FEDERAL RESERVE BANK *of* NEW YORK *Serving the Second District and the Nation*

1998 International ACH Conference

Global Electronic Commerce - The Next Century

Seattle, Washington
March 9, 1998

Ernest T. Patrikis
First Vice President
Federal Reserve Bank of New York

I am very pleased to be here today to discuss global electronic commerce. At the Federal Reserve Bank of New York, we have a tradition of embracing emerging technologies as a means of fostering the growth of commerce. As early as 1914 the Federal Reserve System was using the telegraph to wire funds across the nation. By 1918, the Federal Reserve Banks had introduced their first dedicated funds transfer network. Today, over 350,000 funds transfers are sent over Fedwire every day with a total value of more than $1.1 trillion.

So, electronic commerce itself is not new. What is new is the emerging global network environment and its electronic access capabilities. The promise of this global network has brought electronic commerce to the forefront of public-policy making. The Organization for Economic Cooperation and Development and other international organizations have expressed their belief that "the exponential growth and diffusion of the Internet is quickly making the promise of widespread electronic commerce a reality. High-speed, interconnected global networks like the Internet provide new ways to conduct commercial transactions, generate new markets and revenue streams, lower transactional costs, and forge new relationships between businesses and consumers."

Nowadays, it is impossible to speak about the potential explosion of the Internet and electronic commerce without a discussion of the appropriate role of Government in fostering and regulating electronic commerce. In the United States, the question of the Government's role in global electronic commerce was answered when, in July 1997, the White House released its "Framework for Global Electronic Commerce" white paper. The Framework is the clearest and most comprehensive articulation of the United States Government's view of its role in the creation of the global information infrastructure as a vibrant international market place. The overriding theme of the Framework was summed up in a statement made by President Clinton upon the release of the report. He said that:

Governments can have a profound effect on the growth of electronic commerce. By their actions, they can facilitate trade or inhibit it. Government officials should respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining feature of the new digital marketplace. They should adopt a market-oriented approach to electronic commerce that facilitates the emergence of a global, transparent, and predictable legal environment to support business and commerce.

To ensure that the acts of the United States Government comport with this view, the Framework sets forth five principles intended to inform the Government's actions in this area. The first principle is that the private sector should be allowed to take the lead. Although the Government played a significant role in financing the initial research and development of the Internet, the White House believes that its subsequent expansion has been, and should continue to be, driven primarily by the private sector. The Framework takes as a fundamental principle the notion that innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena. The natural outgrowth of this first principle is seen in the Federal Government's hesitance to issue any regulations governing the use of the Internet and its encouragement of private sector self-regulation.

The second principle in the Framework is really a corollary to the first principle and provides that the Government should avoid undue restrictions on global electronic commerce. This principle is based on the belief that unnecessary regulation of commercial activities on the Internet will distort the development of the electronic marketplace by raising the cost of products and services for consumers the world over.

According to the third Framework principle, where Government involvement is needed, its aim should be to support and enforce a predictable, minimalistic, consistent, and simple legal environment for commerce. This legal environment should be based on a commercial law model that allows for private governance though decentralized, contractual relationships or organized system rules, rather than a top-down regulation model. Moreover, the basic goal of any Government regulation should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution.

The fourth principle directs the Government to recognize the unique qualities of the Internet in relation to existing regulatory models. We should not assume, for example, that the regulatory frameworks established over the past sixty years for telecommunications, radio, and television apply to the Internet. The Framework specifically directs the Government to review, and revise or eliminate existing laws and regulations that may hinder electronic commerce to reflect the needs of the new electronic age.

Finally, in the fifth principle, the Framework announces what, to many, is the most important principle in connection with electronic commerce and the Internet, namely that electronic commerce over the Internet should be facilitated on a global basis. In this regard, the United States Government has identified nine areas where international agreements are needed to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will largely shape the marketplace. The nine areas are: (1) customs and taxation; (2) electronic payments; (3) a Uniform Commercial Code for Electronic Commerce; (4) intellectual property protection; (5) privacy; (6) security; (7) telecommunications infrastructure and information technology; (8) content; and (9) technical standards. These nine areas are discussed in some detail in the Framework. I would like to spend the rest of my time discussing two of these issues in more detail -- specifically, electronic payments and a Uniform Commercial Code on Electronic Commerce.

My interest in these areas reflects my belief that advancements in each are essential to the continued growth of electronic commerce over the Internet both domestically and globally. Users of electronic commerce need safe and reliable payments systems linked to the Internet to facilitate payment for goods and services contracted for over the Internet. More fundamentally, contractual relationships forged over the Internet must have some basis in a sound legal and technological infrastructure.

Electronic Payments

Over the past few years we have seen the emergence of new technology which allows individuals to pay for goods and services over the Internet and over private networks. These payment methods have developed along two lines. First, technology exists that allows individuals to make payments over the Internet and private networks using traditional payment mechanisms such as credit cards. When used in this way, the Internet is simply the next in an evolving line of communications media used to convey payment information. The underlying payment is governed by the same laws that would govern credit card payments at a point-of-sale terminal or over the telephone. Moreover, and perhaps more importantly from a central banker's perspective, these Internet payment methods remain tied to existing payments systems involving the transfer of balances among accounts at financial institutions.

"Electronic money," based on stored-value smart cards and other technologies is also under development. When used in connection with these products, the Internet no longer act solely as an access device to communicate payment information to merchants and banks. Instead, the transfer of "value" over the Internet will become, for all practical purposes, the modern day equivalent of tendering currency in satisfaction of a debt. While private electronic money will not have "legal tender" status, electronic money issuers will use private contractual relationships to effect discharge of their obligations.

"Electronic money" is essentially the reemergence in the United States of privately-issued currency, the value of which depends on the financial health of the issuer. Because electronic value is simply a promise of the issuer to pay on demand, the question arises as to whether the issuance of electronic value should be limited to banks and other supervised institutions. In the United States, banks have been intricately linked to the payments system and, as a result, are subject to unique regulatory burdens such as reserve requirements, deposit insurance premiums, and extensive supervision. Some argue that the safety and soundness of the payments system require limiting the issuance of electronic money to banks. In fact, some foreign jurisdictions, such as Japan and the European Union, have limited the issuance of electronic currency to banks or credit institutions in EU parlance.

Unlike Europe and Japan, however, the United States is, at least for the time being, remaining silent on the issue of nonbank issuance of electronic money. The White House believes that the commercial and technological environment is changing far too rapidly for it to be able to develop policy that is both timely and appropriate. In the near term, therefore, the White House is calling for case-by-case monitoring of electronic payments experiments.

In keeping with the spirit of the White House Framework, Federal bank supervisors in the United States have expressed a clear willingness to listen to what the private sector has to say on issues involving emerging electronic payments. For example, in 1996 the Board of Governors issued proposed regulations concerning the applicability of Regulation E to stored-value cards. As part of that proposed rule making, the Board requested comments from the public as to whether part or all of Regulation E should apply to electronic money or value residing on a computer system or personal-computer hard drive. Similarly, the FDIC requested public comment on the application of Federal deposit-insurance coverage to electronic value represented on computer systems. This openness, combined with an increasing willingness to let the banking industry partner with technology and other industries, reflects a commitment on the part of bank supervisors in the United States to allow the private sector to direct the future of electronic commerce and payments.

From a longer term perspective, however, the market place and industry self-regulation alone may not fully address all of the issues associated with e-money. The White House Framework suggests that Government action may be necessary to ensure the safety and soundness of electronic payments systems, to protect consumers or to respond to important law-enforcement objectives. Of course, the White House would work closely with the private sector to inform policy development and ensure that governmental activities flexibly accommodate the needs of the emerging market place.

From a central bank perspective, one of the most fundamental questions raised by electronic payments is its impact on monetary policy, especially if its development is as widespread as some have predicted. In the near term, it appears that Internet payments systems will not significantly impact monetary policy. For the most part, the Internet and other communication networks are currently being used to facilitate existing banking transactions using traditional banking settlement channels. Most payments over the Internet simply result in the movement of funds from a bank account in one institution to one in the same or another bank. This should have few, if any, implications on the conduct of United States monetary policy or the measurement of the United States money supply. "Money" as defined by M1, M2, or M3, would still be held in accounts at banks and would be reported to the Federal Reserve through existing reporting mechanisms.

If, however, Internet payments evolve to the point where digital "coins" or other private electronic money begin to be widely used and circulated like Federal Reserve bank notes, the potential implications for monetary policy could be much greater. The effect that stored value, whether smart card or computer based, has on monetary policy will in large part turn on the extent to which it shifts the money supply out of the banking sector. When stored value is issued by banks, this is not a real risk. As Governor Edward Kelly noted in a 1996 speech before a cyber-payments conference, bank liabilities incurred through issuing stored-value cards should be included in the statistical reports that banks must currently submit to the Federal Reserve Board.

In addition to monetary policy concerns, other factors could trigger the need for the Government to resolve the issue of bank versus nonbank issuance of electronic value. For example, as I noted earlier, banks are subject to extensive regulation and supervision at least in part to ensure the safety and soundness of the payments systems. If nonbanks begin to take significant market share away from banks because of an inherently lower cost structure, that raises serious questions about a level playing field and whether banks can ever fairly compete. If nonbanks begin offering through the Internet many of the payment services, or alternatives to the payment services, now offered exclusively by banks, it raises a real question about the ultimate value of a bank charter, and what it really means to be a bank. It could be argued, for example, that there is no such thing as a nonbank issuer of e-money -- but only supervised bank issuers and unsupervised bank issuers.

Another related concern is the emergence of nonbank Internet financial firms that have balance sheets closely resembling that of banks, but do not have access to the lender-of-last resort. What happens if these institutions have a liquidity crisis? What if that crisis is so large that it threatens to gridlock the entire payments system? What role do the supervisors play? What role should the supervisors play?

In addition to these domestic policy concerns, the Administration's position on electronic payments will be informed by international developments. A number of international organizations in which the Federal Reserve plays a role, such as the Bank for International Settlements and the G-10 central bank governors, have already completed important studies on aspects of electronic banking and payments. For example, a multi-national task force on the Security of Electronic Money was established by the Committee on Payment and Settlement Systems, and the Group of Computer Experts, of the G-10 central bank governors. This task force, which was chaired by Israel Sendrovic of the Federal Reserve Bank of New York, issued a report on its findings entitled "Security of Electronic Money" in August 1996. The Task Force examined primarily consumer-oriented stored-value products by surveying the leading global suppliers of both card-based and software-based stored-value systems. The report concluded that the technology security measures of these systems are being designed to achieve an adequate level of security relative to other forms of common retail payments, assuming that they are implemented appropriately.

What remains to be seen is whether the infrastructure needed to create binding electronic contracts between previously unaffiliated parties can be developed to meet the needs of consumers and merchants globally. This leads me to my second topic -- the establishment of a Uniform Commercial Code for Electronic Commerce.

Uniform Commercial Code For Electronic Commerce

The White House Framework states that, in order "to encourage electronic commerce, the United States Government should support the development of both a domestic and global commercial legal framework that recognizes, facilitates and enforces electronic transactions worldwide." In keeping with its belief that the private sector should take the lead in electronic commerce issues, the White House is largely relying on the efforts of the National Conference of Commissioners of Uniform State Laws and the American Law Institute, the sponsors of the Uniform Commercial Code, to produce the desired domestic commercial law framework. Internationally, the United States Government is working with organizations such as the United Nations Commission on International Trade Law, the OECD, UNIDROIT and the International Chamber of Commerce to achieve the necessary global commercial law framework.

The United States has adopted, and has urged others to adopt, the following drafting principles. First, parties should be free to order the contractual relations between themselves as they see fit. Second, rules should be technology neutral -- in other words, the rules should neither

require nor assume a particular technology -- and should be forward looking -- should not hinder the use or development of technologies in the future. Third, existing rules should be modified and new rules should be adopted only as necessary or substantially desirable to support the use of electronic technologies. Finally, any drafting process should involve the high-tech commercial sector as well as businesses that have not yet moved on-line.

Unlike the situation in the retail electronic payments area, where there has been significant private-sector resistance to developing legal standards, there is an increasing consensus, both domestically and abroad, that electronic commerce will not flourish until there are laws addressing the validity of electronic contracts and the legal significance of attribution procedures used by parties to determine the identity of the sender of an electronic message.

Domestic Efforts

Domestic efforts to address these needs have proceeded under two very different venues. First, there is the work of the NCCUSL and the ALI to modernize the UCC to reflect the realities of the Internet. In the absence of Federal legislation or regulation, the NCCUSL/ALI drafting process is attractive for at least two reasons. First, the general approach of the UCC is consistent with the views of many in the emerging electronic commerce community in that it allows for variation through private contract. Second, NCCUSL/ALI has been extremely successful in ensuring that commercial law is essentially the same in substance among the fifty states. This success largely results from the care that NCCUSL takes in establishing drafting committees that reflect diverse interests affected by the particular legislation being considered.

With respect to electronic commerce, NCCUSL and the ALI have established a drafting committee that will recommend changes to the general definition provisions of the UCC located in Article 1. The drafting committee=s mandate is broad: consider and draft revisions and additions to Article 1 in light of developments since its adoption. One of the most significant developments that has occurred since the adoption of Article 1 is the shift from paper to electronic media. At a minimum, therefore, it is expected that Article 1 will be revised to recognize the validity of electronic signatures and electronic writings.

Another effort rapidly proceeding under the auspices of NCCUSL and the ALI is a new UCC article on licenses which will govern not only traditional software contracts but any license of information (for example, books, movies, databases). In the process of addressing concerns unique to the information industry, the drafters have considered issues, such as electronic contracting, that every industry will likely need to consider. For example, the February 1998 draft of Article 2B provides that a "record" cannot be denied legal effect solely on the grounds that it is electronic. Article 2B also addresses the use of "attribution procedures" as a signature substitute in an electronic commerce environment. In this regard, Article 2B, as currently drafted, largely mirrors the concept of commercially reasonable security procedures found in Article 4A of the UCC governing funds transfers.

Article 2B does not, however, address some rather important aspects of electronic records namely, the admissibility of electronic records in legal proceedings and the use of electronic records to satisfy legal requirements that original documents be retained. Regardless of whether Article 2B ultimately addresses all of these issues, the adoption by all 50 states of Article 2B is still a long way off. Moreover, the principles stated in Article 2B are restricted to the scope of Article 2B. Thus, even when Article 2B is adopted, it will not affect a significant portion of electronic commerce. With that in mind, NCCUSL established a separate drafting committee to tackle electronic transaction issues generally in a new Uniform Electronic Transaction Act. The ETA, although on a "fast track," is still at a very early drafting stage. Several important decisions, including the scope of the Act, are still being debated. Having said that, the Act is expected to provide for the legal recognition of electronic signatures and records in most commercial transactions, and for the use of electronic records as evidence.

In addition to the uniform state law efforts of NCCUSL/ALI, there has been a proliferation of non-uniform United States state laws addressing electronic commerce that are generally referred to as "digital signature" or "electronic signature" laws. There are at least 43 states that have enacted, or are currently considering, electronic signature legislation. These state law initiatives vary considerably. For example, many states have limited the scope of their legislation to specific types of transactions (for example, transactions with the State, medical records, motor vehicle records). However, the biggest difference concerns the type of signatures covered, electronic signatures versus digital signatures, and the effect of those signatures on electronic documents.

The more general term -- electronic signature -- can be used to describe any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing. Examples of an electronic signature include a name typed at the end of an e-mail message by the sender or a digitalized image of a handwritten signature of the sender. A "digital signature" is a subset of electronic signatures and represents a unique way to "sign" an electronic message.

A digital signature is simply a string of alpha-numeric characters. It is created by running an electronic message through a one-way hash function (thereby creating a unique digest or fingerprint of the message) and then using public key cryptography to encrypt the resulting message digest. Like all electronic signatures, a digital signature can serve the same function as a handwritten signature in that it can be used to signify authorship or assent. A digital signature, however, also serves an important security function that a handwritten signature and many electronic signatures may not. Because of the use of the hash function, a digital signature allows the receiver of a message to determine whether the message has been altered since it was digitally signed.

State legislation in this area tends to address either electronic signatures (23 states) or digital signatures (16 states), but not both. States with legislation on electronic signatures differ on the question of what qualifies as an electronic signature. Several states have taken the UCC Article 1 approach and recognize any form of electronic mark intended to serve as an electronic signature. Other states, however, require that several conditions be met before an electronic signature will be legally enforceable. Generally, for these states, in order for an electronic signature to be effective it must: (1) be unique to the person using it; (2) be capable of verification; (3) be under the sole control of the person using it; (4) be linked to the data in such a manner that if the data is changed the signature is invalidated; and (5) conform to regulations adopted by the Secretary of State.

Digital signature statutes typically provide for the promulgation of regulations governing the implementation and use of a digital signature infrastructure. The digital signature infrastructure contemplated by these statutes involves a trusted third party, usually a certification authority or CA, whose job is to confirm that the private key used by a sender to sign an electronic message is in fact the private key of the purported sender. Because the legitimacy of the digital signature infrastructure largely depends on the procedures established by the CA, most digital signature statutes define the obligations of the sender, relying party, and CA with respect to the use of digital signatures and certificates and set standards of conduct or CAs. In addition, most digital signature statutes establish a licensing procedure for CAs.

As an aside, on January 12 of this year, the Office of the Comptroller of the Currency authorized Zions First National Bank to establish an operating subsidiary that would serve as a certification authority. The OCC determined that acting as a CA is the functional equivalent of notary services long offered by banks and a natural outgrowth of bank identification and verification skills. The operating subsidiary will be licensed and operated in accordance with the Utah digital signature statute. The Utah law, which served as a model for many of the other states' digital signature laws, insulates certification authorities, that properly perform their functions, from liability.

Of course, the ultimate purpose of any digital and electronic signature statute is to provide for the validity of electronic signatures. All of the state statutes provide that use of an electronic or, if appropriate, digital signature on an electronic record will be treated in the same manner as a handwritten signature on paper. Most of the digital signature statutes, however, also include a legal presumption that the person whose name is associated with a digital signature is in fact the person who signed the document.

One final point that I would make in connection with state law initiatives is what lawyers call conflicts of laws law -- that is, most of the legislative efforts just described do not address the degree to which the state enacting the legislation will recognize electronic signatures created in compliance with another state's statutory scheme. These statutes also generally fail to address the validity of unsigned electronic documents or the evidentiary use of electronic records generally.

If you are interested in learning more about these statutes, you might want to visit the www.mbc.com web site. This web site provides a summary of all existing and pending digital and electronic signature legislation in the United States with links to the actual legislation where possible.

Like the states, Congress is also divided on the appropriate scope and content of electronic authentication legislation. In September 1997, the House passed "The Computer Security Enhancement Act of 1997." If passed by the Senate, that act would establish a national policy panel for digital signatures. The panel, which would be composed of Federal and state Government as well as private technical and legal experts and interested members of the public, would serve as a forum for exploring all relevant factors associated with the development of a national digital signature infrastructure. The panel would be expected to produce model practices and procedures for CAs, standards to ensure consistency among jurisdictions that license CAs, and audit standards for CAs.

In addition to this bill, at least three other bills have been introduced into Congress within the past five months that propose specific rules for electronic signatures. The Electronic Financial Services Efficiency Act introduced by Representatives Baker and Dreier (H.R. 2937) on November 8, 1997 is by far the most comprehensive of the three. The Baker bill would place electronic authentication methods on par with traditional written signatures provided that they reliably establish the identity of the sender or maker of the electronic communication, and reliably verify that the message has not been altered. Public key cryptography and signature dynamics technology are specifically recognized as trustworthy electronic authentication techniques. Other technologies would be deemed satisfactory if they meet certain criteria.

One aspect of the Baker bill which has generated a lot of interest is its establishment of an industry self-regulatory organization along the lines of the National Association of Securities Dealers. Any person or entity -- not just a certification authority -- wishing to provide electronic authentication services in the United States would have to be registered with the SRO. The SRO would establish a committee, supervised by the Department of Treasury, to develop, refine, and apply standards respecting the role and responsibilities of parties involved in electronic authentication services and the licensing and registration of certification authorities.

On February 2, 1998, Senator Bennett, Chairman of the Banking Committee's Subcommittee on Financial Services and Technology, introduced the Digital Signature and Electronic Authentication Law of 1998 (S. 1594) which is aimed at facilitating the use of electronic authentication by United States financial institutions. The bill establishes the right of a financial institution to use electronic authentication if it has entered into an agreement with any counterparty or has established a banking, financial, or transactional system using electronic authentication and the use of the electronic authentication would be valid according to the relevant agreement or system rules.

Under this bill, financial institutions would be exempt from state law regulations governing the registration, licensing, or use of electronic authentication as well as from any state law limitations or impositions of fees in connection with electronic authentication services. Absent compliance with state laws, however, use of electronic authentication by financial institutions would not be eligible for the state law presumptions or benefits, including the presumption that an electronic signature is the equivalent of a manual signature.

Moreover, financial institutions remain subject to supervision by the appropriate banking supervisor which may, by regulation or order, preclude a financial institution from using electronic authentication in its business if it determines that such use would not be consistent with safe and sound banking practices, or if such use would threaten the safety and soundness of the institution, subsidiary or affiliate. In addition, like the Baker bill, the Bennett bill expressly provides that state consumer protection laws, as well as the Truth in Lending Act and the Electronic Funds Transfer Act, continue to govern consumer transactions that use electronic authentication.

Finally, in early November 1997, Representative Eshoo introduced the Electronic Commerce Enhancement Act of 1997 (H.R. 2991), which would require Federal agencies to make forms available electronically and to allow individuals to submit forms electronically over the Internet. Digitally signed forms accepted in accordance with this act would have the same force and effect as if they contained a written signature. In addition, the bill calls for the issuance of digital signatures to appropriate Federal employees and the establishment of guidelines governing the manner in which Federal agencies accept certificates for digital signatures. These guidelines will permit a Federal agency to accept certificates issued by the agency or a trusted third party provided that: (1) the trusted third party is licensed or accredited by a state or local Government or an appropriate accreditation body; and (2) "in accordance with commercially reasonable standards, accepts liability for and is insured against negligent issuance or handling of certificates."

International Efforts

While the United States Government has for the most part been an observer of the domestic efforts to establish a legal infrastructure for electronic commerce, it has been an active participant in the international arena through organizations such as the United Nations Commission on International Trade Law (UNCITRAL) and the Organization for Economic Co-Operation and Development (OECD).

UNCITRAL was established by the General Assembly in 1966 with the general mandate to further the progressive harmonization and unification of the law of international trade. In 1996, UNCITRAL adopted a Model Law on Electronic Commerce. The Model Law is aimed at removing legal obstacles to the use of electronic communications. Thus, the Model Law provides that information shall not be denied legal effect solely on the grounds that it is generated, sent, received or stored by electronic means, and establishes rules for when an electronic writing and signature will satisfy existing legal requirements for writings and signatures. The Model Law also provides solutions for legal issues that arise in the use of electronic communications, such as the admissibility of electronic records and the attribution of electronic communications to particular parties.

UNCITRAL, along with OECD and others, has now undertaken to explore possible legal rules underpinning digital and other electronic signature systems; specifically the cross-border recognition of electronic signatures. While the United States would have preferred UNCITRAL to have extended the work of the Model Law to cover additional contracting issues, a large number of other countries supported work on digital and other electronic signatures. The United States has chosen to fully participate rather than risk the emergence of rules which, while not binding on any state, might not be as supportive of market-based commerce as the United States believes it should be, and which would carry a U.N. imprimatur.

The core issues from the United States perspective have been whether agreement can be obtained on rules that are open to all systems, that is rules that recognize leading technologies such as Public Key Infrastructure, or PKI, but also provide legal support for other systems. Moreover, variable PKI formats have been developed, and differing levels of PKI certification will be in commercial use, including CA generated high and low level certs, and probably non-CA issued certs. The United States position has been that the different user paradigms may require different legal standards and presumptions, which should not be limited to existing PKI-based systems.

In addition, the United States has advocated that any U.N. or other international legal text on signature rules should incorporate both regulated licensed systems and private sector non-regulated systems. Furthermore, such rules should be open to non-digital technologies. From the standpoint of commercial law, delineation of fall-back rules on obligations, assurances, and reliance would be necessary to achieve the necessary risk allocation and commercial usage. This will probably require sliding standards for attribution, commercial reliance, liability and security depending on the types of transactions and the imperatives of market cost and pricing. Carveouts may be appropriate for closed or

controlled access systems.

So far, there has been a significant amount of debate, but little agreement, on these and a host of other issues. While a number of countries in the Working Group appear to agree that any project should, to the extent possible, follow the media neutral approach taken in the 1996 Model Law, thus far the focus has tended to be on the cross-border recognition of the use of digital signature technology. This may be indicative of the fact that several countries have enacted or have proposed digital signature legislation. Spain, Germany, Malaysia and Italy are among the foreign jurisdictions that have enacted digital signature legislation. Other countries such as Australia, Japan and the United Kingdom have developed guidelines on digital signatures.

The Working Group has agreed on at least one important issue. Even though PKI technology can be used to encrypt messages, questions relating to the use of PKI and other cryptography for security purposes are outside of the scope of this UNCITRAL effort. Of course the United States continues to advocate the development of a voluntary market-driven key management infrastructure and of key recoverable encryption products. And while this position is not reflected in the OECD's Guidelines for Cryptography Policy, I am sure that the Administration will continue to promote key recovery both domestically and abroad.

In closing, I would like to echo the sentiment expressed in the Framework: "The success of electronic commerce will require an effective partnership between the private and public sectors, with the private sector taking the lead." The creation of private fora such as this conference, which bring together Government representatives and industry, provides an exciting opportunity to further that partnership. I challenge each of you to use this opportunity not just to recite your company's or your agency's views but to listen to the ideas and concerns of other conference participants and incorporate them into both public and private policy initiatives.