Testimony of Daniel Greenwood
Deputy General Counsel for the
Information Technology Division, Commonwealth of Massachusetts
before the
U.S. House of Representatives Committee on Commerce
Subcommittee on Telecommunications, Trade and Consumer Protection

June 9, 1999

Mr. Chairman, members of the Subcommittee, on behalf of the Commonwealth of Massachusetts, thank you for the opportunity to testify today on House Bill 1714, the Electronic Signature in Global and National Commerce Act (E-SIGN). The Commonwealth is home to many information age businesses and our state government is a robust user of electronic commerce technologies. As such, the Commonwealth of Massachusetts has had significant experience with the legal and policy implications of electronic authentication technologies. It has been the policy of the Commonwealth to promote the growth of our emerging electronic commerce industry in a non-regulatory, market-driven fashion.

To the extent that H.R. 1714 facilitates creation of a national consistent legal infrastructure supporting electronic commerce without unduly disrupting related areas of state law, it deserves serious consideration and support. While the current language of the bill contains certain provisions that would benefit from further honing, it seems clear that the objectives of this legislation are wholly consistent with the Commonwealth's policy to assure a sound foundation for electronic commerce. Our desire is to indicate the ways in which this bill can be helpful and to constructively suggest some alternative formulations of certain sections for the purpose of achieving the bill's goals without causing harm to ongoing efforts at the state level to develop more uniform electronic commerce law as part of the overall uniform state commercial legal framework.

Last month, the Commonwealth went on record before the Senate in support of S. 761, by Senator Abraham, which promotes a national legal base-line on certain issues related to electronic commerce transaction contracts and usage of electronic signatures and records. In an Issues Brief dated April 19, 1999, the National Governor's Association questioned the need for federal legislation, but characterized the Abraham bill as follows:

> "Despite the preemption contained in the Millennium Digital Commerce Act, the legislation is fairly friendly to states' interests. The bill's scope is carefully restricted to interstate commercial transactions, over which Congress has jurisdiction through the Commerce Clause. The drafters of the bill have made a concerted effort to avoid interfering with areas of state law that involve records and signatures that are unrelated to interstate commerce." [http://www.nga.org/Pubs/IssueBriefs/1999/990419FedDigitalSigs.asp]

It seems clear that the Abraham bill and H.R. 1714 have very similar goals and are on corresponding tracks through each respective chamber. It is hoped that the final version of H.R. 1714 is refined so as to avoid the problems associated with undue interference with legitimate areas of state laws governing records, signatures and contracts. Assuming that such amendments occur, then this bill would clearly meet the stated interests of electronic commerce industry advocates who have voiced a desire for legal reforms to provide greater certainty in the short term.

Background

Conventional wisdom is evolving regarding the appropriate scope of legislative action effecting electronic commerce. Despite a brief fad in the mid-1990s favoring a regulatory, technology-specific approach to electronic commerce, the vast majority of state governments have recently opted for a minimalist, non-regulatory and technology-neutral stance. Unfortunately, certain foreign jurisdictions and international organizations seem to be several years behind the United States and are currently adopting regulatory, technology specific, and centralized policies regarding electronic commerce generally. Fortunately, both H.R. 1714 and the Abraham bill reflect the U.S. preference favoring free and competitive markets, rather than government intervention.

In 1995, Utah was the first jurisdiction in the world to enact "digital signature" legislation. Reflecting the trends of the time, this law is regulatory (it empowered a state agency to license providers); technology-specific (public key cryptography); promotes a certain business model and implementation (trusted third parties and digital certificates); increases e-commerce user liability (by limiting provider liability); and reverses age-old evidentiary rules regarding proof of signatures (by providing a presumption against the signature technology user).

The passage of time indicates that this approach went too far and created unintended market distortions. In fact, it has not even been generally favored by the very industry it was enacted to promote (virtually every major certificate provider has chosen not to become licensed in the three states—Washington, Minnesota, and Utah--that attempted to regulate their fledgling product or service sector.

Over the past few years, a broad convergence in activity and published policy has evidenced a solid and growing consensus that government actions effecting electronic commerce should generally be non-regulatory, technology neutral, support the rights of parties to structure their business models and technical implementations through contracts and agreements and should not tamper with rules of evidence and liability apportionment as an industrial policy setting mechanism.

The last point, regarding tampering with rules of evidence, bears some additional explanation. There have been proponents of legislation at the state and the federal level which would create an evidentiary presumption against the user of an electronic signature. The rationale was that receivers of electronically signed messages deserve special government protection. This rationale fails to recognize that the proponent of such evidence should be the party with the burden to prove that the signature occurred. Likewise, the receiver of the signature is in the best position to judge the reliability of the authentication in the context of the value of the transaction, and they are the party most likely to have the relevant evidence that a signature was presented to them. Again, both H.R. 1714 and the Abraham language reflects these time-honored legal principles.

The application of these general principles to electronic commerce is swiftly gained wide acceptance over the past few years. In the 1997 *Framework for Global Electronic Commerce*, the Clinton Administration articulated principles supporting a technology-neutral approach to electronic commerce, and opposing regulation. Likewise, in 1997, the Internet Law and Policy Forum drafted a set of principles that promoted a thriving market and strongly resisted regulation (see: http://www.ilpf.org/digsig/principles.htm). And in the Telecommunications Act of 1996, Congress expressly found that ``[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation" and declared that ``[i]t is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." The Commonwealth was pleased to work with Senator Abraham's office and the office of Congresswoman Eshoo on the Government Paperwork Elimination Act last session, which also largely embodied these principles. Over the past two years innumerable additional such positions, statements and policies among states and the federal government as well as from various private

organizations.

General Criteria for Legislation

The success or failure of legislation governing e-commerce this session should be based on the answers to five fundamental questions.

1. Is the legislation narrowly tailored to address existing and well understood market failures?

Another word for this is "minimalist" in other words, limited to address only what is currently necessary and appropriate. The chances of "doing no harm" are increased dramatically when government intervention in the private market is closely restricted to fixing specific and demonstrated problems that the market and existing laws have failed to address. This is especially true in the fast growing and dynamic area of electronic commerce. Relatively small changes in law can have the effect of chilling competition or otherwise distorting the free evolution of efficient solutions in the quickly moving and difficult to predict e-commerce field. Specifically, legislation that focuses on or includes provisions dealing with business or consumer rights or liabilities connected with the use of a public key infrastructure or other particular technologies that are not yet widely used may create harmful and unnecessary results. The actual problems may well turn out to be different than the projected issues.

2. Does it promote a competitive marketplace for different technologies?

Legislation should promote, rather than chill, competition. That means Congress should avoid legislating a market winner. Another way to look at this criteria would be: "is it technology-neutral or does it give a special legislative 'leg up' to a given technology, business model or implementation available for general use in the market?" It is unfortunately common that special interests that stand to benefit from market intervention often lobby for such government action. In the case of electronic commerce, however, it seems clear that the best government action with respect to promotion and facilitation of that market is usually *no action at all*. By enshrining a given technology in legislation, government action may have the counter-effect of reducing incentives for further improvements and innovations.

Legislation can distort the technology markets by regulating the security or reliability criteria that must be applied to create an electronic signature even if it stops short of specifying the particular technology necessary. These types of criteria usually include a requirement that the signature technology is under the "sole control" of the signer and that it can detect or prevent any change to the signed record. These particular implementations may be appropriate in some, perhaps many, situations. However, the specific security features necessary and appropriate will differ dramatically depending upon the transaction and the parties' needs. For example, a "signature machine" (e.g. an institutional check signing mechanism) is clearly not under the "sole control" of the signer. In fact, it is doubtful that a treasurer, comptroller or CFO of an institution has any direct contact at all. The same is true of non-check organizational authentication of many types. It is accessible to several authorized individuals and there are internal controls and systemic security measures in place. Similarly, many popular and adequately safe authentication implementations do not, by themselves, detect or prevent alteration of underlying data. Most PIN and password systems in use today in banking, healthcare, commerce and elsewhere do not possess this specific feature. Nor do many biometric products.

Current implementations live or die based on buyers and users making cost, benefit and risk judgements about the amount of reliability and types of security features needed. Well-intentioned attempts by legislators to come up with a "one size fits all" approach to signature technology features are doomed. The Uniform Electronic Transactions Act at one time had such criteria, but based upon months of discussion it now reflects and supports the common law definition of signature: any symbol executed with the intent to sign. In narrow

cases where legislation is dealing with specific user communities (like a Securities context or a Consumer Protection issue) then it may be appropriate to specify more specific requirements, but general legislation covering every economic and social sector should never distort the competitive and open market for electronic signature and records technologies.

3. Does it include any new or expanded regulation or other government intervention, including legislatively created "accreditation" through government approval or control over technology suppliers or users?

It is increasingly obvious that the United States stands at the opening of a substantively different economic and societal phase: some call it the information society. The economic impacts are profound. Decentralized, self-organizing and distributed systems are gaining dominance. Old industries built on intermediating relationships are disappearing as the Internet and other technologies eliminate the barriers that created a need for such middle-men. Fast changing, dynamic, and rapidly growing markets are evolving before our eyes--in many cases, markets which are little understood.

Unfortunately, some advocates continue to promote industrial-era policy designed for economic and social conditions of the last century. Industrial organizations were inherently centralized and regulations were correspondingly focused at the "choke points." Internet-mediated communications and new forms of relationships between parties are often--and increasingly--organized differently. Centralization of market participants for the sole purpose of making them easier to regulate for government is wrong. And such a policy risks killing the goose to control its eggs. Requiring government licensure of market suppliers or setting up so-called "self regulatory organizations" (which in fact are under the thumb of federal or state regulators) is antithetical to the new economy. Absent serious market failures, government should resist erecting new oversight and control mechanisms over any part of electronic commerce. There are, of course, a large number of existing statutes, regulations and legal doctrines that create a floor of behavior to handle crime, fraud, and threats to national security. These laws currently appear to be quite adequate to prevent known harms.

One useful policy approach is modeled in the draft report developed by the NACHA Certificate Authority Ratings and Trust Task Force, which seek to give parties helpful guidelines, including detailed policy and contractual terms, to assist in the creation of legally enforceable and reliable implementation of authentication technology (background information at: www.state.ma.us/itd/legal). This is an example of a "bottom up" approach rather than an approach that favors central policy making or regulatory oversight. Legislation should simply lift legal barriers and thereby allow parties to use existing bodies of law, such as contract law, to tailor their transactions to their own needs. Ultimately, as national standards and practices emerge, they will be based upon actual proven market experience and they will be far better than any scheme anyone can dream up today through central planning. The current draft 1.0 of the NACHA CARAT Guidelines is available at: http://internetcouncil.nacha.org/CARAT/CARAT921.DOC on the web. A ginchy example of contractually based Operating Rules that are consistent with the CARAT Guidelines can be found at http://www.emall.isa.us/ (a multistate electronic commerce procurement project to buy goods over the web from several private vendors).

4. Does the legislation disrupt other bodies of law or unduly preempt state jurisdiction over commercial law?

There are compelling arguments in favor of generally keeping governance of commerce under state jurisdiction, provided the law is sufficiently harmonized so as not to present an undue barrier to interstate commerce. States are far more agile than the federal government in responding quickly to changing market conditions. As such, states serve as important laboratories of innovation in the realm of public policy and law.

The arguments are particularly strong for continuing state primacy in the context of electronic signatures, records and contracts, because a signature or a record requirement arises under innumerable other areas of state law. A single federal law that purported to grant legal equivalency for electronic signatures, for example,

would almost certainly have the effect of creating significant disruptions in areas of state law that have nothing to do with commerce, such as wills, trusts, powers of attorney, consumer protections, real estate deeds, negotiable instruments, notice requirements, elections law, hospital regulation, and state criminal justice laws. Massachusetts, for example, has some 4,515 different sections of law that relate to a signing or writing. (*See:* http://www.state.ma.us/itd/legal/siglaw4.doc)

However, in some cases, the needs of the nation require that federal action preempt state law. This has been long accepted where states create undue impediments to interstate commerce. The fact that states have adopted such a dizzying array of different laws dealing with electronic signatures and records has been a major contributor to the current efforts for federal action. If states quickly pass uniform law in this area, it is likely that legitimate private sector interests in a national baseline will be satisfied through uniform state law. This is the preferred method of creating the base-line because the draft Uniform Electronic Transactions Act (UETA) clearly represents the single best, most comprehensive, well principled legislative effort to date and, importantly, it causes few or no serious legal disruptions or other harm because it is finely integrated with other areas of law. No federal law yet proposed (or likely to emerge) can claim the same features – in part because the National Conference of Commissioners on Uniform State Law has sponsored a multi-year deliberative process in which interested parties from the public and private sectors have collaborated in open forums to work through these complex and subtle issues. However, to the extent that commercial interests make a convincing case that faster action is needed than can be accommodated via the uniform law process, then the Commonwealth has already gone on record as supporting narrow and temporary federal "bridge" legislation to produce the necessary legal national base-line.

The key criteria for any such bridge legislation is that it must be narrowly tailored to address only those matters upon which immediate action is needed (as distinct from matters that can wait for uniform state law) and that it provide a statutory mechanism that reverts jurisdiction back to the states upon adoption of a consistent base-line legal framework. Since the UETA appears poised to shepherd in such a framework, any federal law in this arena should recognize and promote this uniform law effort.

5. Does the legislation give an undue competitive advantage in this new market to a single industry or economic sector over participants of other economic sectors?

Legislation should not grant any particular sector a special leg up by government. If legislation lifts general legal barriers or solves general problems for only a specific sector of the economy, then an undue competitive advantage may result in unfortunate market distortions. Promoting competition among different sectors in this area is good because many of the problems are far from being solved, and each sector bring its own resources, expertise and approaches to the solutions. Legislation granting special presumptions or validity upon electronic authentication when it is supplied only by vendors in a single market (say, by telecom companies, or network service providers, or licensed attorneys, or even financial institutions alone) runs the risk of ultimately harming, rather than promoting, optimal technical and business-model solutions that would arise from highly competitive marketplace interactions.

Summary and Conclusion

In summary, the apparent goals of H.R. 1714 are worthy of support. Private sector representatives have made a strong case before the House and Senate that some action is needed in the shorter term. The objectives of this legislation are evidently to satisfy these legitimate interests of industry without unduly harming related areas of state law. Review of the bill based upon the five question asked above indicates that this legislation, with some modifications, can directly satisfy key principles for electronic commerce legislation.

I request the privilege to add an addendum to these written remarks within the next 30 days which will provide more detailed comments on the precise provisions of the current legislative language as they relate to

state law and to suggest possible alternative formulations. We anticipate these comments will focus largely on limiting the scope of Title I to contracts effectuating interstate commerce transactions (as opposed to including all agreements that may affect interstate commerce); assuring that the operative provisions of the law merely accord legal status upon electronic transactions that is equivalent to what those transactions would receive if they were carried out via other media (as opposed to granting whole new categories of rights and responsibilities only for electronic transactions); assuring that the formula for states to retrieve jurisdiction under the overall framework of existing commercial law is clear and promotes enactment of the UETA or an equivalent uniform law; minimizing or eliminating federal administrative oversight over state government affairs; and conforming definitions of electronic signatures and other key terms to existing and emerging bodies of law governing electronic transactions.

Please do not hesitate to call upon my office as a supportive resource as this legislation continues to evolve. It is my sincere hope that we can assist you as you seek to hone some of the provisions of this bill to conform more closely to the principles set out above. Again, thank you for the chance to share our views today.