 does, however, obligate intermediaries to maintain the secrecy of transmitted information. *See Projeto*, *supra* note 95, art. 12. While no definition (or other indication of the relationship, if any, between notaries and intermediaries) is provided, it would appear from the examples of the types of services provided by intermediaries (furnishing connections, the transmission of information, etc.) that notaries which issue public certificates are *not* intermediaries. This conclusion draws support from the fact that Brazil's draft law consistently and specifically refers to notaries using the Portuguese term—*tabeliao*—rather than the more general term of "intermediary."

236. *See id.* arts. 43-49. No provision of Brazil's draft e-commerce law addresses a private certifying entity's liability.

237. *See id.* art. 28.

238. Studies conducted in the United States, and applicable by analogy to Brazil, have found that consumer privacy concerns resulted in as much as US$2.8 billion in lost online sales in 1999. Another study estimates lost sales (due to privacy concerns) of US$18 billion by 2002, relative to a projected total of US$40 billion. Stephen Labaton, *White House and Agency Split on Internet Privacy*, N.Y. TIMES, May 23, 2000, at C1.

The draft version of Mexico's e-commerce legislation, focused as it was on digital signatures and public key infrastructure, directly addressed the interrelated issues of privacy, key compromise, and liability. The final legislative reforms diluted this certainty by eliminating the duty of confidentiality that had been imposed on CAs. Currently, Mexican e-commerce legislation obligates undefined "providers" (*provedores*) to uphold the confidentiality of consumer information obtained through electronic means.[239] While the change in focus evident in the terminology (CA to provider) is in line with the technologically neutral disposition of Mexico's legislative reforms, the overly broad nature of the term finally settled on may cause future confusion. Even assuming the term "provider" is intended to encompass CAs, the lack of immediate legislative clarity is a prelude to disagreement and litigation. In regards to subscribers, Mexico's e-commerce reforms contain neither an obligation of confidentiality nor key control. Lastly, unlike e-commerce legislation from Colombia and Brazil, Mexico's law is silent on the forum in which privacy-related disputes are to be resolved.

ix. Other Means of Enhancing the Functionality of Authentication Systems Based on Public Key Cryptography

Subscribers can further assure the privacy and security of their electronic transactions by establishing "trustworthy" computer operating systems. By instituting the "least privilege" principle, users are granted only the access to system resources necessary to accomplish assigned functions.[240] Through this means, information integrity is assured "at the time data enters the system, as well as while it resides on the system or is in transit within the system."[241] The creation and implementation of internal security systems has, in the United States, been left to the discretion of individual entities and professional associations (e.g., National Housing of Clearing Houses American National Standard Institute (NACHA) and (ANSI).[242] By not introducing specific legislation in this regard, Brazil, Mexico, and Colombia have opted for a self-regulatory approach similar to that of the United States.

---

239. *See Ley Federal de Proteccion al Consumidor*, D.O., Dec. 22, 1975. Violations of this duty can be sanctioned by a fine. *Id.* art. 128.

240. *See* Winn, *supra* note 152, at 1194.

241. *Id.*

242. *See id.*

d. Electronic Signatures and the Latin American Notary

In the course of ordinary, paper-based commerce, certain acts or contracts may be subject to additional formalities or solemnities. The realization of such enhancements can easily be accomplished by notary publics.[243] Numerous transactional circumstances necessitate the involvement of a *notario* (or equivalent) in Latin America. Noting a "tendency to authentication formalities," one regional scholar points out that "multiple statutes provide for a number of steps and solemnities that have to be accomplished in advance to the celebration of several acts and contracts."[244] Nonadherence to requisite formalities (for example, the performance of a certain act before a notary public) may result in the release of a party from an otherwise binding contract.[245]

As an electronic, Internet-based model of commerce slowly eclipses the traditional, paper-based model, the interrelationship between electronic signatures and notarizations has become an increasingly important issue. To date, the degree to which an electronic signature provides the additional layers of reliability, traceability, and inalterability inherent in an "authenticated" or notarized legal act is unclear. The MLEC offers little guidance on the subject, noting clearly that its focus is on the relationship between originators and addressees, and not that between either the originator or the addressee and any "intermediary" or provider of "value-added" services.[246] To this disclaimer the MLEC suggests "it might be desirable to develop functional equivalents for the various types and levels of signature requirements in existence."[247] Reflecting this general lack of agreement and guidance, the nations of

---

243. Civil law notaries are legal professionals:

> whose practice derives from the Roman Germanic notarial tradition. Notaries are duly-appointed officers, whose public office it is to draw up, attest to, or certify deeds and other documents, including conveyances of real and personal property, and powers of attorney . . ., to certify transactions relating to negotiable instruments, to incorporate, modify and dissolve . . . companies, to prepare wills or other testamentary documents; to draft protests and other formal papers relating to . . . ships and . . . the carriage of cargo.

See Notarial Procedures for Digital ID Requests, *at* http://www.verisign.com/repository/notaryfaq.html (last visited Mar. 14, 2000). Acts or documents which have been notarized are accorded a superior evidentiary quality by courts. Unlike the United States, almost all nations of Latin America require notaries to be lawyers by way of primary training.

244. Reyes, *supra* note 121, at 15.

245. *See id.* at 25.

246. *See* MLEC, *supra* note 73, ¶ 39. Value-added services may be performed by network operators and/ or intermediaries, and include receiving, formatting, transmitting, translating, recording, authenticating, certifying, and preserving data messages. The pending DURES does not expressly address the issue of the interrelationship between electronic signatures and notarizations. *See supra* note 131.

247. *Id.* ¶ 55.

Latin America are developing divergent perspectives on the issue of the interrelationship between electronic signatures and notarizations.

No provision of Colombia's Law 527 expressly states that properly executed digital signatures are an acceptable substitute for traditional, face-to-face, paper-based notarizations. Rather, Law 527 indiscriminately provides that any party meeting the requirements to be a CA can emit certificates in support of digital signatures.[248]

Pointing to the absence of contrary statutory language and the open-ended nature of CA eligibility, some Colombian lawyers advocate that "it is foreseeable that CAs will substitute the notarial function in the near future."[249] Under this view, digital signatures executed in accordance with the appropriate technology and procedures can provide a *greater* degree of accuracy and reliability than paper-based notarizations.[250] According to a leading authority on the subject, online notarizations of electronic documents can have the same degree of trustworthiness enjoyed by traditional notarizations, provided steps are taken to ensure the security and integrity of the electronic documents.[251] The use of transactional certificates, attesting that "some fact or formality was witnessed by the observer," could provide additional assurances of trustworthiness.[252]

By placing data messages that are digitally signed in accordance with the procedures of a strict PKI on par with traditional notarizations, the inefficiencies associated with having to obtain a notarized public deed in for certain transactions could be eliminated. This outcome would be good for business because it would drive down transaction costs and expedite Latin America's transition from formalistic, paper-based methods of doing business to electronic commerce without jeopardizing security. Keying in on the progressive implications of this view, Colombian scholar Reyes notes that "Law 527 offers an

248. *See Law 527*, *supra* note 99, art. 30(1).

249. Reyes, *supra* note 121, at 43.

250. *See* Gripman, *supra* note 22, at 782.

251. *See id.* at 773.

252. Froomkin, *supra* note 78, at 63. As previously discussed, this is but one type of certificate that CAs can issue. In the context of the United States, transactional certificates could be issued by members of the recently proposed cybernotary profession. As presently conceived by the ABA, cybernotaries would be quasi-public officials with the technical and legal expertise required to realize both a traditional and electronic notarial practice. *See* Barassi, *supra* note 192. This idea is similar to Florida's International Notary which, by law, must be a lawyer with five years of experience and appointed by the Secretary of State. Said notaries are only authorized to issue authentication instruments for use in non-U.S. jurisdictions. *See, e.g.*, FLA. STAT. ch. 118 (1999). It is hoped that the involvement of an internationally experienced legal professional in the authentication process will make U.S.-generated documents more readily acceptable to foreign jurisdictions, thereby reducing the need for lawyer opinion letters.

unparalleled opportunity to challenge old-fashioned constructions related to the law of contracts."[253]

This forward-looking interpretation has not been unanimously accepted in Colombia. In October 1999, the *Colegio de Colombiano de Abogados Notarios* filed an public action of unconstitutionality (*accion publica de inconstitucionalidad)* against Law 527 in Colombia's Constitutional Court. The Colombian notary association's principal claim is that in permitting entities distinct from notaries to emit certificates regarding the veracity of digital signatures, Law 527 directly infringes article 131 of the Colombian Constitution.[254]

Several responses to this challenge can be made in support of Law 527. First, to the extent that Colombian CAs do not actually provide "public faith,"[255] there is no conflict with the public service provided by traditional notaries. Second, notwithstanding constitutional article 131's recognition of the public service provided by notaries (and registrars), it does not state that the function of certifying the veracity of signatures belongs exclusively to notaries.[256] Finally, the fact that different consequences attach to services performed by CAs and notaries underscores their professional and functional distinctiveness. For example, where CAs can suspend or revoke certificates already issued, civil notaries are not permitted to withdraw or take back notarizations. On the basis of the foregoing points, the Colombian notary associations claim appears weak.

The outcome of this matter is being closely watched by parties with business interests in Colombia.[257] Should the Constitutional Court con-

---

253. Reyes, *supra* note 121, at 43.

254. Article 131 of the Colombian Constitution establishes that the rendering of public faith is a public service which corresponds to notaries. *See Constitucion Politica de Colombia*, Gaceta Num. 114, July 7, 1991.

255. It should be realized that unlike civil law notaries, Colombian CAs are not required to be commissioned public officials. *See* John C. Anderson & Michael L. Closen, *Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority*, 17 J. MARSHALL J. COMPUTER & INFO. L. 833, 858 (1999). Moreover, where a civil law notary must receive and service all interested parties, a CA may select for whom he or she is willing to work. *See id.* Lastly, the fact that CAs are responsible to their clients (and not the situation, as is the case for a notary) underscores the argument that the functions of a CA are not to be confused with the rendition of public faith. *See id.*

256. Providing further support for the second argument is the interpretational principle of Colombian law which establishes that acts not expressly prohibited by law are presumed to be valid.

257. This process is also being watched by notary groups outside of Colombia, many of which have a strong interest in preserving their professional "monopoly." Notary groups are maneuvering to ensure their future involvement in the authentication and attestation business. Typical of this are the *Union Internacional del Notoriado Latino*, the *Colegio de Escribanos de la Capital Federal* (Argentina), and the *Associacion Nacional del Notariado Mexicano*. The *Colegio de Escribanos* emphasizes activities developed by CAs coinciding with the functions and infrastructure of the Latin notary. *See* Mauricio Devoto, *Claves para el Exito de Una*

clude that the CA provisions of Law 527 do violate constitutional article 131, significant portions of Colombia's e-commerce regulations would be subject to revision. The suspension of either the entire law (or parts thereof) would eradicate the sense of certainty and predictability Law 527 has instilled in merchants and judges with respect to electronic commerce. Internet-related developmental activity would slow pending the legislation's revision. This process may, itself, become dragged out as special interest groups enter the Colombian legislative arena seeking to implement their version of e-commerce regulation. Considered on another level, moreover, success on the part of Colombia's notaries may embolden notarial groups which have not previously challenged the e-commerce legislation in their own nations, thereby slowing or interrupting the advance of e-commerce in other parts of the region.

Brazil's draft e-commerce legislation similarly fails to clarify the nature of the interrelationship between digitally signed, certificate backed data messages and traditional paper-based notarizations. Brazil avoids the Colombian problem described *supra*, however, by expressly establishing various classes of CAs whose certificates have distinct legal values (the most reliable of which is that issued by a notary). By taking this approach, Brazil simultaneously keeps the CA profession open to a diverse set of potential service providers, assures security and flexibility to subscribers and relying parties, and preempts the raising of Colombian-style challenges by Brazil's notarial profession in connection with Law No. 8935 of 18 November 1994 and article 236 of the Brazilian Constitution.[258]

Infrastructura de Firma Digital: La Importancia de la Intervencion Notarial en la Solicitud del Certificado de Clave Publica, *at* http://www.colegio-escribanos.org.ar/Clves.htm (last visited Mar. 6, 2000) (on file with author). In Mexico, as noted above, notaries and brokers have entered into an agreement with SECOFI which would permit them to control the future issuances of certificates supporting digital signatures. Similarly, the President of the United States noted the transferability of traditional pen and ink notarial functions to the arena of digital signatures and electronic documents. Milton G. Valera, *New Technology and a Global Economy Demand That American Notaries Better Prepare for the Future: Upgrading the Current Common Law System May Mean Establishing a New Class of Cyber Professional*, 32 J. MARSHALL L. REV. 935, 957 (1999).

258. *Lei No. 8.935, de 18 de novembro de 1994*. Article 3 delegates the right to exercise the notarial function and give public faith to a class of professionally accredited "officials." Notwithstanding the way in which Brazil's draft law effectively preserves their power, it is possible Brazil's notaries may challenge the grant of authority to private (non-notary) certifying entities to issue certificates on the ground that private CAs are performing a notarial function without the requisite notarial training. *See* C.F., de 5 de outubro de 1988, art. 236. This is unlikely, however, given the substantial difference between the certificates issued by these two groups in terms of reliability and admissibility. Even if a demand for cheap certificates or closed trading systems were to develop in Brazil, it would be hard to foresee the minimum inquiry, and subsequently less acceptable, certificates issued by private certifying entities posing a threat to the more regulated and judicially recognized certificates of notary CAs.

Mexico's e-commerce legislation specifically provides for the participation of notaries in electronic transactions. This approach breaks from that of Brazil and Colombia in that it does not envision a role for nonnotaries in the authentication process. Article 93 of the Commercial Code[259] and article 1834. of the Civil Code[260] establish that when a judicial act must be authorized in an instrument before a notary public, the parties can, without having a face-to-face meeting, express the exact terms of their mutual obligations to the notary by way of a data message. These articles represent a significant departure from Mexico's draft e-commerce law which contained elaborate electronic signature and PKI provisions (including CAs), and nothing about notaries. This radical shift was most likely attributable to the successful pre-vote lobbying campaign Mexico's notarial and broker associations ran in order to preserve the security of their monopolistic and lucrative profession. Consistent with the aforementioned lack of provisions pertaining to electronic signatures, certificates, and public key infrastructure, Mexico's final e-commerce legislation does not take up the issue of the interchangeability between data messages created in accordance with appropriate levels of security and traditional notarizations.

III. CONCLUSION

A. Observations

The future of Latin America's economic and commercial development is inextricably linked to the Internet and electronic commerce. Over the last five years, demographic, technological, commercial, political, and cultural forces have coalesced to create an explosive electronic market, the potential value of which is estimated to be billions of dollars. Properly managed, the realization of electronic transactions over the Internet can increase revenue, efficiency, and productivity in a way that benefits governments, merchants, consumers, and the environment.

Latin America's future e-commerce development will be a function of its ability to innovate and implement smarter Internet business strategies, provide an adequate technological and physical infrastructure, and establish a legislative framework characterized by consistency, security, and fairness. The elements composing this developmental formula are particular to the region, having little in common with those encountered in markets with higher PC penetration rates, larger amounts

259. CÓD.COM., *supra* note 103, art. 93.
260. C.C.D.F., *supra* note 102, art. 1834 bis.

of disposable income, advanced education levels, more extensive credit availability, and better developed infrastructures. For this reason, great care should be taken to forego the inclination to view and understand Latin American Internet issues through the filter of United States, European, and Asian experience.

While piecemeal technological, infrastructure, and regulatory advances have been made since the commercial advent of the Internet, the nations of Latin America have not yet succeeded in establishing a foundation capable of supporting the region's extraordinary growth projections. The cost of continued failure in this regard is high. The inability of parties to harness online resources for the purpose of becoming more competitive and efficient constitutes a wasted commercial opportunity for Latin American merchants and consumers alike. Moreover, the existence of unpredictable technology, delivery, and legal infrastructures present an unattractive risk factors while driving up transactional costs. These facts preclude the rapid development of lucrative and sophisticated e-commerce practices in Latin America.

B. Recommendations

If Latin America is to realize its substantial e-commerce potential, its public and private sectors must make improvements on the following fronts:

1. Implement Smarter Internet Strategies

Many Latin American corporations and individuals currently underuse available Internet resources by not expanding beyond simple marketing and internal communications activities. This tendency may reflect users' general lack of technological training and expertise.[261] Going forward, Latin American corporations and individuals need to shift away from practices which underutilize the Internet's potential and focus on the development of true electronic B2B and B2C models of doing business. In this connection, emphasis should be placed on the widespread introduction and use of intranets, extranets, trustworthy operating environments, payment processing systems, and trading partner arrangements. Governments, institutions, commercial entities, and universities can help merchants and consumers obtain the knowledge

261. In contrast to U.S. experience, much of Latin America has yet to see the emergence of a hybrid class of business-technology managers capable of implementing and overseeing sophisticated applications, networks, and interfaces. *See* Charles H. Davis, *The Emergence of Electronic Commerce in Spanish-Speaking Latin America*, Apr. 1999, *at* http://www.lexmercatoria.org (last visited Feb. 22, 2000) (on file with author).

necessary to maximize their e-commerce potential by increasing the number of specialized training and technology-oriented degree programs.[262]

2. Address Infrastructure Limitations

Notwithstanding numerous improvements in the Latin America telecommunications sector over the last ten years, e-commerce-related services and products can still be prohibitively expensive and unreliable. More importantly, the region must guard against a near term capacity problem. While existing networks are able to handle today's volume of Internet traffic, it is uncertain whether they will be able to accommodate an exponentially expanding base of users.[263] The successful implementation of fiber optic networks, broadband services, and network access points throughout the region will be crucial to overcoming future congestion related problems. The realization of these developments depends on the continued openness of the region's telecommunications markets to foreign investors and competition.

Another significant infrastructure issue involves the generalized absence of harmonized technological standards. At this early stage in the evolution of e-commerce, companies are rushing to introduce products and services with the hope of becoming market leaders. Because these companies often do not coordinate any overriding strategy with respect to design specifications in advance, the resulting hardware and software is frequently characterized by low levels of inter-operability. Examples of ways in which this phenomenon touches e-commerce include the existence of incompatible protocols for the processing of electronic payments (SET and SSL), corporate data exchange software (SAP, Oracle, Peoplesoft), security and encryption programs, as well as, computer operating environments, lines, and bandwidths. Left un-

---

262. Although there have not, to date, been a large number of programs dedicated to e-commerce in the region, this is quickly changing. For example, Mexico's *Tecnolgico de Monterrey* recently inaugurated a Masters program in e-commerce. Similarly, the ITAM just announced the creation of an eight-month course in the business and technology of e-commerce. *See* Quinones, *supra* note 19, at 32. Other programs have been put together in Brazil, Argentina, and the other nations of Latin America. An example from the corporate realm is Oracle, which provides ongoing training for regional users of its technology. *See Oracle Education Training Methods Seminar*, *at* http://www.skylab.us.oracle.com/seminars/lacountries.html (last visited Aug. 21, 2000) (on file with author). It may also be desirable to provide judges with a training course introducing them to the basics of the Internet and e-commerce so that they may, in turn, better understand the technologies and procedures involved in controversies.

263. Consider, for example, the fifteen-fold increase in Internet traffic that is estimated to have occurred between 1995 and 2000. *See* Neil Gross & Irma Sagor, *Yellow Flags for E-Commerce*, BUS. WK., June 22, 1998, at 166, *available at* http://www.businessweek.com/1998/25/b3583030.htm last visited Jan. 24, 2000).

addressed, disharmonious technological standards could be an impediment to the future growth of e-commerce. To avoid this outcome, international standard-setting initiatives should be encouraged. Standards subsequently agreed upon should be written in a technologically neutral way, thereby assuring the accommodation of future innovations.

Lastly, as is the case with traditional, paper-based commerce, the primitive state of Latin America's physical delivery infrastructure is a bar to the optimum development of e-commerce. To derive the maximum benefits associated with e-commerce, regional delivery practices must be made more reliable and secure. The recent opening of the delivery services market to foreign service providers, coupled with the formation of new local services and improved tracking capabilities (for example, using GPS and handheld wireless computing devices), suggests that Latin America will ultimately succeed in removing this *de facto* trade barrier.

3. Create a Harmonized Legislative Framework

The MLEC was designed to help enacting states draft legislation capable of overcoming domestic legislative obstacles to the introduction and growth of electronic business and communication practices. Its success in this regard is evident in the ever increasing number of nations with new or pending MLEC inspired e-commerce legislation. Notwithstanding the generally positive nature of this development, little emphasis has been placed on harmonizing key aspects of national and international initiatives. Invariably, nations have deviated from the MLEC's suggested provisions, electing instead to draft laws more precisely attuned to national circumstances and/or interests. Such deviation is exacerbated by the MLEC's silence on specific subjects (e.g., security and PKI). The end result, exemplified by recent and forthcoming legislation from Brazil, Colombia, and Mexico, has been the spawning of a widely divergent set of approaches to the regulation of e-commerce. To the extent that inconsistent and conflicting provisions present a new barrier to the growth of e-commerce, the MLEC may have created more problems than it solved.

The most effective way of overcoming this derivative barrier is to create and enact a uniform convention on electronic commerce, either at the supranational or regional level. It has been suggested that the terms of the MLEC be incorporated into a convention.[264] While this would be a step in the right direction regarding fundamental contracting issues

264. *See* Boss, *supra* note 78, at 1954.

(i.e., writing, signature, originality) the large number of security issues not addressed by the MLEC renders the suggestion inadequate.

A better solution would be to create a new convention covering basic contract formation and validity issues, in addition to security standards, options, and procedures.[265] Assuming the DURES meets with the same broad ranging acceptance as its predecessor, the MLEC, said proposed convention could be a hybrid of each model law.

Core formation provisions would, in a uniform and minimalist manner, establish scope of application and interpretation provisions which are international in orientation. Additionally, the principle of nondiscrimination with respect to the recognition of data messages as writings, technologically neutral recognition of electronic signatures, the absolute right of parties to make their own agreements regarding data messages and electronic signatures,[266] and clear original and data message retention provisions should also be adopted.

These fundamental contract terms would be supported by uniform security and authentication provisions.[267] Technical, background, and financial qualifications, along with the duties and liabilities applicable to an authenticating entity, should be clearly identified and standardized. Binding procedures should be promulgated for discrete levels of identification inquiry. Certificate issuance, content, and lifespan terms should be harmonized for each type of certificate (i.e., identity, transactional, authorizing, etc.).[268] A publicly accessible, real-time CRL should be created and maintained for the benefit of relying parties around the world. Uniform cross-jurisdictional certificate recognition standards should be established, thereby eliminating the obstacle to international e-

---

265. This idea has been widely advocated. The White House GII has called consistently for the development of an "international uniform commercial code" that can facilitate e-commerce. *See A Framework for Global Electronic Commerce, Executive Summary, at* http://www.whitehouse.gov/WH/New/Commerce/Summary.html (last visited Jan. 24, 2000). Similarly, the European Union has proposed an "international charter." *See Rapid Expansion of Internet Commerce To Be Subject of WTO Report in March*, 15 INT'L TRADE REP., 313 (Feb. 25, 1998); *see also* Randy V. Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed First Step Toward Signing on the Dotted Line*, 46 AM. U. L. REV. 511, 513 (1996); Sanu K. Thomas, *The Protection and Promotion of E-Commerce: Should There Be a Global Regulatory Scheme for Digital Signatures*, 22 FORDHAM INT'L L.J. 1002, 1022 (1999). The drafters of such a convention could look to the miscellaneous e-commerce related agreements, directives, guidelines, rules, and models that have been promulgated by supragovernmental, governmental, and nongovernmental bodies such as the UNCITRAL, WTO, OECD, UPU, EU, ICC, and ISO. *See* Ivascanu, *supra* note 70, at 225.

266. The flexibility associated with party autonomy is crucial to trading agreements structured around cheap or closed-system certificates.

267. Care should be taken to draft these provisions, as connected as they are with digital signatures, in a way that assures technological neutrality.

268. These certificates need not have the same expiration date.

commerce posed by today's variable practices. In this regard, it would be beneficial to establish a root CA which is acceptable either on a global or regional basis.[269] Subscriber duties and liability should be unambiguously set forth. Lastly, the interrelationship between notaries, CAs and certificates should be clarified. As is the case with binding procedures, any provision adopted should assure party freedom of choice with respect to the issuer of certificates.

The creation and execution of an international convention with harmonized e-commerce provisions would sharply curtail the current tendency toward divergent legislation at the national level. While such a convention should, minimally, encompass the aforementioned issues, it could also address more specialized (but equally important) issues such as the protection of intellectual property, the automation of customs procedures, the collection of taxes, consumer protection, and Alternate Dispute Resolution (ADR).[270] Regardless of the scope ultimately adopted, the drafters of such a convention should strike an appropriate balance between heavy-handed over-regulation and the promulgation of predictable terms that inspire the confidence and trust necessary for the growth of e-commerce. The introduction of a harmonized regulatory framework would benefit the growth of e-business practices by overcoming the legislative inconsistencies spawned by the disharmonious adoption of the MLEC's different provisions and provide the textual foundation for the formation of a unified body of e-commerce jurisprudence.

269. At the global level, the UN or UPU might serve as a root CA. Regionally, the task could be performed by a body such as the EU, OAS, FTAA, etc.

270. These considerations could, alternatively, be incorporated into separate conventions or treaties. This outcome may be desirable insofar as it would expedite the multilateral consensus building and drafting process.

APPENDIX: KEY E-COMMERCE PROVISIONS FROM BRAZIL, COLOMBIA, AND MEXICO

Issue	SPHERE OF APPLICATION
MLEC	Data messages in the context of commercial activities (accompanying guide notes scope of MLEC can be extended to cover uses outside commercial sphere).
Brazil	No express equivalent.
Colombia	Applicable to all types of information in data message form, regardless of commercial or civil character.
Mexico	Mexico's federal civil code and commercial code, inter alia, were reformed to accommodate e-commerce, although not in exactly the same way.

Issue	INTERPRETATION
MLEC	With regard to the MLEC's international origin, the need to promote uniformity, and the observance of good faith. Questions not expressly settled by the terms of the MLEC are to be settled in conformity with the general principles on which the MLEC is based.
Brazil	Tracks MLEC provisions in all regards, save its use of the language "the dynamic progress of technological instruments" in place of the MLEC's "the need to promote uniformity."
Colombia	Tracks MLEC provisions exactly.
Mexico	No express clause included in package of legislative reforms. There are however, pre-existing interpretational provisions in both the civil and commercial code. Mexico's civil code mandates interpretations in accordance with the usage and customs of different countries, the general principles of contract law, and the stipulations of parties. The commercial code mandates interpretations in accordance with the common customs of merchants. Moreover, because Mexico is a party to the CISG, interpretations are to have a regard for a transaction's international origin, as well as the need to promote uniformity and good faith.

Issue	LEGAL RECOGNITION OF DATA MESSAGES
MLEC	The "non-discrimination" principle establishes that information shall not be denied legal effect, validity, or enforceability solely on the grounds that is in the form of a data message.
Brazil	No express equivalent.
Colombia	Tracks MLEC provisions in all regards, save its use of the language "all information" in place of the MLEC's "information."
Mexico	No express equivalent.

Issue	WRITINGS
MLEC	Invoking the "functional equivalent" approach, data messages can satisfy writing requirements where the information contained is accessible so as to be usable for subsequent reference.
Brazil	No express equivalent.
Colombia	Tracks MLEC provisions exactly.
Mexico	Data messages can satisfy commercial code writing requirements, provided the data message is attributable to the obligated person and available for subsequent reference. In contrast, "electronic means" can satisfy civil code writing requirements, provided said means are

	attributable to the obligated person and accessible for subsequent reference.

Issue	IDENTIFICATION OF EXCLUSIONS
MLEC	None directly identified in body of MLEC. The accompanying guide, however, notes several situations which enacting states may leave outside the scope of domestic e-commerce legislation including, for example, consumer protection laws and international treaty obligations.
Brazil	No express indication provided.
Colombia	Consumer protection laws and international treaty obligations.
Mexico	No express indication provided.

Issue	SIGNATURES
MLEC	Data messages can satisfy signature requirements where (1) a method is used to identify a person and indicate his or her approval, and (2) the method is as reliable as appropriate for the purpose for which the data message was generated or communicated, in light of all circumstances, including any relevant agreement. No specific method advocated, but fourteen factors to take into consideration are provided.
Brazil	No express equivalent. Notwithstanding this shortcoming, it is abundantly clear that where utilized in accordance with regulations pertaining to identity, approval, and security, electronically generated signatures will be accepted in Brazilian courts.
Colombia	Tracks MLEC provisions in all regards, save its elimination of the clause affirmatively recognizing relevant inter-party agreements.
Mexico	Data messages can satisfy commercial code signature requirements, provided the data message is attributable to the obligated person and available for subsequent reference. In contrast, "electronic means" can satisfy civil code signature requirements, provided said means are attributable to the obligated person and accessible for subsequent reference.

Issue	TECHNOLOGICAL NEUTRALITY OF ELECTRONIC SIGNATURES
MLEC	No express provision, but accompanying guide advocates this approach.
Brazil	Ostensibly so, insofar as no provision expressly mandates the exclusive use of signatures based on one specific technology. This said, however, only digitally signed documents will be considered originals. Moreover, a presumption of truth in relation to a signer will apply to declarations contained within digitally signed documents, provided that the digital signature is (1) unique and exclusive to the signed document, (2) capable of being verified, (3) generated under the exclusive control of the signatory, (4) linked to the electronic document in such a way that any subsequent change invalidates the signature, and (5) and not generated after the expiration, revocation, or suspension of a key.
Colombia	Ostensibly so, insofar as its signature provision does not make any technology based distinction. This said, however, only digital signatures which are (1) unique to the user, (2) susceptible of being verified, (3) under the exclusive control of the user, (4) linked to the information or message in such a way that subsequent changes invalidate the signature, and (5) otherwise conform to regulations adopted by the national government are accorded the same force and effect as a manual signature.
Mexico	Accomplishes true technological neutrality by declining to set forth regulations regarding one specific type of electronic signature.

Issue	THE CREATION OF PUBLIC KEY INFRASTRUCTURES
MLEC	No express provision, but contemplated in the reliability factors contained in the accompanying guide.
Brazil	Creates a system of public CAs which must obtain a favorable technical endorsement (*parecer tecnico*) prior to commencing operations. A government agency serves as the root certificate. Private CAs are also created, but not made subject to any regulation or oversight.
Colombia	Creates a system of public or private CAs which must meet minimum financial, technical, and background standards in order to become licensed. A government agency serves as the root certificate.
Mexico	No equivalent provision.

Issue	"BINDING" IDENTITY
MLEC	Outside of articulating the general standard, no specific guidance is provided with respect to its realization.
Brazil	Subscriber requests for certificates must be made on paper. Moreover, in order to certify the authenticity of a subscriber's public key, the duly identified holder of the signature device must first appear personally before the public CA. Only when these requirements are satisfied will a certificate be issued. No equivalent regulations are set forth with respect to private CAs.
Colombia	Colombian CAs are required to elaborate the rules that define their relationship with subscribers and the form in which services are to be provided. They must also indicate the methodology used to verify a subscriber's digital signature. No provision addresses the specific way these requirements are to be satisfied.
Mexico	No equivalent provision.

Issue	PRESUMPTIONS REGARDING THE ATTRIBUTION OF DATA MESSAGES
MLEC	Sets out a series of circumstances in which a data message is that of an originator, is deemed to be that of an originator, or is entitled to be regarded as that of an originator. Also identifies circumstances which foreclose the application of presumptions (timely notice of denial, error, duplicates).
Brazil	No equivalent provisions.
Colombia	Tracks MLEC provisions in all regards, save for its elimination of the provision which forecloses the application of presumptions where an addressee receives notice from the originator that a data message is not from the originator and the addressee has reasonable time to act accordingly.
Mexico	Establishes a commercial code presumption with respect to the originator of a data message where the data message was sent (1) using a means of identification, such as keys or passwords, or (2) by an information system programmed by, or on behalf of, the originator to operate automatically. While these two clauses come directly from the MLEC, Mexico's e-commerce legislation declines to include the great majority of the Model Law's other presumption and entitlement related provisions. Similarly, Mexico's reforms do not address those situations which foreclose the applications of presumptions. Last, no civil code reforms touch on the subject of presumptions.

Issue	THE ISSUANCE OF CERTIFICATE OF IDENTIFICATION
MLEC	No express provision, but accompanying guide generally advocates their use.
Brazil	Certificates issued by public certifying entities in support of the

	authenticity of public keys must contain, at a minimum, (1) the identification of the notary's digital signature, (2) the date of the certificate's issuance, (3) the identification of the public key of a holder in the event the certificate is not directly appended, (4) elements that permit the identification of the cryptographic system utilized, and (5) the name of the holder that solicits a certificate, as well as the holder's power of representation, where holder is a juridical person. No guidance is provided with respect to private certifying entities.
Colombia	Certificates must contain (1) the name, address, and domicile of the subscriber, (2) the identification of the subscriber named on the certificate, (3) the name of the CA as well as the address and place of where the CA realizes its activities, (4) the public key of the user, (5) the methodology used to verify the digital signature of the subscriber, (6) the series number of the certificate, and (7) the date of issuance and expiration of the certificate.
Mexico	No equivalent provisions.

Issue	LIFESPAN OF CERTIFICATES
MLEC	Not addressed.
Brazil	Two years from date of issuance, unless otherwise noted.
Colombia	No limit specified.
Mexico	No equivalent provisions.

Issue	ISSUANCE OF OTHER CERTIFICATES ("AUTHORIZING CERTIFICATES")
MLEC	No express provision to this effect. Not contrary to the general principles and factors of the Model Law.
Brazil	Neither created nor prohibited.
Colombia	Neither created nor prohibited.
Mexico	Neither created nor prohibited.

Issue	CERTIFICATE REVOCATION LISTS (CRL)
MLEC	No express provision to this effect. Consistent with the MLEC's emphasis on use of reliable methods in connection with digital signatures.
Brazil	Public certifying entities must maintain a publicly accessible, real–time, electronic information service which identifies revoked certificates. No guidance is provided with respect to private CAs.
Colombia	CAs are required to maintain a registry of certificates, without specifying whether this means certificates issued, revoked, or both.
Mexico	No equivalent provisions.

Issue	CROSS-JURISDICTIONAL RECOGNITION OF CERTIFICATES
MLEC	No express provision to this effect. Consistent with the MLEC to the extent that the harmonized use of such certificates can facilitate international commerce.
Brazil	Certificates issued by foreign CAs will have the same juridical value as those issued by a national certifying entity, provided that the nation of the foreign CA and Brazil are subject to the same international accord relative to the judicial recognition of certificates.
Colombia	Certificates issued by foreign CAs may be recognized under the same terms and conditions demanded of national CAs, provided that the foreign certificate is recognized by an authorized foreign CA whose issuance procedures are on par with Colombia's.
Mexico	No equivalent provisions.

Issue	THE INTERRELATIONSHIP BETWEEN ELECTRONIC SIGNATURES AND THE LATIN AMERICAN NOTARY
MLEC	No express provision. The accompanying guide clearly notes that the Model Law's focus is on the relationship between originators and addressees, and does not concern issues pertaining to intermediaries. The accompanying guide also notes the desirability of developing functional equivalents for the various types and levels of signature requirements.
Brazil	No provision expressly states that properly executed digital signatures are an acceptable substitute for traditional, face-to-face, paper-based notarizations. While the certification profession is technically open to all, only certificates issued in accordance with heightened standards, including the involvement of a notary, will be recognized as an original in a court of law.
Colombia	No provision expressly states that properly executed digital signatures are an acceptable substitute for traditional, face-to-face, paper-based notarizations. Any party (for example, a notary, a chamber of commerce, individual, etc.) meeting promulgated standards to be a CA can issue certificates in support of digital signatures.
Mexico	No provision expressly states that properly executed digital signatures are an acceptable substitute for traditional, face-to-face, paper-based notarizations. While Mexico's legislation does not create a CA profession characterized by relatively open access, both the commercial and civil code establish that when a judicial act must be authorized in an instrument before a notary, parties may express the exact terms of their mutual obligations to a notary via electronic means (civil code) or data messages (commercial code).

Issue	CA AND SUBSCRIBER PRIVACY OBLIGATIONS AND LIABILITY
MLEC	Beyond the scope of the MLEC. The concept is, however, generally consistent with the MLEC's underlying goal of facilitating electronic commerce in that it bolsters CA certainty and subscriber/relying party confidence.
Brazil	Neither public nor private certifying entities are expressly obligated to assure the privacy of the information entrusted to them. Brazilian subscribers have an express duty to adopt those measures necessary to maintain the privacy and confidentiality of information, although the consequences of noncompliance are not specified. All controversies are to be resolved by the judicial power.
Colombia	CAs are obligated to protect the confidentiality and use of information. Breaches of this duty can result in fine, suspension of activity, or revocation of operating authority at the discretion of executive branch agency. Subscribers are obligated to maintain control of their digital signatures. Subscribers are responsible for noncompliance, although no specific consequences are identified. All cases and controversies involving privacy and liability are to be resolved by the *Superintendencia de Industria y Comercio*.
Mexico	Mexico's federal consumer protection law mandates that "providers" uphold the confidentiality of consumer information obtained through electronic means. While no clarification of the term "provider" is set forth, it is conceivable that CAs and intermediaries would qualify. The law imposes no corresponding duty on subscribers, nor does it identify which branch of government is responsible for receiving and adjudicating privacy related disputes.