THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

H.R. 1714

JUNE 9, 1999

Serial No. 106–32

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
57–447CC WASHINGTON : 1999

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL G. OXLEY, Ohio,
Vice Chairman
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
BILL LUTHER, Minnesota
RON KLINK, Pennsylvania
THOMAS C. SAWYER, Ohio
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

WEDNESDAY, JUNE 9, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin, (chairman) presiding.

Members present: Tauzin, Stearns, Gillmor, Deal, Largent, Cubin, Shimkus, Ehrlich, Bliley (ex officio), Gordon, Rush, Eshoo, Sawyer, Green, McCarthy, and Dingell (ex officio).

Staff present: Paul Scolese, professional staff member; Mike O'Reilly, professional staff member; Ed Hearst, majority counsel; Donn Salvosa, legislative clerk, and Andy Levin, minority counsel.

Mr. TAUZIN. The committee will please come to order.

A number of years ago, the "New Yorker Magazine" ran a cartoon showing two dogs seated at a computer. One dog says to the other, "On the Internet, nobody knows you are a dog." That is also true, by the way, in some voter registration systems in some of our States. I think there was a newspaper in Lake Charles, Louisiana, that managed to register two dogs in the Louisiana elections.

For the first few years of the Internet, that was true. You really didn't know who was on the other end. However, with the explosion in electronic commerce activities, a clear need has developed for knowing who you are and who you are dealing with online; especially now that online transactions are becoming more and more complex. Many companies are currently at work developing products and services that seek to electronically authenticate parties to online transactions.

One hurdle the companies that are seeking to use the electronic authentication face is the uncertain legality of electronic signatures. States have begun to update laws to address this problem. To date, 44 States have enacted some type of electronic signature law. However, no two States have adopted the same law. Therefore, the result is a patchwork of State laws on the recognition of electronic signatures.

In my opinion, 40 of 50 different State standards will make interstate commerce very difficult; if not in some cases impossible. The subcommittee is aware that there is an effort underway to create a uniform State electronic signature law. Even under optimistic assumptions, adoption by all 50 States will take 3 to 5 years. Now

that may not seem like a long time. But in the fast-changing world of electronic commerce, that is nearly an eternity.

Today this subcommittee will be examining H.R. 1714, the Electronic Signatures In Global and National Commerce Act, "E-SIGN." The goal of this act is to further promote the development and growth of electronic commerce by clarifying the legal status of electronic signatures and records. Contracts or agreements cannot be invalidated solely because the agreement or contract is in an electronic form, or has been signed electronically. The legislation does recognize the efforts by States, and allows States to enact their own legislation to recognize electronic signatures and electronic records.

The efforts to create a uniform State electronic signatures law, and the goal of H.R. 1714 are, therefore, in no way incompatible. Rather, they are complementary in that they are working toward a single, uniform standard.

Another important element of this legislation is that it provides this sector of Commerce with guidance in promoting American principles on electronic signature laws overseas. It would clearly harm American interests to have foreign nations enact laws that would, or could, discriminate against American products and companies; or create closed systems that do not recognize the technologies and systems used by American companies. I think we only have to look at the controversy surrounding the third-generation wireless standards to see how important the international marketplace is.

We will be hearing from a panel of witnesses today that will give us many perspectives on the issues of electronic authentication, and on H.R. 1714 in particular. The panel includes developers and users of these technologies, as well as representatives from State governments and the administration.

H.R. 1714 is clearly the beginning of a process. I fully anticipate that this committee will be working with Chairman Bliley and all interested parties to work out a final bill that will meet our goal of furthering the use of electronic signatures and promoting electronic commerce. Additionally, we look forward to hearing comments from our colleague from Tennessee, Mr. Gordon, on the work that he has done on H.R. 1572, his Digital Signature Act of 1999, which I understand has been referred to a different committee.

I thank you and look forward to hearing the testimony from our distinguished panel.

The Chair is pleased to recognize the author of the legislation, the Chairman of the full Commerce Committee, the honorable gentleman from Richmond, Virginia, Mr. Tom Bliley.

Chairman BLILEY. Thank you, Mr. Chairman. You know, I represent a district in the Commonwealth of Virginia, better known as the "Internet Capital of the World." It is home to Internet companies, both large and small. As a result, I have the chance to talk with leading Internet business executives and visit cutting-edge technology companies. Everywhere I go and everyone I speak to tells me how important it is for Congress to pass legislation that provides legal recognition to electronic signature and electronic records.

While I am speaking of Virginia, I also want to welcome Don Upson, the Secretary of Technology for Virginia. Virginia was the first State in the Nation to create a cabinet-level position for technology secretary. I think this clearly shows the commitment by Governor Gilmore and others in the State to promote the growth of electronic commerce and information technology.

We saw the explosion of electronic commerce during last year's Christmas shopping season—far in excess of all the predictions. The pace has not let up. When many people think of electronic commerce, they think of buying books or airplane tickets. But recently, we have seen people starting to buy automobiles; getting approved for mortgages; or investing their retirement funds online—something we could not have imagined just a few years ago.

As the value and complexity of online transactions grows, the need for knowing that the transaction is legally binding becomes even more important. That is where H.R. 1714, the Electronic Signatures in Global and National Commerce Act, comes in. By clearing away the legal uncertainties surrounding electronic signatures and records, more businesses will use electronic signatures and consumers will feel more comfortable doing business online. The technologies used to create and transmit electronic signatures also provides much greater safety and security to online transactions.

As I have stated many times during last year's series of hearings on electronic commerce, I want to see that the safety, security, and privacy of online consumers is protected. Encouraging businesses and consumers to use electronic authentication will help to do just that. I believe that H.R. 1714 is the correct approach to creating a legal framework for accepting electronic signatures and records.

The legislation lays out a single nationwide standards for the acceptance of electronic signatures and electronic records. We do not pick or choose a specific type of electronic authentication; nor do we choose what types of businesses should be allowed to offer electronic signature services. The legislation also provides guidance to the Department of Commerce in the their international negotiations on electronic authentication. I believe that the principles laid out in this bill, such as technological and business neutrality and market leadership, should be promoted overseas. I do not want to see foreign nations instituting electronic authentication regimes that would discriminate against American manufacturers or providers of electronic authentication technology.

H.R. 1714 also amends Federal securities law to provide for the legal acceptance of electronic signatures and records. This provision will be the subject of an upcoming legislative hearing in Mike Oxley's subcommittee. I do want to recognize the efforts that States have been making in this area. Today more than 40 States, as the chairman has said, have enacted legislation that provides recognition of electronic signatures. My concern is that every law is different. Many only allow State agencies to accept electronic signatures; and some provide legal recognition only to signatures generated by a specific technology.

It is clear that for unfettered interstate commerce to take place, we must establish a single, nationwide standard. I understand that a uniform State law on electronic signatures is being developed. I believe H.R. 1714 recognizes this effort by allowing States to enact

their own electronic signature bills that follow the principles laid out in H.R. 1714.

I look forward to hearing the comments and issues raised in this hearing and the future hearings on H.R. 1714. I am hopeful that we will move H.R. 1714 through the committee and to the House floor before the end of the year. These hearings move far down the road to having this bill signed into law.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. TAUZIN. I thank the chairman for his statement and for his extraordinary attention to the issues of electronic commerce at this committee and other subcommittee levels. By the way, I want to commend you, Mr. Chairman, for not seeking to claim the invention of the Internet.

Chairman BLILEY. We already have a claimant to that.

Mr. TAUZIN. The Chair is now pleased to recognize the gentlelady who has a been a leader for a long time in the digital signature area, the gentlelady from California, Ms. Eshoo.

Ms. ESHOO. Thank you very much, Mr. Chairman, for your kind words, as well. This is an important hearing today. I am delighted to not only be a part of it, but to welcome everyone that is here to testify. We are discussing legislation in which we and Congress are trying to prevent a revolutionary way of business from being really strangled by outdated laws. Specifically, this legislation updates the law by declaring that electronic signatures will be deemed valid.

This legislation extends the principle of electronic authentication we established last Congress, with the passage of my legislation which was entitled, "The Government Paperwork Elimination Act." That law required the Federal Government to accept electronic signatures. We are now seeking to extend that advancement to the commercial world. This is more than an appropriate step for the Congress to be taking.

The Internet has really introduced many new buzzwords into our lexicon, our vocabulary, words like: "browser," "web page," and "e-mail." The newest term, of course, is "e-commerce." The projections for the growth of electronic commerce and its effect on the global economy are indeed staggering. Last year, shoppers spent an estimated $9 billion buying products online. That is quite an eye-opener—$9 billion. Business-to-business electronic commerce was nearly five times greater than in the consumer market, reaching $43 billion just last year. By the year 2003, Forester Research predicts business-to-business electronic commerce will climb to $1.3 trillion. At the Federal level, we understand these sums. That would constitute nearly 10 percent of all U.S. business trade.

Not only are the Fortune 500 companies taking advantage of this new way of doing and transacting business; but it offers an extraordinary opportunity to over 5 million small businesses in our country. Not long ago, small businesses, like the jewelry store that my father owned in Connecticut, were limited to doing business in the community that they were located in. Now with the web page and some creative marketing, a store in Connecticut may be repairing watches sent all the way from my district, Palo Alto, California. Or jewelry stores in Connecticut may be selling their products to department stores in California.

The electronic commerce bill I introduced and the bill before us today are attempts to make sure our laws permit that businesses in Connecticut and stores in California do business by utilizing the latest form of electronic signatures. Both bills aim to ensure that those conducting business online and who chose to sign electronic contracts with electronic signatures will be able to do so with legal certainty.

Many States have already passed legislation. The chairman of our committee just iterated that in his comments before us. They have passed legislation allowing for the acceptance. Unfortunately, this has resulted in a confusing maze of State laws that hamper interstate commerce. States have been working on developing a uniform model law to create one standard for acceptance of electronic signatures and contracts similar to what the Uniform Commercial Code accomplished for contract law. It is expected to be completed soon and offered to the 50 State legislatures for adoption.

The bill I introduced and the one we are discussing today bridge the gap from now until the fiftieth State has passed a version of this model law by preempting the existing confusion of multiple State laws. In fact, identical bipartisan legislation of mine, introduced in the Senate, has already been endorsed by State governments and industry, alike.

I am concerned in this particular area that the bill we are discussing today has somewhat of a heavy hand in implementing a 2-year deadline on States, and would inappropriately give the Secretary of Commerce the ability to enjoin State laws. So I look forward to discussing with the panelists today their impression of the section in question: section 102 of H.R. 1714.

I want to salute the chairman of our committee for his broad and important interest in this area of electronic commerce. I look forward to working with him and Chairman Tauzin on improving this legislation so that it can, indeed, be adopted in the 106th Congress, at a time when it really is going to count the most. Thank you, Mr. Chairman. I yield back.

Mr. TAUZIN. I thank the gentlelady. Indeed, the committee is grateful to her for her pioneering work in this area and her commitment to continue this process. The Chair is now pleased to welcome and recognize the gentlelady, Ms. Cubin, for an opening statement.

Mrs. CUBIN. Thank you, Mr. Chairman. Thank you also for holding this important legislative hearing on H.R. 1714, the Electronic Signatures in Global and National Commerce Act, or E-SIGN.

The commercial activity that takes place over the Internet is staggering. It is growing rapidly. We are witnessing an incredible expansion of business transactions over the network. I am personally amazed at how much commercial activity was conducted over this past Christmas season. You know, since I like to shop, it was even better.

E-commerce moves us from making traditional face-to-face purchases, of which we have all grown accustomed, to blindly trusting a stranger at the other end of a computer screen to responsibly and honestly carry out the transactions that we want. H.R. 1714 will allow some semblance of trust when making these blind trans-

actions over the Internet. It will not only bring some peace of mind to those of use who engage in e-commerce; it will also promote growth and development of the electronic commerce industry.

It is important the consumers be assured that there is legal validity of contract or transaction that is made over the Internet. I am a strong advocate for States' rights and developing an environment where States can establish policy that works best for each particular State. In the case of electronic signatures, there are currently over 40 States that have enacted some sort of legislation to recognize the validity of electronic signatures. The problem, however, is that no two States have an identical law. This makes it difficult to do business transactions across State lines; and at the same time ensure the legal validity of a contract where one State recognizes it as being binding because is it was signed electronically, rather than with a physical signature.

H.R. 1714 would establish a uniform, national framework for the acceptance of electronic signatures and records. I support the intent of Chairman Bliley's legislation, and I commend his hard work in bringing this bill forward for discussion. I do look forward to hearing from today's witnesses. I yield back the balance of my time. Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair thanks the gentlelady from Wyoming. The Chair would now recognize the gentleman from Tennessee, but the gentleman from Michigan, the ranking minority member has arrived. I wonder if the gentleman from Tennessee would allow me to recognize him out of turn.

Mr. GORDON. Be happy to.

Mr. TAUZIN. The gentleman from Michigan, the ranking member of our full committee, Mr. Dingell, is recognized.

Mr. DINGELL. Mr. Chairman, I thank you. I thank the gentleman from Tennessee.

Mr. Chairman, I commend you for your holding this hearing. This is an important matter. For centuries a legal contract was not considered valid unless it was impressed with the seal of the signer to prove its authenticity. More recently, China is just beginning to move away from the idea that everything has to be processed with a chop added to the document to establish the authenticity of the document.

Just a few years ago, most of us would never have predicted that a written signature on a sales contract would be obsolete, but that situation appears to be coming upon us. As today's business is conducted increasingly over the Internet and through vast computer networks, the electronic signature is becoming just as crucial for the smooth operation of commercial law. In order for this new world of electronic commerce to take shape, grow, and prosper, we must make sure that electronic signatures are recognized as legal, secure, and binding. Emerging technologies demand that our policies keep pace.

I congratulate Chairman Bliley for his efforts in this area. His legislation, H.R. 1714, would make great strides in furthering the use of electronic signatures in commerce. In these goals he has my strong support. There is, however, one area of this bill that causes me concern. While I agree that it is useful at times to have a uniform national policy, we must be careful not to impose our judg-

ments on the States, particularly at time when they, too, are actively studying these same issues. In fact, I understand that a model State code is currently under development. Many State legislatures are likely to enact it in one form or another.

I believe that we should not interfere with their ability to do so. We should enable the States and utilize the States for the purposes of achieving a uniform national policy; but allow the States to serve as a nursery for the development of good, useful and new ideas. The States should have enough time to fully evaluate this model code; then to write, debate, and pass their own legislation. Unfortunately H.R. 1714, as drafted, would limit to 2 years the period in which the States would not be threatened by Federal preemption. I am afraid this limitation may deny many States the opportunity to act on their on behalf.

Again, I want to commend Chairman Bliley for his hard work. But I want to recognize and commend, as well, my good friend from California, Ms. Eshoo, for her strong commitment and leadership in this issue.

I look forward to hearing from today's witnesses about how we can develop a strong policy on electronic commerce, while at the same time respecting the important role of the States. Mr. Chairman, I thank you for your kindness to me this morning.

Mr. TAUZIN. I thank the gentleman from Michigan. The Chair is pleased now to recognize the gentleman from Tennessee, Mr. Gordon, the author of the Digital Signature Act of 1999. Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman. My compliments for having this hearing. My compliments to Chairman Bliley for introducing this important bill. I want to be on record as being supportive today.

I am going to poach a little time, if it is okay, to bring up another collateral bill that I think is complementary. I hope that we will have a chance to discuss it.

I first became interested in electronic signatures 2 years ago, when the issue came up as part of the Computer Security Enhancement Act of 1997. At that time, I was concerned about how to encourage the widespread use of electronic signature technologies essential to ensure consumer trust in electronic commerce. In H.R. 1907, the computer enhancement bill that passed the House, I inserted the provision that established a national policy panel to address developing consensus on a national electronic signature infrastructure.

Since then, with the leadership of my colleague and good friend, Ms. Eshoo, Congress passed the Government Paperwork Reduction Act, which requires Federal agencies to accommodate electronic transactions by the year 2002. There have also been a number of bills to deal with the legal status of electronic signatures and electronic records. My concern for the last 2 years is how do we promote the widespread use of electronic signatures by electronic commerce beyond the legal structure?

I introduced H.R. 1572, the Digital Signature Act of 1999, with Science Committee Chairman Sensenbrenner, and Ranking Member, George Brown. The bill directs NIST to develop technology-neutral standards on interoperability to encourage the effective use of electronic signature technology by the Federal agencies, and en-

courages agencies to use off-the-shelf commercial products and services. In addition, the bill establishes a national working group under the Department of Commerce to start working on other elements necessary to encourage the widespread, everyday use of electronic signature technology.

If electronic authentication systems are deployed by agencies with little thought to interoperability, it will make it harder—not easier—to conduct business electronically with the Federal Government. We should ensure this is done in a coordinated, technologically neutral way that promotes interoperability and encourages agencies to commercial, off-the=shelf products and services.

In a recent "Federal Technology Week" article, Tony Trinkle, the Director of Electronic Services at the Social Security Administration, said the following, "The bill moves the debate about standards in the right direction, especially at a time when agencies are trying to comply with the GPEA passed last year. The OMB guidelines do not provide much additional help for agencies trying to choose an electronic infrastructure in a growing market."

These same concerns are what prompted me to introduce the bill. Many of our international trading partners recognize the importance of electronic authentication for electronic commerce, and are already working on national electronic signature infrastructures to facilitate the widespread use of electronic signatures. My bill would address this critical challenge by establishing a national working group with industry, States, and other stakeholders to start to develop consensus for this country. This would not only encourage electronic commerce, but will also enhance our position in the world market.

Again, Mr. Chairman, thank you for allowing me to bring in some collateral issues. I am supportive of this bill you have before us today.

Mr. TAUZIN. The Chair thanks the gentleman. Does any other member desire to make an opening statement? Mr. Sawyer? Mr. Deal?

The Chair is pleased, now, to ask unanimous consent that all members be permitted time to introduce into the record written opening statements. Without objection, so ordered.

[Additional statements submitted for the record folow:]

PREPARED STATEMENT OF HON. MICHAEL G. OXLEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

The *E-SIGN* legislation we consider today represents an important advance of law in the electronic age. Since $32 billion changed hands in electronic commerce last year, it's time we act.

We need a federal law to overlay the patchwork quilt of 40 state laws that now govern. E-commerce businesses need that legal certainty, and their customers do, as well.

This legislation has a number of features that should commend it to this committee.

It maintains the important concept of technology neutrality. It applies to all businesses, regardless of their product lines or sizes. It allows the parties to choose what kind of technology they want to use in making their electronic agreements.

And, it has an international section so that we can promote our principles overseas as the global standard.

All state contract law remains intact, with the only change being the federal overlay of the digital signature law. All anti-forgery and anti-fraud law would remain in place without change.

This change will begin to save unnecessary costs and time wasted while paper signatures cross the country through the mail.

E-commerce is booming, and this legislation will support that healthy growth by offering efficiency to businesses and convenience to customers.

Thanks to Chairman Bliley for crafting this legislation. I look forward to conducting another hearing on this bill in the Finance and Hazardous Materials Subcommittee later this month.

PREPARED STATEMENT OF HON. THOMAS C. SAWYER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Thank you Mr. Chairman for holding this legislative hearing this morning on H.R. 1714, the Electronic Signatures in Global and National Commerce Act. I also want to thank our witnesses for coming to share their views on this legislation.

A few years ago, a lot of attention was focused on the use of the Internet as a means for expression and communication. We have seen the effects it has on the way students, teachers and everyday citizens share and use information. Similarly, in a relatively short period of time, the Internet has grown in importance as a major tool for conducting commerce. It has profoundly reshaped the traditional ways in which business is conducted both domestically and internationally. Therefore, it should come as no surprise that there would be increasing demands for more innovative and efficient ways for completing electronic commerce transactions using digital signatures or some other personal authentication devices, that are legally binding, without ever leaving the confines of your computer room. We have become a society that looks for and that wants convenience.

Today, our witnesses will testify on the merits of H.R. 1714. The intent of the legislation is to provide uniform national standards with respect to electronic signatures and their authentication because, for the most part, each state has their own set of guidelines in place. I would also like to thank Congresswoman Eshoo and Congressman Boucher for introducing legislation in this area as well. Although their bills differ from H.R. 1714, the underlying intent is the same. That is to prevent personal transactions that are completed by electronic signature mechanisms from being discriminated against because they were not done in a traditional way.

H.R. 1714 contains two provisions that I hope to hear more about. The first is that states will have two years in which to develop alternative electronic signatures policies and procedures in order for state statutes to supersede provisions within H.R. 1714. My concern is that some state legislatures don't meet as often for legislative business, in some cases once a year. The second issue is that the legislation gives the Secretary of Commerce the ability to enjoin legal proceedings if the Secretary believes state statutes violate the spirit of this bill. I hope Mr. Pincus will be able to share his views on this particular topic.

For the most part Mr. Chairman, I think this bill is a good piece of legislation. Clearly, this new era of telecommunications has affected the way we function as a society. We must be able to adapt to the new technologies being deployed to continue addressing the needs of our constituencies and to help further promote business.

Again, thank you Mr. Chairman for holding this hearing. I look forward to our witnesses' testimony.

Mr. TAUZIN. The Chair also wants to advise our distinguished panel today that your written statements are automatically part of our record. As I introduce you today I would ask you to please summarize those statements in a conversational fashion with us, by hitting the high points of your testimony, so we can do it within the 5-minute rule; then have time to enter into a dialog with you on your comments.

So we will begin by introducing this very distinguished panel, beginning with Mr. Andy Pincus, the General Counsel for the U.S. Department of Commerce. Mr. Pincus, you are now recognized to make your opening statement.

STATEMENTS OF ANDREW J. PINCUS, GENERAL COUNSEL, DEPARTMENT OF COMMERCE; DONALD W. UPSON, SECRETARY OF TECHNOLOGY, COMMONWEALTH OF VIRGINIA; JEFFREY SKOGEN, INTERNET MARKET MANAGER, FORD MOTOR CREDIT COMPANY; DANIEL GREENWOOD, DEPUTY GENERAL COUNSEL, INFORMATION TECHNOLOGY DIVISION, COMMONWEALTH OF MASSACHUSETTS; ARI ENGELBERG, PRESIDENT AND FOUNDER OF STAMPS.COM, INCORPORATED; JOHN E. SIEDLARZ, PRESIDENT AND CHIEF EXECUTIVE OFFICER, IRISCAN, INCORPORATED, ON BEHALF OF THE INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION; AND CHRISTOPHER T. CURTIS, ASSOCIATE GENERAL COUNSEL, CAPITAL ONE FINANCIAL CORPORATION

Mr. PINCUS. Thank you, Mr. Chairman. I am honored to appear before the subcommittee today.

As you and the other members of the subcommittee have mentioned, the Internet is revolutionizing every aspect of business, not just in our country, but throughout the world. These developments require the attention of governments to ensure that we are doing everything that we can to enable the development of this important new medium of commerce.

Chairman Bliley, Mr. Dingell, you, Mr. Chairman, and the other members of this committee clearly recognize this fact. You have taken a leadership role in ensuring that our country remains at the forefront in creating and exploiting the possibilities of electronic commerce. As other countries begin to recognize the potential of this new medium, we must continue to lead the way, not just in the private sector where we clearly are leading the way; but also in crafting the appropriate policy framework for these new developments. As we have in the past, the administration, and especially those of us at the Commerce Department, look forward to working with you on these important issues.

H.R. 1714 addresses a subject that is at the very core of enabling electronic commerce. It is obvious that e-commerce will grow only if parties' transactions over the Internet are just as legally binding as their transactions in the physical world. Although everyone hopes they will not have to end up in court and hire a lawyer, they obviously want to be sure that there is a way to hold the other party to the contract to their obligations, in case something does go wrong.

There are basically, as we see it, two issues in accomplishing this goal. First, eliminate statutory rules that require paper contracts. We obviously have to be sure that electronic agreements have the same legal status as paper contracts. The second question is when and how does an electronic contract become legally binding on the parties? In the physical world, the general rule is that the party has to manifest his or her intent to be bound. This can be done with a written signature; but it can also be done with an "X," or by an exchange of telegrams or various other means by which a court will conclude that there was an intent by both parties to be bound by the contract.

In the online environment, we advocate the same approach. There already are—and certainly, the way technology is evolving, there will be even more in the future—different ways to electroni-

cally sign a contract: everything from typing your name at the end of an e-mail and sending it, to using very sophisticated biometric or digital signature technology to evidence one's intent to be bound.

The market is in a very, very early state of evolving. It is clear that companies and individuals are using different types of authentication technology for different kinds of transactions, as they do in the physical world. We think it is very, very important to let that evolution take place and let the market continue to examine and test various forms of signature technology. In fact, last week I was privileged to participate in a workshop held in California by the OECD and the private sector that spent 2 days hearing presentations from various sectors—the manufacturing sector, the financial sector—on the kinds of signature technologies and the different business models that are being used to provide a legal basis for agreement in those sectors.

I think that we are in agreement on the basic principles that should govern the resolution of these two basic issues. First, as I said, eliminate barriers, paper contract requirements, and requirements of pen-and-ink signatures that are relics of an earlier age. Ensure technological neutrality, as several members of the subcommittee have said. It is very important that any legal rules that are adopted allow all these different technological approaches to have legal validity. Finally, be sure that parties are free to agree upon a means of authenticating their transactions; and if they do that, their subsequent agreements that are authenticated in that manner will be legally binding.

What we are seeing right now in electronic commerce is those kinds of systems where parties—auto companies and their suppliers, for example—set up an electronic structure for engaging in electronic ordering and electronic contracting and agree to use a particular technology for authentication. In order to allow those kinds of—what has come now to be known as—"closed systems" to develop, we have to be sure that they do create legally binding agreements.

We also agree that, as H.R. 1714 provides, there must be considerable attention paid to promoting these principles internationally. One of the most promising aspects of the Internet is its ability to facilitate cross-border transactions. It used to be that to be an exporter you had to be a big company and have agents all around the world to hawk your products. Now, all you need is a website and you will have access to every market in the world. Of course, we need international rules that will ensure that cross-border contracts that are made as a result of that access actually are legally enforceable.

As discussed in my written testimony, we have been working very hard on this issue. It is certainly useful to be sure that the entire U.S. Government, the administration, and the Congress, make clear to the rest of the world that these basic principles are important to us.

Domestically, as several members of the subcommittee have mentioned, we also need rules that implement these principles. This area of contract law has long been the province of the States. Through the uniform law process, the National Conference of Commissioners on Uniform State Laws has developed the Uniform Elec-

tronic Transactions Act, as a number of the members of the subcommittee mentioned; and plan to submit that act for adoption to the States at the end of July.

If we could wave a wand and have all 50 States enact that law, clearly the problem would be solved. We would have a very strong basis in domestic law for electronic commerce that meets all of our principles. There is concern, as you mentioned, Mr. Chairman, about the speed by which the States will adopt this. We don't think, right now, that there is evidence that the absence of uniform law is obstructing the growth of e-commerce. Although people have pointed to some differing laws, many of those laws only relate to government transactions. A lot of the States haven't spoken to the question of private commercial transactions. Certainly, at some point it may become true that the absence of a national standard is inhibiting domestic commerce. We need to create an environment that will encourage the States to move quickly to adopt the UETA. Our view is that the States should be given a chance to do that. If there is not quick action, it may then well be appropriate to establish some Federal rule to fill the gap until the States have adopted that measure.

Thank you very much, Mr. Chairman, I look forward to answering the subcommittee's questions.

[The prepared statement of Andrew J. Pincus follows:]

PREPARED STATEMENT OF ANDREW J. PINCUS, GENERAL COUNSEL, DEPARTMENT OF COMMERCE

Mr. Chairman, members of the Subcommittee, thank you for inviting me to testify today about H.R. 1714, the "Electronic Signatures in Global and National Commerce Act." As suggested in your letter inviting me to testify at this hearing, Mr. Chairman, my statement addresses the Administration's views concerning only titles I and II of the bill. Also, other agencies, including the Department of Justice, are reviewing this legislation and may have additional comments or concerns.

It is now an undeniable fact that the Internet is revolutionizing every aspect of business, not just in our country, but throughout the entire world. Although the amount of commerce conducted over the Internet is small as a percentage of our total economy, it is growing at a very rapid rate. In early 1998, experts estimated that Internet retailing might reach $7 billion by the year 2000. In all likelihood, this level was exceeded last year, and forecasters now project on-line retail sales greater than $40 billion by 2002. Similarly, in last year's Emerging Digital Economy Report, we noted that forecasters were suggesting that electronic commerce might rise to $300 billion by 2002. More forecasters now consider the estimate to be low, with Forrester Research estimating that all electronic commerce (including business-to-business activity) will rise to $1.3 trillion by 2003.

The *Framework for Global Electronic Commerce* issued by President Clinton and Vice President Gore in July 1997 pointed out that "[m]any businesses and consumers are still wary of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions." President Clinton directed Secretary Daley to "work with the private sector, State and local governments, and foreign governments to support the development, both domestically and internationally, of a uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide." The *Framework* identified several key principles to guide the drafting of these legal rules:

- parties should be free to order the contractual relationship between themselves as they see fit;
- rules should be technology-neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technology in the future);
- existing rules should be modified and new rules should be adopted only as necessary or substantially desirable to support the use of electronic technologies; and

- the process should involve the high-tech commercial sector as well as businesses that have not yet moved online.

The basic legal framework needed to enable electronic transactions in a commercial context consists of two essential elements. First is the elimination of statutory rules requiring paper contracts. There is a broad consensus that—with the exception of a few specialized agreements (wills and property deeds, for example)—parties' electronic agreements should have the same legal status as paper agreements.

The second element involves when and how an electronic commercial contract becomes legally binding on, and therefore enforceable in court against, a person or entity that is a party to the contract. In the off-line world, the key question is whether a party has manifested its intent to be bound by the contract, which generally occurs through a written record, and often, affixing a written signature to that written record. A signature, however, often is not a legal requirement (for example, a binding contract may be formed through an exchange of telegrams). The issue is, how can we apply and use long-standing commercial principles in connection with transactions in cyberspace?

As in the off-line world, there are a large variety of means by which a party may electronically evidence his agreement to the terms of a contract—what has come to be termed "electronic authentication." He could type his name at the end of an e-mail message containing the terms of the agreement. He could end the message with a previously agreed-upon code-word. He could end the message with an electronic facsimile of his written signature created by using an electronic stylus. He could "sign" the message using some form of digital signature technology. He could also "sign" the message using some form of biometric technology. Moreover, the technology models are evolving rapidly, and we will see further new technologies in the future. The private sector today is using a variety of forms of electronic authentication.

One other variable is important in understanding the legal standards governing electronic authentication. When electronic commerce was first beginning, some observers imagined a world in which everyone would have a single, universal digital identifier that would be used to authenticate each individual's electronic transactions. That would enable each individual to surf the Internet and enter into transactions with anyone he encountered, confident that the other party's digital identifier provided a legally valid means of identifying that party in the event the transaction ended up in court.

Although the future may see creation of both a market and the infrastructure needed for such as system to authenticate transactions, it does not exist now and is not likely to exist in the near term (and probably not even in the medium term). Most of today's electronic transactions occur in what are termed "closed systems"—systems in which parties that already are related in some manner conduct electronic transactions with each other pursuant to a system that the parties have agreed by contract or practice to utilize for that purpose. This model is reflected in sectors as diverse as manufacturing and banking and financial services where commercial parties establish the technological approach they will rely on, as well as the rules by which they will operate, assign risk and settle disputes. One example is the effort by the three major U.S. auto makers to develop on a unified basis a global system to tie product development together with more than 15,000 suppliers operating around the world. This Automotive Exchange Network will begin operating this fall. In a more traditional vein, the international network by which credit transactions are managed is predicated in large part on a series of agreements between banks and retailers, and by users. And, as a further example, the consortia of financial institutions that established Identrus enabled companies to conduct worldwide trusted business-to-business electronic commerce with any member of their network.

With this background, I would like to describe briefly what we in the Commerce Department have been doing over the last two years to carry out the President's directive to support creation of an appropriate legal framework for electronic commerce.

State law has long supplied the basic standards governing private commercial transactions within the United States. The National Conference of Commissioners of Uniform State Law (NCCUSL) has been working since early 1997 to adapt these legal standards to cyberspace by drafting a new model "Uniform Electronic Transactions Act" (UETA) to establish a predictable, minimalist framework to provide legal recognition to both electronic records and electronic signatures. The NCCUSL process involves broad consultation with legal experts and other interested parties, and permits observers to attend and participate in meetings of the drafting committees. As this Committee knows, NCCUSL's primary task is to determine which areas of the law would benefit from uniformity, and to write and recommend uniform laws to State legislatures for enactment. NCCUSL has written more than 200

uniform laws, including the Uniform Partnership Act, the Uniform Trade Secrets Act, the Uniform Probate Code, the Uniform Limited Partnership Act, and the well-known Uniform Commercial Code, a joint project with the American Law Institute. I understand that the UETA will receive final consideration at the NCCUSL Annual Meeting to be held at the end of July. If, as expected, the UETA is finally approved, it will be submitted to the States for adoption.

In our view, taking into account the principles that guide the Administration's policy in this area, the current UETA draft will provide an excellent domestic legal framework for electronic transactions, as well as a strong model for the rest of the world. It is enabling, not prescriptive, and also technologically neutral. We hope that this measure will be adopted quickly by the States.

The Government Paperwork Elimination Act passed by Congress last year addresses the appropriate balance to be struck by the Federal Government in selecting technologies for use in its communications with non-government entities and persons.

Let me turn to the international arena, where the situation is more complicated, and where our efforts focus on ensuring that our principles form the basis for enabling electronic commerce worldwide.

On the one hand, there is a broad consensus, reflected in the UNCITRAL Model Law on Electronic Commerce adopted in 1996, that communication of legally significant information in electronic form may be hindered by legal obstacles to the use of such data, or by uncertainty as to their legal effect or validity. The Model Law offers a set of internationally acceptable rules as to how such legal obstacles may be removed and a more secure legal environment may be created to facilitate electronic commerce across national borders. We are pleased that the U.S. efforts in the UETA are built on this international consensus.

On the other hand, with respect to electronic authentication, at least two different legal models are developing internationally. The first is the model represented by the UETA and the UNCITRAL Model Law, which eliminates barriers to electronic agreements and electronic signatures but does not grant special legal status to any particular type of authentication.

The second model provides for a greater degree of government regulation of authentication services. It allows a government to create a preference for one or more forms of electronic authentication by establishing specific technical requirements for electronic signatures and often providing a presumption that electronic contracts signed using that methodology are legally binding. The European Union's Electronic Signatures Directive, scheduled to be considered by the Parliament this fall, follows this approach.

Since July 1997, we have been consulting with countries to encourage their adoption of an approach to electronic authentication that will assure parties that their transactions will be recognized and enforced worldwide. Under this approach, countries would: (1) eliminate paper-based legal barriers to electronic transactions by implementing the relevant provisions of the 1996 UNCITRAL Model Law on Electronic Commerce; (2) reaffirm the rights of parties to determine for themselves the appropriate technological means of authenticating their transactions; (3) ensure any party the opportunity to prove in court that a particular authentication technique is sufficient to create a legally binding agreement; and (4) state that governments should treat technologies and providers of authentication services from other countries in a non-discriminatory manner.

We have been successful in encouraging the adoption of this approach in a variety of multilateral and bilateral contexts. In October 1998, the OECD Ministers approved a Declaration on Authentication for Electronic Commerce affirming these principles. In addition, we negotiated joint statements affirming these principles with several important trading partners, including France, Japan, Korea, Ireland, Australia and the United Kingdom. Further, we have asked UNCITRAL to consider a binding international convention on electronic transactions that would embody these principles. (A copy of this proposal is attached.)

Let me now turn to the provisions of H.R. 1714. Subsection (a) of Title II requires the Secretary of Commerce, acting through the Assistant Secretary for Communications and Information, within 90 days of enactment, to complete a comprehensive inquiry to identify, among other things, any domestic or foreign impediments to commerce in electronic signature products and sources. This study would be updated annually. Although such a study would provide useful information, we of course do not have sufficient resources to examine for ourselves the legal rules of every State and every country. If a study were authorized, therefore, we would base our report upon information obtained as a result of outreach to the private sector.

Title II also requires the Secretary of Commerce to promote internationally the acceptance and use of electronic signatures in accordance with principles spelled out

in section 201(b)(2). As I have discussed, we believe that the global nature of electronic commerce mandates close consultation with other countries to ensure that the legal standards for the formation of electronic contracts foster, rather than obstruct, cross-border electronic transactions. We plan to continue those efforts.

In general, the principles set forth in section 201(b)(2) are consistent with those that we have espoused with respect to these issues. We do have a few suggestions regarding the particular language of this section.

First, we are concerned that section 201(b)(2)(C), dealing with the autonomy of parties to electronic transactions, might be read to allow government regulation of such transactions, because the modifier "reasonable" could be read to permit government second-guessing of the parties' choice of authentication method. In addition, the paragraph does not clearly state that agreed-upon authentication measures must be given legal effect.

Second, because the fourth principle (section 201(b)(2)(D)) applies only where there is an agreement among the parties, it does not encompass the general principle that, even in the absence of an agreement, electronic records and electronic signatures should as a general matter have the same legal status as their paper equivalents.

Third, these principles apply with respect to the legal framework established by governments for private commercial transactions. But governments will also be making decisions concerning authentication technology as market participants—for example in selecting the particular technology to use in entering into government contracts electronically or in providing various types of government benefits to citizens. In that situation, governments will not be able to observe the neutrality principle set forth in section 201(b)(2)(B), because they will have to choose among competing authentication providers.

We would be happy to work with the Subcommittee on these and other drafting issues. Also, because the Commerce Department's current efforts with respect to these issues are led by the General Counsel's office, with support from several bureaus within the Department in addition to the National Telecommunications and Information Administration (NTIA), we request that any responsibilities conferred by the bill upon this agency be vested in the Secretary alone so that he may organize the Department's implementation of the law in the most effective and efficient manner possible.

Title I of the bill focuses on the domestic legal standards governing electronic contracts. It appears to extend to both government transactions (both Federal and State) and agreements between private entities. For such agreements, section 101 requires that agreements and signatures in electronic form be given the same legal effect as written agreements and written signatures. It would also enable the parties to establish "reasonable requirements" regarding the types of electronic records and electronic signatures acceptable to them.

With respect to private commercial agreements, as I have discussed, State law has long supplied the governing legal standards. Through the NCCUSL process, our commercial law has been made consistent nationwide and is the envy of the world. We believe that strong evidence of a problem should be required before casting aside this tried and true method for establishing the legal standards for commercial transactions.

We do not believe that the case has been made for overriding this State law process. Some have expressed concern about the current lack of uniformity among the States on these issues, but they have not been able to point to any real-world problems in this specific area that are currently obstructing the development of electronic commerce. Rather, the concern appears to be that at some point in the future, the absence of uniform legal standards for electronic authentication will create a problem.

The issuance of the UETA at the end of July responds directly to this concern. The States will then have the basis to adopt uniform rules. It is true that the State adoption process has in the past taken a number of years, but there is considerable eagerness among the States to foster the development of electronic commerce. Accordingly, there is reason to believe that adoption of this measure may proceed at a quicker-than-usual pace.

Of course, if the States do not act in a timely manner, problems could well develop and then it would become necessary to use Federal law to fill the gap created by less than unanimous enactment of the UETA. But I believe it is appropriate to work with the NCCUSL process to urge the States to act promptly and responsibly in this area, and to give the States time to act—before creating a new regime of Federal law.

Caution is also appropriate because enacting specific Federal rules may be a cure that is worse than the disease. As the UETA is adopted by the States, there may

be disputes about the extent to which it satisfies the Federal standard and the extent to which State law rules left undisturbed by the UETA are nonetheless invalid under section 101 or saved by section 102(a). Although H.R. 1714 does not create a private right of action, it presumably would permit any party in an action to enforce (or invalidate) an electronic contract to argue that section 101 overrides (or saves) the State law rules invoked by the other party. Rather than creating uniformity and certainty, therefore, Federal standards might compound the uncertainty over the governing legal rules.

We also have concerns about section 102(c), which would empower and require the Secretary of Commerce to bring actions to enjoin the enforcement of State statutes, regulations or rules prohibited by this Act. As a practical matter, the simple availability of this injunctive authority could undermine confidence in the validity of States' laws and regulations affecting electronic commerce, and significant use of this authority would cause additional uncertainty and delay in clarifying both State and federal laws in this area.

Let me also mention some specific concerns about the language of Title I.

First, section 101(b), which is designed to enable contractual systems, is limited to "reasonable" requirements established by the parties and therefore could lead to judicial second-guessing of the validity of an authentication method chosen by the parties. The provision also does not make clear that the type of electronic signature chosen by the parties should be accorded legal effect (as evidencing the intent of the parties to bind themselves to the terms of the contract).

Second, although section 102(a) allows the States to supersede the Federal rules, paragraph (a)(3) places a two-year time limit on their authority to do so. Given the rapidly evolving nature of the Internet, and of technology in general, we do not believe it would be appropriate to limit the States' power in this manner.

Third, section 102(b)(4) bars the States from superseding section 101 in a manner that "is otherwise inconsistent with the provisions of section 101." Because any State measure that is preempted by section 101 would be inconsistent with that provision, this paragraph of section 102(b) could be read to eliminate all State authority to supersede section 101.

Fourth, H.R. 1714's definition of "electronic signature" (section 104(2)) combines two separate concepts—the identity of a party to the transaction and that party's intention to be bound to the agreement, on one hand, and the integrity of the document on the other hand. The UETA separates these concepts (see the separate definitions of "electronic signature" and "security procedure"). This separation is important because, for example, some methods of "signing" do not, by themselves, ensure the integrity of the document (but may rely on other approaches for this function), and those technological methods would appear not to receive protection under the bill's definition, regardless of the intent of the parties.

Fifth, we are concerned about the effect of Title I on the ability of the Federal Government, and of State governments, to choose particular authentication methods for use in government contracting or in distributing government benefits. In making those decisions, there obviously will be rules, and perhaps statutes as well, that require the use of certain types of electronic authentication in order for the agreement to be binding. This problem could be solved by focusing Title I on government steps to enable private transactions and excluding government transactions from its scope.

Thank you Mr. Chairman. I would now be happy to answer any questions you may have.

DRAFT INTERNATIONAL CONVENTION ON ELECTRONIC TRANSACTIONS

CHAPTER I:

Proposed Goal of Chapter I: To set forth any necessary definitions. To be developed after Chapter II and III.

CHAPTER II:

Proposed Goal of Chapter II: In order to implement the legal rules articulated in the second section, as set forth below, it may be necessary for states to review their existing and proposed legislation to assure that it is appropriately tailored to electronic transactions. In order to facilitate such review and adoption on a harmonized basis, the following general obligations are proposed as the framework states should use to support electronic transactions on a global basis.

POSSIBLE LANGUAGE:

II. General Obligations

To encourage the free flow of electronic transactions and to avoid the creation of barriers to these transactions, subject to overriding public policy, the Contracting States hereby agree as follows:

- **Modification of Existing Rules and Minimal Adoption of New Rules**—States shall make only those changes to their laws that are necessary to support the use of electronic transactions. Existing rules should be modified and new rules adopted only in cooperation with the private sector and where necessary.

Contracting States recognize that parties to a transaction may determine the method of authentication for that transaction. Recognizing that parties may make this determination and recognizing that this determination should have the legal effect intended by the parties, the Contracting States agree as follows:

- **Party Autonomy**—Parties to a transaction should be permitted, to the maximum extent possible, to determine by contract the appropriate technological and business methods of authentication with the assurance that those means will be recognized as legally binding, whether or not those technological and business means are specifically addressed by legislation or regulation. The terms of any agreement (including closed systems) between parties governing their transaction should be enforced without regard to any statutory framework governing electronic authentication.

Further, Contracting States recognize that cryptography is not the sole means of proving the source or existence of a message. Recognizing that parties may establish the source or existence of a message in different ways, Contracting States agree as follows:

- **All Authentication Technologies and Business Methods May Be Evidence of Authenticity**—Where the law requires evidence of the authenticity or integrity of a message, a party shall be permitted to use any authentication technology or business method, whether or not such authentication technology or business method has been specifically addressed by legislation or regulation.

Electronic Authentication methods should not be "locked in" through legislative fiat but rather should allow for changing applications for existing and future technologies. Therefore, the Contracting States agree that:

- **Technology Neutrality**—Any rules should neither require nor hinder the use or development of authentication technologies. States should anticipate that authentication methods will change over time and avoid legislation that might preclude innovation or new applications. States should avoid laws that intentionally or unintentionally drive the private sector to adopt only one particular technology for electronic authentication to the exclusion of other viable authentication methods.

Authentication technologies may be implemented and used by businesses in ways that were not originally envisaged when legislation was passed. Recognizing that technology may be used for purposes such as establishing age or authority, which may go beyond verifying identity and achieving non-repudiation, and recognizing that business models for authentication may not use third parties, the Contracting States agree that:

- **Implementation Neutrality**—Any rules should neither require nor hinder the use or development of new or innovative business applications or implementation models.

To remove barriers to the free flow of electronic transactions and to avoid the creation of new barriers, subject to overriding public policy, the Contracting States agree that:

- **Non-Discrimination**—States shall accord to providers and users of authentication technologies and business methods of another state treatment no less favorable than it accords in like circumstances to its own providers and users of authentication technologies and business methods.
- **Avoid Unnecessary Barriers to Trade**—States should enhance the flow of cross-border electronic transactions and not create unnecessary barriers to trade.

CHAPTER III:

Proposed Goal of Chapter III: To recognize the acceptability of electronic signatures for legal and commercial purposes, define the characteristics of a valid electronic writing and an original document, support the admission of electronic evi-

dence and the electronic retention of records. These provisions would be drawn from the enabling provisions of the UNCITRAL Model Law on Electronic Commerce.

POSSIBLE LANGUAGE:

III. Specific Obligations

Contracting States recognize the work of the United Nations Commission on International Trade Law and the importance of establishing its governing provisions on a uniform, international basis. Contracting States also recognize information is increasingly generated, stored, sent, received or otherwise processed electronically, rather than in a paper based form. Recognizing these important business practices, the Contracting States hereby agree on the following:

- **Legal Recognition of Data Messages**
  Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message. [Source Model Law on Electronic Commerce Article 5]
- **Formation and Validity of Contracts**
  (1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.
  (2) The provisions of this article do not apply to the following . . . [limited exception]. [Source Model Law on Electronic Commerce Article 11]

Contracting States recognize that the formal requirements that currently exist under many legal regimes may constitute insurmountable barriers to the conduct of electronic transactions on an international basis. As a result, there is a paramount need for assuring that electronically transmitted messages are allowed to satisfy these formal requirements subject to overriding public policy. Therefore, the Contracting States agree as follows:

- **Writing**
  (1) 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.
  (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
  (3) The provisions of this article do not apply to the following . . . [limited exception]. [Source: Model Law on Electronic Commerce Article 6]
- **Signature**
  (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
    (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
    (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
  (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
  (3) The provisions of this article do not apply to the following . . . [limited exception]. [Source: Model Law on Electronic Commerce Article 7]
- **Original**
  (1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
    (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
    (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.
  (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
  (3) For the purposes of subparagraph (a) of paragraph (1):
    (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following . . . [limited exception]. [Source: Model Law on Electronic Commerce Article 8]

The Contracting States recognize that the inability of parties to prove the existence of electronic transactions in the event of dispute and formal judicial proceedings may itself be an inhibition to the conduct of electronic transactions. To assure the legal equivalence of electronic documents with paper based ones, the Contracting States agree that:

- **Admissibility and Evidential Weight of Data Messages**

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor. [Source: Model Law on Electronic Commerce Article 9]

Contracting States further recognize that requirements for record retention, which exist both as a matter of law and business practice, may prove to be obstacles for electronic transactions. The Contracting States agree, therefore, that:

- **Retention of Data Messages**

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy these requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions in subparagraphs (a), (b) and (c) of paragraph 1 are met. [Source: Model Law on Electronic Commerce Article 10]

Mr. TAUZIN. Thank you very much, Mr. Pincus. I was just thinking about how a handshake counts in some States, as well. You go to Texas; that is as good as a signature.

The Chair is now pleased to welcome the Hon. Donald Upson, the Secretary of Technology for the Commonwealth of Virginia, who has already been welcomed by the chairman of the full committee.

Secretary Upson, I might note that it would be good if you had a conversation with the Secretary of Transportation. I understand you had a little difficulty getting over here today. Many of us do every morning, trying to get to work. We appreciate and welcome your testimony.

STATEMENT OF DONALD W. UPSON

Mr. UPSON. Thank you, Mr. Chairman. I apologize for being late. I was stuck on 66. I am glad I am not the Secretary of Transportation.

Mr. Chairman, Chairman Bliley, and members of the committee, it is a special privilege to be here on behalf of Governor Gilmore and the Commonwealth of Virginia, and for me personally, to talk about this important legislation for two reasons.

First, you may not know I spent 13 years up here, most of which as Congressman Horton's staff director on government operations. Second, I have often wondered what it would be like to sit on this side of the table. Recalling some of your investigations, I have often preferred not to. It is a special privilege to be before this committee because I believe—and I know Governor Gilmore believes—that in terms of the technology environment for the United States, this committee has done far more than the general population appreciates in terms of setting that environment: the Telecommunications Act, the Internet Tax Freedom Act, and now digital signatures.

I would like to suggest that from Virginia's point of view, the action that you are taking in considering this legislation focuses on digital signature. But is more important than that; it is about commerce. It is about the United States and the competitive advantage we have in an electronic world. The legislation, in our point of view, reflects the U.S. global framework on Internet policy, which we endorse and include as part of our comprehensive Internet proposal. We focused upon the framework established at the Federal level, which generally suggested that the private sector should continue to lead. We should be very careful about imposing standards and restrictions on a medium that has just grown incredibly fast on its own and developed its own uniformity through market forces.

I am here to speak in support of H.R. 1714. First, it keeps the United States moving forward in terms of our competitive advantage by stating that where signatures are required in legally binding instruments, electronic signatures will satisfy that requirement. On the other hand, you give the contracting parties and the States the flexibility to enact standards amongst themselves that satisfy that basic fundamental requirement. This is important, we believe, for a significant reason; and that is if we impose technology standards, all of us know how quickly that technology changes. There are different levels of authentication required for different kinds of transactions. So I applaud the flexibility provided.

In Virginia, I would like to say these same principles guided the formulation of our current law on electronic signatures. Our law, simply stated, establishes the following; first, where any Virginia law requires a signature, or provides for certain consequences in the absence of a signature, that law is satisfied by an electronic signature. Second, electronic signatures must meet certain functional requirements. They must be unique to the signer; capable of verification; under the signer's sole control; linked to the record in such a manner that it can be determined that any data contained in the record was changed subsequent to the electronic signature being affixed; and created by a method appropriately reliable for the purposes for which the electronic signature was used.

We in the Commonwealth believe that our approach to electronic signature legislation allows the private sector to lead; avoids undue restrictions on electronic commerce; and establishes a simple, yet

enforceable set of functional requirements. That is what I think the legislation that you are considering before this committee does. I think it complements what is the beauty of this medium and the electronic environment. It is doing fine on its own; but the government, being an enabler—and not an imposer or an impeder—is important. I think it is reflective of the work in this legislation.

[The prepared statement of Donald W. Upson follows:]

PREPARED STATEMENT OF HON. DONALD W. UPSON, SECRETARY OF TECHNOLOGY, COMMONWEALTH OF VIRGINIA

Mr. Chairman and members of the Subcommittee, good morning. On behalf of Governor Gilmore and the Commonwealth of Virginia, I extend my appreciation for the opportunity to address members of Congress regarding the important topic of electronic commerce and, more specifically, the issue of electronic signatures.

Electronic commerce over the Internet is a centerpiece of the global information revolution. Virginia is the Internet capital of the world. In addition to being the birthplace of the Internet, almost half of the Internet backbone is in Virginia and nearly half of all online service subscribers are served by companies located in the Commonwealth. Accordingly, Virginia has taken the lead in establishing model policies that empower her citizens to reap the full benefit of technological opportunities like electronic commerce.

Because citizens are going on-line at an ever-increasing rate, electronic commerce is at once global, national and local in both scope and impact. Sound policy, at both the national and local level is essential for both the Internet and on-line commerce to reach their full potential. It is our hope that intelligent local policy will flow smoothly into sound federal policy, which in turn will cascade into a sensible global policy. However, inappropriate policy can be detrimental. I think this point is best illustrated by a quote from Governor Gilmore, who said, "Government can act in ways that will enhance this new technology, speed its development and growth, and encourage the fulfillment of its potential to improve our lives. Just as surely, it can erect roadblocks to progress that result in new ideas being left to atrophy and the stream of progress slowing to a stagnant pool."

We believe that the Commonwealth of Virginia is crafting the right local policy for Internet based commerce, a model of government facilitation of responsible industry and citizenry empowerment. Unlike other mediums, the Internet allows for an unprecedented amount of choice and control over use of the medium. Technology and market-based solutions can and should be used to address many of the concerns that have been brought on by technology and the market itself.

These solutions should be encouraged because they have the potential to exceed the effectiveness of traditional legal approaches. They are fueled by competition for "consumer satisfaction," which is at the heart of every business plan. As the profit motive drives companies to compete to provide better customer experience, it also sets off a race for better protections than traditional regulations would be likely to achieve. Whenever such traditional regulatory schemes are unavoidable, however, (i.e. where technology and market-based programs have been ineffective) we in the Commonwealth believe they should focus only on the responsible empowerment of citizens and industry.

Once again, our approach to electronic commerce in Virginia, to include electronic signatures, has not been the traditional "top-down" model that provides solutions dictated by government to industry, but more of a partnership with all the individuals and groups that have an interest in the creation of technology policy. Governor Gilmore believes in a "stakeholder" driven process that includes industry representatives as equal partners with government to address the complex issues that surround the Internet and electronic commerce. Our approach is based upon the inventive principles detailed in the 1997 U.S. "Framework for Global Electronic Commerce." As you know, this framework has been widely supported by industry.

It was with these five principles in mind that Virginia recently passed the most comprehensive Internet legislation in the country. In December 1998, Governor Gilmore's Commission on Information Technology issued a series of recommendations contained in a report entitled: "Toward A Comprehensive Internet Policy for the Commonwealth of Virginia." That report focussed on the expanding use of the Internet and electronic commerce in Virginia. The 1999 General Assembly adopted several pieces of legislation that, taken together, embody the Commission's recommendations for a Virginia Internet Policy Act.

These principles, which reflect the need for global cooperation spurred by technological and market-driven solutions, are as follows:

- **1. The private sector should lead.** Though government played a role in financing the initial development of the Internet, its expansion has been driven primarily by the private sector.
- **2. Governments should avoid undue restrictions on electronic commerce.** Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention.
- **3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.** In some areas, government agreements may prove necessary to facilitate electronic commerce and protect consumers. In these cases, governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation.
- **4. Governments should recognize the unique qualities of the Internet (and commerce over the Internet).** The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age. Finally, and maybe most importantly,
- **5. Electronic Commerce over the Internet should be facilitated on a global basis.** The Internet is emerging as a global marketplace. The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides.

Each one of these principles is reflected in the Virginia approach and the separate pieces of legislation and law that comprise our Internet Policy Act. For example, our encryption "resolution" law states that there should be no interference from government regarding the level of encryption businesses wish to employ to protect their property. Moreover, our laws regarding "spam" and "content" do not restrict any of our freedoms with undue government interference and regulation, but severely punish those individuals and groups for abusing the rights and privileges guaranteed by this medium and protects the growth of this form of commerce.

These same principles also guided the formulation of the current Virginia law on electronic signatures. Simply stated, that law establishes the following:

1. Where any Virginia law requires a signature, or provides for certain consequences in the absence of a signature, that law is satisfied by an electronic signature.
2. Electronic signatures must meet certain functional requirements. They must be: (a) unique to the signer; (b) capable of verification; (c) under the signer's sole control; (d) linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record; and, (e) created by a method appropriately reliable for the purpose for which the electronic signature was used.

We in the Commonwealth believe that our approach to electronic signature legislation: allows the private sector to lead; avoids undue restrictions on electronic commerce; and, establishes a simple yet enforceable set of functional requirements. Our approach does not discriminate in favor of or against any particular technology or company.

It is also clear that if electronic signatures are to become a convenient and widely used part of everyday business, for either the private sector or for government, we must simplify the means of authenticating digital certificates. If there are dozens of sources with which you must register your private key or must go to in order to authenticate a key provided to you, the process will be too cumbersome for many to participate in, and artificially expensive for the rest.

Virginia is moving to simplify the process for state government purposes and is headed in the direction of a central authentication source. While we are doing this, we must also look at what the proper role of (state) government is in facilitating or even providing a central source for authentication of certificates used in commerce and legal proceedings in Virginia.

Governor Gilmore plans to issue an executive order requiring my office, with the assistance of several other state agencies, to review available alternatives and recommend a plan to facilitate the use and authentication of electronic signatures by both the public and private sectors in the Commonwealth. We hope to achieve several results once our plan is fully implemented, including more efficient and expedi-

tious transactions between government, individuals and those businesses that contract with government. We also hope to raise consumer confidence through the use of electronic signatures in government transactions, such as renewing your driver's license on-line. Once the citizens of the Commonwealth are comfortable with these types of transactions, they will then feel more comfortable purchasing goods and services on the Internet in the private sector. Again, emphasis is on "facilitation."

With this important background in mind, I have reviewed the draft of H.R.1714 and offer these specific comments regarding the proposed legislation:

1. First, it is certainly prudent for members of Congress and the House Committee on Commerce to examine critical issues surrounding electronic commerce over the Internet. The Commerce Committee has always been at the forefront of technology issues, and has been especially effective under the leadership of its relatively new Chairman, Tom Bliley, and the Telecommunications Subcommittee Chairman, Billy Tauzin. One of the first, great achievements of this Committee under Chairman Bliley was enactment of telecommunications reform in 1996. Now, more Americans are going on-line in ever increasing numbers. They want to be able to conduct business over the Internet with confidence and peace of mind. Legislation, like H.R. 1714, which promotes that confidence, is most appropriate.
2. Second, national and international commerce has entered upon a sea change. The private sector of our economy is no less concerned than government with security issues surrounding the use of electronic commerce. I firmly believe that we must allow the market a chance to operate. We in the Commonwealth support the overall approach you have taken in H.R. 1714. The bill facilitates electronic commerce without placing undue restrictions on those who choose to do business on-line. It clearly supports the principles, contained in the 1997 U.S. "Framework for Global Electronic Commerce," that have guided our legislative efforts in Virginia.
3. Finally, I strongly support the requirement for continued inquiry and consultation regarding impediments to electronic commerce contained in H.R.1714. It is our plan in Virginia to monitor the implementation of Web-enabled government, including electronic commerce, through the establishment of a Web-based Commonwealth "best practices" center. The rapid evolution of this technology demands our full attention, so that we may continue to benefit from its use. At this time, I ask that I be permitted to offer one recommendation to the Electronic Signatures in Global and National Commerce Act, and that is the following: amend this draft legislation to include a provision establishing a national best practices center to further promote on-line commerce initiatives. It is my hope that Virginia will be able to work in consultation with the Secretary of Commerce to establish a similar Web-based center at the national level.

In closing, I would like to again thank you for the opportunity to present the Virginia perspective on the issues of electronic commerce and electronic signatures. We support what you are doing and stand ready to provide appropriate assistance.

Mr. TAUZIN. Thank you very much, Mr. Secretary.

The Chair would now interrupt the proceedings and ask you all to join with me in welcoming an honored guest who has arrived and will be honored at a luncheon later today. Mr. Yoshio Utsumi, the newly elected Secretary General of the International Telecommunications Union, is with us today. Mr. Utsumi, if you would be recognized. We all want to welcome you here today.

The Chair is now pleased to introduce and welcome for his testimony, Mr. Jeffrey Skogen, Internet Market Manager for Ford Motor Credit Department in Dearborn, Michigan. Jeffrey, if you would please summarize your statement for us.

STATEMENT OF JEFFREY SKOGEN

Mr. SKOGEN. Good morning, Mr. Chairman and members of the committee. I am Jeff Skogen, Internet Marketing Manager for Ford Motor Company in Dearborn, Michigan. I appreciate the opportunity to appear before the subcommittee.

The Ford Motor Credit Company is the world's largest company dedicated to automotive finance, with more than 8 million cus-

tomers in 36 countries. Ford Credit is continuously looking for ways to improve the value of its service that it delivers to its customers. Consumer power to choose and business' ability to meet consumers' and marketplace demands will be enhanced by the establishment of a reliable, trusted, cost-efficient flow of electronic commerce. For that reason, we are committed to harnessing the efficiencies that electronic commerce represents.

Electronic commerce is the exciting medium of business growth and consumer convenience. It is integral to the rapid development of a global, information-based economy that appears destined to coexist with the traditional industrial model. Electronic signatures are a fundamental building block for electronic commerce itself. They are the key to the widespread use and acceptance of electronic commerce. H.R. 1714 would facilitate transactions on the Internet and other electronic paperless transactions for dealer and consumer contracts by assuring that they are given the full legal validity of a written contract.

Our research shows that 57 percent of consumers in the market for a new vehicle within the next year prefer to research their automotive purchases online. Forty-four percent of consumers who use the Internet online services have visited a financial website. About one-third of the customers want to at least start the financing process online, according the Ford Credit's research.

Ford Credit has implemented a new credit-approval process called "Auto Apply," which customers can use to complete a credit application and securely send it to Ford Credit via the Internet. Ford Credit provides a decision online for the customer and their preferred dealer, usually within minutes of receiving the application at the company's website. While Ford Credit offers online approval through the dealers, its customers must still physically go to the dealership to sign the credit application and the contract. With the electronic signatures, the entire transaction could be handled online, making the process easier and more efficient for everyone involved.

In addition, we offer customer electronic funds transfer online, allowing them to enroll in the program; make a change, or cancel payments drawn directly from their checking account. Uniform standards for electronic signatures would enhance the public confidence in online applications of electronic commerce like electronic funds transfer.

We believe the United States should be actively involved in the development of uniform global standards for electronic signatures and commerce. The lack of uniform, nationwide rules may inhibit our country's ability to influence development beyond its borders. Therefore, it is appropriate to consider the establishment of a Federal standard or uniform guidelines.

I appreciate the opportunity to appear before you this morning. I will be happy to answer any of your questions.

[The prepared statement of Jeffrey Skogen follows:]

PREPARED STATEMENT OF JEFFREY SKOGEN, INTERNET MARKETING MANAGER, FORD MOTOR CREDIT COMPANY

Good morning, Mr. Chairman and members of the Subcommittee. I am Jeffrey Skogen, Internet Marketing Manager for Ford Motor Credit Company in Dearborn, Michigan. I appreciate the opportunity to appear before the Subcommittee. Ford

Motor Credit Company is the world's largest company dedicated to automotive finance with more the 8 million customers in 36 countries. Ford Credit is continuously seeking ways to improve the value of the services it delivers to customers. Consumers' power to choose and businesses' ability to meet consumer and marketplace demands will be enhanced by the establishment of a reliable, trusted, cost-efficient flow of electronic commerce. For that reason, we are committed to harnessing the efficiencies that electronic commerce represents.

Electronic commerce is the exciting medium for business growth and consumer convenience. It is integral to the rapid development of a global information-based economy that appears destined to coexist with the traditional industrial model. Electronic signatures are a fundamental building block for electronic commerce itself and they are the key to the widespread use and acceptance of electronic commerce.

H.R. 1714, the Electronic Signatures in Global and National Commerce Act, lays the foundation for nationwide acceptance of electronic signatures. H.R. 1714 begins the process of removing operational and legal obstacles to the broad-scale use of electronic commerce. In addition, the bill would promote the certainty necessary to conducting electronic commerce on a national and international basis.

The ability to establish binding legal contracts between unaffiliated parties is clear when the transaction is documented on paper or, in the alternative, where the parties conduct their transactions face to face. In these physical world environments, identities of the parties are invariably firmly established and certain. In the electronic marketplace, acceptance of electronically authenticated signatures in lieu of paper signatures is necessary; without it the transaction which was advertised, negotiated and agreed upon electronically still has to be "consummated" with a paper document.

This bill would facilitate transactions on the Internet and other electronic paperless transactions for dealer and consumer contracts by assuring that they are given the full legal validity of a written contract.

Our research shows that 57 percent of consumers in the market for a new vehicle within the next year prefer to research their automotive purchase online and 44 percent of consumers who use the Internet or online services have visited financial sites.

About one-third of customers want to at least start the financing process online, according to Ford Credit research. Ford Credit has implemented a new credit approval process—Auto Apply—which customers can use to complete a credit application and securely send it to Ford Credit via the Internet. Ford Credit provides a decision online for customers, and their preferred dealer, usually within minutes of receiving the application at the Company's web site.

While Ford Credit offers online credit approval through its dealers, its customers must still physically go to the dealership to sign the credit application and contract. With electronic signatures the entire transaction could be handled online making the process easier and more efficient for everyone involved. In addition, we offer our customers electronic funds transfer (EFT) online allowing them to enroll in the program, make changes or cancel payments drawn directly from their checking account. Uniform standards for electronic signatures would enhance public confidence in online applications of electronic commerce like EFT.

Technology neutrality is another necessary component of efficient electronic commerce. Recent advances in electronic and digital technology severely test the ability of government policymakers, regulators, and legislators to remain knowledgeable about the latest technology and its application. In addition, these rapid developments easily outdistance the traditional legislative and regulatory processes. Technology neutrality will serve to guard against regulations that quickly become outdated and impede the development of electronic commerce, both domestically and internationally.

We believe the United States should be actively involved in the development of uniform global standards for electronic signatures and commerce. The lack of uniform nationwide rules may inhibit our country's ability to influence developments beyond its borders. Therefore, it is appropriate to consider the establishment of a federal standard or uniform guidelines.

I appreciate the opportunity to have appeared before you this morning. I would be happy to answer any questions you may have. Thank you.

Mr. TAUZIN. Thank you very much, Mr. Skogen.

The Chair is now pleased to recognize Mr. Daniel Greenwood, Deputy General Counsel, Information Technology Division, Commonwealth of Massachusetts. I am sure if Mr. Markey were here, he would want to issue a special welcome to you, Mr. Greenwood.

STATEMENT OF DANIEL GREENWOOD

Mr. GREENWOOD. Thank you very much, Mr. Chairman and members of the subcommittee. On behalf of the Commonwealth of Massachusetts, I really do appreciate the opportunity to testify today on H.R. 1714, the Electronic Signatures in Global and National Commerce Act, "E-SIGN." I should probably depart from my remarks to indicate that you have won the important battle in this town of the best, all-time acronym for bills in this area: E-SIGN.

Mr. TAUZIN. That is an important title around here. We appreciate it.

Mr. GREENWOOD. It just rolls off the tongue—back to the merits for a moment.

To the extent that H.R. 1714 does facilitate a national baseline and a consistent legal infrastructure that supports electronic commerce without unduly disrupting related areas of State law, we believe that it does deserve very serious consideration; and it does deserve support. While we think the current language in certain sections ought to be looked at further, and the legislation should be honed to avoid some disruptions in related areas of State law; it does seem clear to us that the objectives of your legislation are wholly consistent with the Commonwealth's policy to assure a sound foundation for electronic commerce.

Last month, the Commonwealth went on record supporting the Abraham legislation in the Senate, S. 761, which by our lights supports very similar principles. It does set a minimum national framework.

When we are looking at legislation from a State perspective in Massachusetts, and evaluating whether or not it really should succeed from a preemption perspective and from a perspective of supporting e-commerce and commercial law generally; we ask these types of questions: is the legislation narrowly tailored to address existing and well-understood market failures, or failures in law? In other words, is it minimalist? Is it doing only what is necessary to right a wrong, or to facilitate a place where the free market—or at least our existing market system—is not operating optimally?

Does it promote a competitive marketplace for different technologies? This has been mentioned a couple of times today. Locking into a single technology for authentication or electronic records, in our view, is not generally a good idea. Federal legislation can have a negative effect by distorting the market.

We also ask whether it includes any new or expanded regulation, or other government intervention; including a legislatively created accreditation, or some other government approval or control that is necessary for technology providers or users. It is our view that, especially in the e-commerce area, we are looking at an economic sector that is quite decentralized. It is almost self-organizing and distributed, the way that it is put together. Therefore, legislation that centralizes the market players for the purpose of controlling and regulating them is a bad idea.

Finally, does the legislation disrupt other bodies of law? Does it unduly preempt State jurisdiction? This is what I would like to talk about in a little bit more detail. We think there are compelling arguments that favor generally keeping governance of commerce under State jurisdiction, where it primarily exists today under the

Uniform Commercial Code and related law. The provided law is sufficiently harmonized so as not to present undue barriers to interstate commerce. We think generally States are more agile. We are somewhat smaller. We can react somewhat more quickly to changing market conditions and that is going to be particularly important in this e-commerce space.

However, there are certainly cases where the national interest requires that Federal action does preempt State law. This has long been accepted when States create undue impediments to interstate commerce. The fact that—as has been noted this morning, many times, so far—we have enacted so many different laws governing electronic signatures and records has clearly been a contributor to the current efforts for Federal action.

If States were to quickly pass uniform law in this area, we believe that it is likely that the legitimate private-sector interests in a national baseline would be satisfied. It would be satisfied through the uniform law process. We think, in the end, this is the preferred method of creating a baseline. The draft Uniform Electronic Transactions Act, which Andy Pincus had mentioned, represents at this point the single best, most-comprehensive, legislative effort to date. It causes no serious legal disruptions in other areas of law. It comprehensively deals with many issues about contract formation, contract interpretation, and notice requirements—all of the secondary and third-level issues that are implicated when one lists legal barriers to using electronic records.

There are many interdependencies with many areas of law. These people have done a very good job through a multi-year, open process, with a lot of State law experts in the public sector and the private sector deliberately going through all of these interrelated areas of law and crafting a very good, comprehensive act.

We have a problem in the timing, which has been pointed out very convincingly, I think, by advocates for the private sector. They need legal reform soon. I think the objectives of the legislation today, H.R. 1714, are evidently crafted to satisfy the legitimate interests of industry to come with some baseline quicker as we wait for uniform law to evolve. Looking at the criteria I mentioned, the bill really can directly satisfy the industry needs without disrupting these other policy concerns.

I would request the privilege to add an addendum to my remarks within 30 days, under House rules, for the purpose of providing some more detailed comments on some the precise provisions of the current language as they relate to some of these other areas of State law and to the emerging Uniform Electronic Transactions Act.

Mr. SHIMKUS [presiding]. There is no one here to object, so I will let you do it. How about that?

Mr. GREENWOOD. Thank you, sir. The long and short of it is we support the principles that appear to underlie this legislation. We would look forward for an opportunity to continue to offer any service or assistance we can to this committee and the other committees that are working on the legislation as you try to work through the very complicated issues with State law.

Thank you, again, for the opportunity to testify today.

[The prepared statement of Daniel Greenwood follows:]

PREPARED STATEMENT OF DANIEL GREENWOOD DEPUTY GENERAL COUNSEL FOR THE INFORMATION TECHNOLOGY DIVISION, COMMONWEALTH OF MASSACHUSETTS

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 indi-

cates 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.

Mr. SHIMKUS. Thank you.

Our next witness is Mr. Ari Engelberg, Vice President of Strategic Web Development, Stamps.Com. Of course, your written statement is in the record. You may summarize for 5 minutes. Welcome.

STATEMENT OF ARI ENGELBERG

Mr. ENGELBERG. Mr. Chairman and members of the subcommittee, my name is Ari Engelberg. I am a founder of an Internet company called Stamps.Com. Stamps.Com, working in conjunction with the Information Based Indicium program at the United States Postal Service, has developed an exciting mainstream application of digital signature technology. I thought I would use my few minutes here this morning to tell you about a little bit about how our technology works and how it relates to this bill.

What we are is one of the first companies to develop an e-commerce system that enables individuals and businesses to purchase and print U.S. postage over the Internet using nothing more than an ordinary laser or ink-jet printer. Our service is a simple one. Users download a small piece of software from our website, or from the website of one our partners. After a short registration process, which includes U.S. Postal Service meter licensing, users may purchase postage through a variety of payment methods including wire transfers and credit or debit cards. The postage payment is then transferred directly to the Postal Service.

To print postage, users log onto their accounts on our postage servers over an encrypted link and designate a delivery address. The postage servers then perform a variety of functions. The user's postage balance is debited by the appropriate amount. Spelling and zip-code mistakes in the address are corrected by a national address data base to ensure higher address quality and more efficient mail piece routing through pre-barcoding. Most importantly, a digital signature is generated for each stamp, using a cryptographic key unique to each user. The digital signature is then sent back across the link to the user's P.C., where it is encoded in a two-dimensional barcode. This barcode is the security-critical portion of the Postal Service's new Information Based Indicium.

Each of you has in front of you an envelope which is adorned with Internet postage. That is live postage and you may take that back and mail it back to your district office. The barcode on the envelope can be scanned using a hand-held or a stationary device. Through a system that connects the cryptographic keys generated by our postage service to a certificate authority maintained by the Postal Service, the authenticity of a given stamp can be ascertained.

This system provides tremendous advantage to users. Postage is available 24 hours a day, 7 days a week from the desktop. Addresses are corrected by our data base to increase delivery reliability. Postage can be printed from within the word processors and personal information managers upon which so many small business professionals already rely. By transforming what was once a product—postage meters, into a service—Internet postage; Stamps.Com has fundamentally altered cost structures in this industry, making postage convenience more affordable to a broader share of the business and consumer population than traditional postage meters.

The enterprise comprises one of the most complex, highly secure electronic commerce systems ever developed. It has been 2½ years in the making. Our system involves sophisticated cryptography, advanced data center operations, and secure financial transactions. The advantages of this advanced system are enabled by the security of the Information Based Indicium, and the security of a strong digital signature as a means of authentication of postage value.

H.R. 1714 provides a welcome legislative foundation for furthering e-commerce by explicitly legitimizing electronic signatures as proof of contract acceptance. For the purposes of this discussion, each or indicium, or stamp, is a micro-contract authenticated by the electronic signature between Stamps.Com, the Post Office, and the customer. That is; if the customer uses Stamps.Com to pay for and print U.S. postage, the Post Office will deliver the mail. This contract, and the opportunity to offer this service, is made possible by the integrity, authenticity, and non-reputability of a strong digital signature.

Thus, Stamps.Com strongly supports H.R. 1714. Thank you for the opportunity to testify.

[The prepared statement of Ari Engelberg follows:]

PREPARED STATEMENT OF ARI ENGELBERG, FOUNDER, STAMPS.COM, INC.

Mr. Chairman, Members of the Subcommittee: My name is Ari Engelberg. I am a founder of an Internet company called Stamps.com. Stamps.com is one of the first companies to develop an e-commerce system that enables individuals and businesses to purchase and print US postage over the Internet using nothing more than an ordinary laser or inkjet printer. Two and a half years ago, Stamps.com was founded upon the promise—and reality—of electronic commerce. Indeed, we have developed one of the few e-commerce applications to make possible the purchase and delivery of a product—in our case US postage—entirely online: the payment and service are bits; the inventory and shipment, ones and zeroes.

Our service is a simple one. Users download a small piece of software from our web site, or the web site of one of our partners. After a short registration process, which includes US Postal Service licensing, users may purchase postage through a variety of payment methods including wire transfers and credit or debit cards. The postage payment is transferred directly to the Postal Service

To print postage, users login to their accounts on our Postage Servers over an encrypted link and designate a delivery address. The Postage Servers then perform a variety of functions:

The user's postage balance is debited by the appropriate amount. Spelling and ZIP Code mistakes in the address are corrected by a national address database to ensure higher address quality and more efficient mailpiece routing through pre-barcoding. And, most importantly, a digital signature is generated for each stamp using a cryptographic key unique to each user. The digital signature is then sent back across the link to the user's PC, where it is encoded in a two-dimensional barcode. This barcode is the security-critical portion of the Postal Service's new Information Based Indicium. It can be scanned using hand-held or stationary devices, and through a system that connects the cryptographic keys generated by our Postage Servers to a Certificate Authority maintained by the Postal Service, the authenticity of a given stamp can be ascertained.

The system provides tremendous advantage to users. Postage is available 24 hours a day, 7 days a week from the desktop. Addresses are corrected by our database to increase delivery reliability. Postage can be printed from within the word processors and personal information managers upon which so many small business professionals already rely. And, by transforming what was once a product (postage meters) into a service (Internet Postage), Stamps.com has fundamentally altered cost structures in this industry, making postage convenience more affordable to a broader share of the business and consumer population than traditional postage meters.

The enterprise comprises one of the most complex, highly secure electronic commerce systems ever developed and has been two and a half years in the making. Our system involves sophisticated cryptography, advanced data center operations, and secure financial transactions. The advantages of this advanced system are enabled by the security of the Information Based Indicium, by the security of a strong digital signature as a means of authentication of postage value.

However, while digital signature technology affords Stamps.com and companies like ours the opportunity to take advantage of the efficiencies and immediacy of ecommerce, it also imparts upon us a responsibility towards our customers and partners, a responsibility to secure each and every transaction against mistake or misuse.

H.R. 1714 provides a welcome legislative foundation for furthering ecommerce by explicitly legitimizing electronic signatures as proof of contract acceptance. In its current form, however, H.R. 1714 leaves open a prospect for abuse. While H.R. 1714 aims to achieve vendor-neutrality, in the world of ecommerce not all algorithms are created equal.

In Stamps.com's business, electronic signature technology ensures that each indicium is unique and cannot be created fraudulently. Moreover, it ensures that each indicium cannot be hacked or spoofed or electronically replayed—all favorite tools of electronic criminals. For purposes of this discussion, each indicium is a micro-contract, authenticated by the electronic signature, between Stamps.com, the Post Office, and the customer. That is, if the customer uses Stamps.com to pay for and print US Postage, the Post Office will deliver the mail.

The Stamps.com application was developed using published and government-approved encryption standards. Sound encryption requires years of open testing to expose and remedy flaws. For that reason, the government has issued standards for a variety of encryption and digital signature algorithms, the Federal Information Processing Standards. These standards provide a base-level of protection that the private sector often uses or exceeds. H.R. 1714 provides for no base-level of protection and potentially leaves open the exploitation of contracting parties with little or no experience with relatively complex technical issues. If companies are allowed to choose any "reasonable" method, they may choose one that is weak enough to be attacked and exploited to falsify contract acceptance. Furthermore, any algorithm, no matter how tried-and-true, is susceptible to failure if implemented incorrectly. Thus, it is my company's belief that H.R. 1714 should contain some reference to the fact that not all electronic signature methods are "reasonable" and that parties should be encouraged to investigate and choose electronic signature methods that meet their specific needs for security and ease of use.

Thank you for the opportunity to speak before this Committee.

Mr. SHIMKUS. Thank you.

Our next panelist is Mr. John Siedlarz.

Before I do that, I want ask unanimous consent that we give all witnesses 30 days to include any—obviously, I am not going to object. You will get questions, probably, that members may ask you to respond to in writing. Without objection, I request unanimous

consent for 30 days for that response to be received for the official record.

And, now, the next panelist, Mr. John Siedlarz, President and CEO of IriScan, Incorporated. Welcome. You have 5 minutes.

STATEMENT OF JOHN E. SIEDLARZ

Mr. SIEDLARZ. Thank you, Mr. Chairman. Good morning, Mr. Chairman and members of the committee.

Mr. SHIMKUS. Pull that mike closer to you. Thank you.

Mr. SIEDLARZ. In addition to being president of IriScan, I am also the vice chairman of the International Biometric Industry Association. The Association very much appreciates the opportunity to speak to you today and comment on H.R. 1714.

As one example of the technologies that are covered by the Association, IriScan—my company—develops a leading biometric product that identifies and authenticates individuals through the unique iris pattern of the eye, the visible colored ring surrounding the pupil.

I wanted to pass this on to Chairman Tauzin on his comment about dogs. Not only can we make a sharp distinction between humans—an absolutely positive one; but we can tell the difference between a dog and human. We will shortly be able to be in the position of being able to tell the difference between the dogs that are on the Internet.

I would appreciate it if you would convey that to him.

The IBIA is a trade association that represents many technologies, and the interests of the biometric industry as a whole. It includes groups of proven technologies that identify or verify individuals based on physiological characteristics. In other words, what you are; not what you hold or what you do—a very important distinction that I would like to focus on later in comparing how you use biometrics with an encryption for a more secure transaction.

Biometric identification and verification are accomplished by using computer technology in non-invasive ways to match patters of live individuals in real time against enrolled records. Examples include products that recognize faces, hands, fingers, signatures, irises, voices, and fingerprints. Biometrics are most commonly used to safeguard international borders; protect computer network security; control access to sensitive work sites; authenticate financial transactions; verify time and attendance; prevent benefits fraud, and provide secure transactions on the Internet. Biometrics, in sum, are excellent means to secure privacy and prevent identity theft.

IBIA supports H.R. 1714 and the efforts of Chairman Bliley and the committee to move this legislation forward. We specifically endorse the attempt to make sure that the technology is essentially neutrally identified, as far as the legislation concerned. Our only argument with the bill—and it is a very small one—is in the language in section 104, which defines an electronic signature as, "A signature in an electronic form." We think that it is appropriate to have that language broadened slightly, maintaining the focus on neutral technology approaches in the legislation; and be consistent with what the Senate dealt with in S. 2107, the Government Paperwork Elimination Act, last year. Based on testimony from ex-

pert witnesses, the Senate chose to strike language that would favor a digital signature; and instead substituted the technology-neutral phrase, "electronic authentication."

The specific reason for this action was to avoid a constricted definition that would have the combined effects of unnecessarily restricting the market for biometric products; creating a competitive advantage for a small group of solutions; and freezing options for substituting newer technologies as they are perfected.

Once again, we wanted to emphasize that in our view, the growing recognition among the community is that the combination of encrypted data and biometrics at either end of the transaction, in effect, provide the only means of a secure solution for transactions on the Net. Biometrics cannot do that by themselves. Encrypted data cannot do it by itself. It is the combination of those two technologies which, I think, is being recognized. I think this bill ultimately supports that in its technology-neutral language.

The IBIA strongly encourages the committee to take a similar approach to the action in the Senate. This can be accomplished by rewording the first part of the definition contained in section 104[2] to read as follows, "Electronic signature. The term "electronic signature" means a biometric or other sequence of data in electronic form." This change would ensure that the bill does not rule out the use of sound biometric authentication solutions that have been specifically designed to accomplish the purpose of the bill.

The IBIA thanks both subcommittees for this opportunity to express its views in supporting H.R. 1714. I would welcome your questions about biometric technologies and their relevance to this important bill. Thank you, Mr. Chairman.

[The prepared statement of John E. Siedlarz follows:]

PREPARED STATEMENT OF JOHN E. SIEDLARZ, PRESIDENT AND CHIEF EXECUTIVE OFFICER, IRISCAN, INC., ON BEHALF OF THE INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION

My name is John Siedlarz. I am President and Chief Executive Officer of IriScan, headquartered in Marlton, New Jersey. I am also Vice Chairman and a member of the Board of Directors of the International Biometric Industry Association (IBIA). IBIA very much appreciates the opportunity to testify before you today.

IriScan develops a leading biometric product that identifies and authenticates individuals through the unique iris pattern of the eye—the visible colored ring surrounding the pupil.

IBIA is a trade association that represents the interests of the biometric industry as a whole. Biometrics include a group of proven technologies that identify or verify individuals based on physiological characteristics. Biometric identification and verification are accomplished by using computer technology in noninvasive ways to match patterns of live individuals in real time against enrolled records. Examples include products that recognize faces, hands, fingers, signatures, irises or irides, voices, and fingerprints. Biometrics are most commonly used to safeguard international borders, protect computer network security, control access to sensitive work sites, authenticate financial transactions, verify time and attendance, and prevent benefits fraud. Biometrics, in sum, are excellent means to secure privacy and prevent identity theft.

IBIA supports the intent of Chairman Bliley and his co-sponsors to recognize the economic potential of e-commerce, and to update our laws to specify how electronic documents can be properly authenticated in the digital age. We believe that Chairman Bliley's bill, H.R. 1714, "The Electronic Signatures in Global and National Commerce Act," would both encourage and protect the use of electronic records in national and international commerce. This is an essential step toward automating cumbersome processes that can otherwise hinder trade and stifle economic growth. If the bill became law, complex and highly confidential transactions in banking, real

estate, securities, and retail sales, in particular, will be quicker, far more secure, and much more efficient.

The biometric industry has one concern about the bill—the wording of Section 104, which defines an "electronic signature" as "a signature in electronic form." This definition could be construed to mean that only a limited range of signature-based technologies are acceptable.

Last year, the Senate dealt with this same issue while deliberating the provisions of S. 2107, "The Government Paperwork Elimination Act." Based on testimony from expert witnesses, the Senate chose to strike language that would favor a "digital signature," and instead substituted the technology-neutral phrase, "electronic authentication." The specific reason for this action was to avoid a constricted definition that would have the combined effects of unnecessarily restricting the market for biometric products, creating a competitive advantage for a small group of solutions, and freezing options for substituting newer technologies as they are perfected.

The IBIA strongly encourages you to take a similar approach. This can be accomplished by rewording the first part of the definition contained in Section 104 (2) to read as follows:

> "ELECTRONIC SIGNATURE—The term 'electronic signature' means *a biometric or other sequence of data* in electronic form, attached to or logically associated with an electronic record, that . . ."

This change would ensure that the bill does not rule out the use of sound biometric authentication solutions that have been specifically designed to accomplish the purpose of this bill.

The International Biometric Industry Association thanks both subcommittees for this opportunity to express its views about H.R. 1714. I would welcome your questions about biometric technologies and their relevance to this important bill.

Mr. TAUZIN. Thank you very much, Mr. Siedlarz. I understand you made the case for identifying dogs?

Mr. SIEDLARZ. I have, indeed.

Mr. TAUZIN. My wife would contest that, by the way. She thinks our dogs are humans, so that would be a problem.

We are pleased now to welcome Mr. Christopher Curtis, Associate General Counsel of Capital One, here in Falls Church, Virginia. Welcome, Mr. Curtis.

STATEMENT OF CHRISTOPHER T. CURTIS

Mr. CURTIS. Good morning. I am Christopher Curtis, Associate General Counsel of Capital One Financial Corporation. I appreciate the opportunity to testify today in support of H.R. 1714.

Capital One is one of the world's largest issuer of credit cards, and a direct marketer of consumer and small business lending products. We are also a pioneer in the direct marketing of wireless telephone service through our subsidiary, America One Communications.

On behalf of Capital One, I would like to thank the subcommittee for considering this legislation. I hope you will report favorably on it. The world of online commerce is exploding all around us, offering more efficient commerce, and hence, greater wealth for all Americans. However, further development of electronic commerce may be impeded by the issue of online authentication: the means by which one party, such as a merchant or financial institution knows who it is dealing with; as well as the issue of online signature: a means by which a party legally binds itself to a transaction. Without resolution of those issues, we fear that parties will be reluctant to enter into larger transactions with numerous and remote counter-parties.

I will refrain from any technical discussion of the electronic signature technologies currently available. Instead, I want to endorse what I see as the two basic principles of this legislation. First, the

bill establishes a national principle of recognition of electronic signatures. Second, the bill rejects any prescribed technical standard and instead allows the marketplace to decide what technologies are best.

By establishing a uniform rule of recognition, the bill provides what we see as the keystone in a sound legal architecture for electronic commerce. In the current chaotic legal environment, the validity of electronic transactions is governed by the law of each State. A number of States have moved to recognize electronic documents and signatures, but not in a consistent manner. Electronic signatures that are valid in one State may not be valid in another State. Moreover, some States still don't recognize electronic signatures at all. While there is the uniform State process which is underway, as has been discussed this morning, we know that may take a long time, and may not in the end, in fact, result in a uniform product. Sometimes the uniform process does not.

As a result of the current situation, individuals and companies doing business on the Internet face considerable uncertainty as to the enforceability of their transactions. There is a significant concern that a party to an agreement can simply deny making the agreement. The ability to do so opens the door to fraud in electronic commerce and hinders growth in this medium. We will never achieve the full potential of electronic commerce until agreements entered into on the Internet are valid and enforceable.

We also support the bill's principle of free development of electronic signature technology. This will allow the market, not the government, to determine the desirability of a specific technology. We at Capital One would not presume to tell you what electronic signature technology is best. Even if we could, what is best today may not be best 5 years now, 10 years from now, or even 1 year from now. The proposed legislation takes the right approach by insisting that those issues be left to human ingenuity as tempered in the marketplace.

In conclusion, Capital One strongly supports the enactment of H.R. 1714. We believe it provides the best legal basis for unleashing the Internet's potential to transform commerce. We are grateful for the leadership of Chairman Bliley in introducing this legislation; and to the subcommittee for considering it. Thank you for the opportunity to testify before you today.

[The prepared statement of Christopher T. Curtis follows:]

PREPARED STATEMENT OF CHRISTOPHER T. CURTIS, CAPITAL ONE FINANCIAL CORPORATION

Mr. Chairman and Members of this Subcommittee, my name is Christopher Curtis. I am Associate General Counsel of Capital One Financial Corporation, headquartered in Falls Church, Virginia. I appreciate the opportunity to testify today on H.R. 1714, the Electronic Signatures in Global and National Commerce Act. The subject of electronic signatures is an important one to Capital One, to the national economy, and, we think, to the world.

First, a word about Capital One. Through our subsidiary credit card bank and thrift, we are one of the world's largest issuers of credit cards and a direct marketer of consumer and small business lending products. We are also a pioneer in the direct marketing of wireless telephone service through our subsidiary, America One Communications, Inc.

As of March 31, 1999, Capital One had $17.4 billion in managed loans outstanding and over 18 million customers in the United States, Canada and the United

Kingdom. We have over 12,000 employees based in Virginia, Texas, Florida, Washington State, Massachusetts, and the United Kingdom.

In each of the last four years, Capital One surpassed its goals of achieving annual earnings growth and annual return on equity of at least 20% and is on track to surpass that goal this year as well. In 1998 alone, we added nearly 5 million net new customers and are currently adding new customers at the rate of 15,000 net new accounts a day. To support that account growth, our Company hired 4,500 new employees during 1998 and expects to hire at least 3,500 additional employees in 1999 across all of our sites.

On behalf of Capital One, I want to thank the Subcommittee for considering the legislation that is before you today, and I hope that you report favorably upon it. The world of on-line commerce is exploding all around us. Its capacity for enabling more efficient commerce and hence greater wealth for all Americans, as well as residents of other nations, is so large that it cannot be quantified and can scarcely even be envisioned. Significant burdens to further development of electronic commerce, however, are the issues of on-line authentication—the means by which one party, such as a merchant or a financial institution, knows who it is dealing with—and on-line signature, a shorthand expression for a party's legally and formally binding itself to a transaction. Without resolution of those issues, parties will be reluctant to enter into larger transactions with more numerous and remote counterparties. Their reluctance will be grounded in practical concerns about fraud, and also about the risk that a counterparty could disavow a transaction under a state's statute of fraud or related legislation or doctrines.

I will refrain from any technical discussion of the electronic signature technologies currently available—indeed, one of the virtues of the proposed legislation, as I will describe in a moment, is that it rejects any prescribed technical standard or approach to the problems of on-line authentication and signature—but instead discuss what I see as the two basic principles of the legislation, both of which Capital One strongly supports.

They are, first, the establishment of a national principle of recognition of electronic signatures; and second, the adoption of what we at Capital One call an "open platform" approach to technology, allowing the marketplace to decide what technologies are best. I will discuss those two principles in order.

National Recognition

The proposed legislation takes the essential step of establishing a uniform rule of recognition, which we see as the keystone in a sound legal infrastructure for electronic commerce. The current legal environment, in which the validity of electronic transactions is governed by state law, can fairly be described as chaotic. While a number of states have moved to recognize electronic documents and signatures, states have not done so in a consistent manner. Valid electronic signatures in one state may not be valid in another state. Moreover, some states still do not recognize electronic signatures at all. As a result, individuals and companies doing business on the Internet face considerable uncertainty as to the enforceability of electronic transactions.

In fact, the single biggest problem that parties face in conducting business on the Internet is that of repudiation. Under the current environment, there is a significant concern that a party to an agreement can simply deny making the agreement. The potential ability to repudiate an electronic agreement opens the door to fraud in electronic commerce and hinders growth in this medium. Ultimately, we will be unable to achieve the full potential of electronic commerce until agreements entered into on the Internet are valid and enforceable. While those issues are also present in that older medium of paperless remote commerce—the telephone—Internet commerce, because of its greater speed, power, and flexibility, offers immensely greater opportunities for abuse and fraud.

This problem cannot be adequately addressed at the state level because of the inconsistencies in state law. Currently, state law determines whether or not there was an enforceable contract and whether that contract was valid. This creates significant uncertainty for Internet transactions. For example, imagine a scenario in which Capital One, a Virginia company, maintains a web site on a server in our facilities in Texas and enters into an electronic contract with an individual residing in California. In determining whether the contract is valid, it is not clear which state's law applies. Thus, in order to ensure that an individual or a company is entering into an enforceable transaction, a company or a consumer doing business across the country may need to comply with the different, and possibly conflicting, laws of a number of different states depending on where the other parties to the transaction are legally located. As a practical matter, this uncertainty and duplication will increase the cost of doing business electronically as individuals and businesses seek

to comply with the laws of all fifty states and other relevant jurisdictions or simply forego electronic commerce at levels that they would otherwise find desirable.

Open Platform

We also support the bill's open-platform approach to electronic signature technology. By permitting a number of different technologies that meet minimum standards to qualify as electronic signatures, the bill will foster technological innovation. A number of different signature technologies, including promising new technologies, may easily be incorporated into the legal framework established by this bill. This will allow the market, and not government, to determine the viability and desirability of a specific technology. An open environment will also keep the cost of electronic signature technology in check by allowing a number of competing technologies to emerge in the market without bestowing a monopoly on a single company or technology. We at Capital One would not presume to tell you what electronic signature technology is best; and even if we could, what is best today may not be best five years from now or ten years from now—or even one year from now. The proposed legislation takes the right approach by insisting that those issues be left to human ingenuity, as tempered in the marketplace.

Conclusion

In conclusion, Mr. Chairman and members of the Subcommittee, we at Capital One strongly support the enactment of H.R. 1714. We believe that it provides the best legal basis for fostering electronic commerce and unleashing the Internet's potential to transform our economy and the world's. We are grateful for the leadership of Chairman Bliley, the original motive force behind this legislation, and we commend the Subcommittee for its consideration of it. Thank you for the opportunity to testify.

Mr. TAUZIN. Thank you very much, sir.

The Chair now recognizes himself for 5 minutes, and members, in order.

First of all, Mr. Pincus, you are aware, of course, of the July 1997 German Digital Signature Law that seems to be very restrictive in terms of using only digital signature technology, and the government's August 1998 position paper on international recognition of digital signatures reinforcing their own law. Can you tell me how the U.S. is responding to this very alarming direction that the government of Germany is already taking in this area?

Mr. PINCUS. Certainly, Mr. Chairman. Let me mention one set of international developments that is relevant. Just as we are having this discussion here, the question of promoting uniformity has been very much an issue in Europe within the European Union. In fact, the European Commission has proposed an electronic signature directive that is now working its way through their process, and is expected to be finalized sometime toward the end of this year. It is much closer to—although not completely congruent with—the principles I discussed earlier and will require significant changes in the German law.

We have made it clear to the Germans that we think their approach is not technology-neutral. It is technology-specific, which would create real problems in global commerce. The European Union approach is much closer to ours and more technologically neutral. It is different from the approach we advocate in that it provides for some government identification of preferred technologies, and giving them a legal presumption, which we think is not the way to go. But it is a lot closer to where we are and would require significant changes in the German law.

Mr. TAUZIN. Andy, you have mentioned that you are not sure yet; you don't know whether or not electronic commerce is impeded yet by the lack of a national standard that is technologically neutral,

but nevertheless moves all the States in the same direction. How do you know what activity is not going on? How do you identify what is not happening in e-commerce? We can identify what is happening. But how much is not happening? Maybe you can jump in and help me with this, some of you other witnesses.

It seems to me that is a hard thing to quantify. It seems to me that if we are smart enough to pass a national standard that is amenable to all the States, a lot of things could happen that aren't happening today. Am I wrong in that?

Mr. PINCUS. I think you are right. It is hard to know. I think in talking to the private sector, which obviously has its finger much closer to the pulse than we in government do, most of the concerns that we hear expressed are in terms of what happens if we don't get to a uniform standard soon. We don't hear a lot of examples of people saying, "We are thwarted from doing something right now."

Mr. TAUZIN. Well, let's find out. Ford Motor Company indicates, Mr. Skogen, that you are doing a lot of online customer activities. But the customers still have to go to a dealership, right, and sign a contract at the end of it all; is that correct?

Mr. SKOGEN. That is correct.

Mr. TAUZIN. Would it be helpful if, in fact, we had a national standard so that you could do all of that business online, including the contract? Could we end up 1 day where customers could design their cars; order them from you online; and the factory would build it and ship it?

Mr. SKOGEN. Well, I guess anything is possible.

But we do, in fact, receive requests from customers and e-mails on trying to make the process a little smoother for them; allow them to do as much of it from home as possible. In fact, even some dealers today are delivering vehicles to the customers' homes that have ordered it over the Internet.

Mr. TAUZIN. Yes. So I mean that a lot more is possible if we are wise enough to have a nice set of standards.

Let me ask you in terms of the current bill, Mr. Siedlarz, you have made the case for technological neutrality here. Is our bill sufficiently technologically neutral?

Mr. SIEDLARZ. I think it is. I think, Mr. Chairman, it is very close. With our little sensitivity on the issue of biometrics; the way we link biometrics to encryption; and the growing understanding of those who have to work together, I think that is true.

One added comment to your previous question, if I may: It has to do with the issue of how we judge what is happening on the Internet today. I don't think we know the true story. Because we measure everything in terms of financial losses, for example, and the misuse of a credit card, or having that information stolen; we don't know, in fact, whether or not privacy is being invaded at a significant level, and yet not realized today by the consumer. We simply don't know the levels of penetration.

Mr. TAUZIN. You don't know how many consumers refuse to use e-commerce until they know all this has been worked out.

Mr. SIEDLARZ. That is correct. I suspect that it is a large number.

Mr. TAUZIN. Mr. Curtis, let me get you to help us, too. How deep is the concern about disavowal of transactions, right now, repudi-

ation, and the losses that might be incurred by companies without a digital standard?

Mr. CURTIS. Our concern about that is fairly high. We are moving forward with a number of initiatives that will have us more active online. But concern about disavowal, and consequently, fraud, actually are a high-level concern with us. They are holding up some of those initiatives that I really don't want to talk about in detail. They are company-confidential. We probably would be moving faster and providing more online, Internet service sooner, if there were greater certainty of transactions over the Internet and a more secure legal basis for them.

Mr. TAUZIN. So you have that same sense that we seem to have. Consumers, in many cases, are going to be much more willing to engage in e-commerce once we have some kind of national standard established.

Mr. CURTIS. Yes, I think that is true. Definitely.

Mr. TAUZIN. Secretary Upson, before I leave you and go to the members, would you give us a little clearer understanding of the Virginia concept of the best practices center? What is it? How does it work? What does it do?

Mr. UPSON. Yes, Mr. Chairman, I would be pleased to. In fact, I am sorry that I neglected that in my remarks.

One of the things that we are trying to do is encourage the State agencies to—and Governor Gilmore is about sign an Executive Order that will require State agencies to—think about the electronic signature environment and putting up systems that facilitate it in their contractual arrangements. What we are establishing is a statewide, best practices website, where agencies—smaller agencies in particular—can go and get information on how the process works; what other agencies are doing; and what other States are doing. This is so we might have the ability to take advantage, without having to reinvent the wheel, and really build a best practices center across government that we can use for a number of information technologies and electronic commerce initiatives. Digital signatures is just one of them.

In fact, one of the recommendations that you might consider is a best practice site at the Commerce Department, or an appropriate place, for States to be able to at one stop understand where they can go and see what the best practices are, and find out what other States are going.

Mr. TAUZIN. Interesting. Thank you very much, sir.

Finally, Mr. Engelberg, we have a number of members now. I wanted to wait until we had a sufficient number, because I thought this would be interesting for everyone.

Here is your digital signature on Stamps.Com, right? Explain to us how it works. How is it secure? How is it authenticated?

Mr. ENGELBERG. Sure. Each barcode is unique. Each one contains a digital signature that is generated for that particular piece of mail. The barcode contains additional information like the delivery routing; zip code; where it came from; a date/time stamp, and the amount of the postage. A digital signature is generated by a private, cryptographic key, which is unique to a particular user.

Before we create that key set, it is sent to the Postal Service's Certificate Authority, where a digital certificate is generated. That

certificate's serial number is embedded in the barcode. In the event that the Postal Service wants to authenticate the postage, they can scan the barcode; get the certificate's serial number; and from the Certificate Authority get the public key to read the digital signature. If the two match, then you know it was generated by a valid key. So, that is the full process.

Mr. TAUZIN. So, it is an encrypted system with a private key, with the availability of the Postal Service to use a public key to authenticate it, if necessary?

Mr. ENGELBERG. Correct.

Mr. TAUZIN. Thank you very much.

The Chair will now yield to the gentlelady from California, Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman. My thanks to each one of the panelists for your excellent testimony to us.

I would like to start out with Mr. Pincus. Thank you, again, for your testimony and your good work at the Commerce Department on the international front of this very important issue.

My question to you concerns the section on preemption. I am sure you would have guessed that is what I would be asking you about: section 102 of the bill. As you point out in your testimony, this section would empower the Secretary of Commerce to file an action to enjoin the enforcement of State statutes prohibited by this act.

I have two questions. First, did the Secretary of Commerce seek this authority? Second, what effect do you believe such a statute would have on State laws addressing electronic authentication? Then, as a follow-up, I would like Mr. Greenwood and Secretary Upson to also comment on the questions and Mr. Pincus' response.

I am asking you to divvy up the time now. Those are my questions. Mr. Pincus?

Mr. PINCUS. Thank you, Congresswoman Eshoo. We certainly did not seek this authority. As I mentioned in response to the chairman, we are not aware that the case has been made yet that there is a need for preemption, although it is risky. When the chairman is making a case, you sort of always now that you are going to get on the bad side.

Ms. ESHOO. But that is what hearings are for, so that we can flush out the different parts of the bill; develop consensus, and have the strongest one that is going to work well for the country.

Mr. PINCUS. No, I understand that. So we didn't see a case for preemption at this time. I think to the extent there is such a case, as I said in my oral statement, it seems to us that it is a case to create a gap-filler rule until the States enact the Uniform Electronic Transactions Act. I think that everyone agrees, as I said, that if we could wave a wand and be sure that every State would do that in a short period of time, then there would be no problem, because the UETA would be a very strong, uniform basis of national law.

That, it seems to us, is what we should be doing. Some of the concerns that are expressed in my written testimony are that this bill really goes beyond that goal and could create some continuing questions about the preemptive effect of this measure vis-a-vis any

uniform State law that is enacted. That could cause a lot of confusion about what the governing rules are.

Ms. ESHOO. Thank you.

Mr. GREENWOOD. I tend to agree with Mr. Pincus. I guess I would just emphasize one part of it. We really are, I think, at the cusp of uniform State law in this area. National Conference of Commissions on Uniform State Law has been almost at the end of a multi-year process of developing the Uniform Electronic Transactions Act. I feel like I have been privileged to be at almost all of their drafting meetings. It is quite an incredible process to see them go through so many interrelated areas of State law and common law; and get down to the fundamental interests that industry has in creating a better legal framework; and make sure they are meeting those interests, while also balancing other interests, as well.

Ms. ESHOO. Do you think that the States, in developing the model legislation, would have that completed within the 2-year deadline that I think the bill establishes?

Mr. GREENWOOD. That is going to be one of the areas that we will be proffering comments on within our 30 days. The 2-year time limit, in our view, is somewhat problematic. The preemption balance is going to be the most delicate one in a measure like this. A key criteria is that it allows jurisdiction to revert back to the States, as part of our comprehensive Uniform Commercial Code, commercial law, and Uniform Electronic Transactions Act process. We have some States that are not even going to be in session. They have legislative sessions every other year. Texas, and some others, for example.

The other issue in this is that we are talking about an area of law which is going to be evolving over many, many years. The markets will evolve. The technologies will evolve. Things will come up. So long as you have States around; so long as we have these legislatures; and we have other interrelated areas of law, we are going to need the flexibility to maintain the jurisdiction—and in a sense, the sovereignty—to continue to discharge our duties to make sure those laws are appropriate and responding to those changing conditions in 2 years, in 20 years, and hopefully, in 200 years.

Ms. ESHOO. Secretary Upson?

Mr. UPSON. It is an interesting question. I would just comment that I think that what I understand the statute does—or is attempted here—is that uniform standard of recognition across the country in recognizing an electronic signature is in the interest of the citizens of every State. Of course, it is a little moot for Virginia. We are in place, or will be within the 2 years.

Part of me thinks—to speak as a consumer—I hope that the States would have that in place within 2 years for the ease and the ability to do the kinds of transactions that are multi-State, in terms of insurance; buying a car; registering with a financial institution, or anything. I am not sure that in the Internet speed that our society is moving at that will be an issue in 2 years. Maybe I am an optimist. I hope that the national standard that this law establishes itself is in place. I would feel differently if there were a prescription for how we do it, as opposed to that there is a rec-

ognition that an electronic signature is binding. I think that is the significant part.

Ms. ESHOO. I don't think the committee has ever, in any of its legislation, prescribed to a certain technology. I don't think that is for the Congress to do.

Mr. UPSON. No. I understand that.

Ms. ESHOO. So we agree with you there. The area that I am pursuing, as you clearly understand, is how we marry the "test kitchens," as it were, of the States; not dampen their creativity; develop something that is timely across the Nation; but not trample on one another. That is the area that I am asking you about. I am not so sure what your answer is.

Mr. UPSON. I guess I don't see the trampling in the legislation. I don't.

Ms. ESHOO. So you think that the States are being respected? If they don't come up with something in 2 years, the bill would impose——

Mr. UPSON. I would hope that the States, in 2 years, would have it in place. I just think that in 2 years we will be so far along with electronic commerce, I think it is important that——

Ms. ESHOO. This is electronic signatures that we are talking about, though.

Mr. UPSON. Well, electronic signatures I consider to be integral.

Ms. ESHOO. You are doing your best to give me answer, and be very respectful of Chairman Bliley. I appreciate that.

Mr. PINCUS. Congresswoman, can I underline one thing that Mr. Greenwood said, because I think it is important.

One of the problems of the 2-year period is if 10 years from now—and this frequently happens with uniform laws—there is an update that is done because of changes in technology, or things we cannot even anticipate. I think the way that this is currently drafted, it would prevent the States from coming back with another uniform law that updated the first one. I think that is what he was getting at. It has this continuing preemptive effect.

Ms. ESHOO. I appreciate the comments that you have made, each one of you. I think, Mr. Chairman, it is a section of the bill that needs some dusting up. I yield back.

Mr. TAUZIN. I thank the gentlelady. The Chair now recognizes the gentleman, Mr. Shimkus, for a round of questions.

Mr. SHIMKUS. Thank you, Mr. Chairman.

I want to first direct my question to Mr. Engelberg. Based upon your response, you saw us all chuckling. Encryption is part of this issue, but we also have another big issue before us on encryption. I guess the question I want to ask, first, is in our issue addressing the ease of export controls for encryption products. What is role of that, in perspective? I will just ask for your comments.

Mr. ENGELBERG. Well, as a company, Stamps.Com does not have a formal position on export controls of encryption. We are working with international postal authorities to try to achieve a international standard, along with the U.S. Postal Service, for the digital signature and two-dimensional barcode, so that this form of postage can be recognized worldwide. Right now, it is restricted for domestic use.

Mr. SHIMKUS. Why is it restricted for domestic use?

Mr. ENGELBERG. There are a bunch of reasons, mostly Postal Service decisions. International postal authorities do not yet have the ability to recognize that type of postage.

Mr. SHIMKUS. Does it depend, in any amount, on our encryption policy?

Mr. ENGELBERG. I don't believe so. I would want to investigate that further and provide a written response.

Mr. SHIMKUS. Also, you talked about public access and private access of keys. Is the perception on your end as far as mail fraud and the ability to have access to keys, both public and private, a concern? Is it not a concern?

Mr. ENGELBERG. In our system, the keys that are used to generate the postage are not actually in the hands of the user. They are always maintained on our server. When a user logs in and is authenticated through a proprietary authentication process, the keys that are used to generate postage for their unique account—their meter—are pulled from a data base and used, within the boundary of a highly secure, cryptographic device.

One of the concerns that I highlighted in my written statement was that a private key in the hands of somebody who does not know how to use it can be dangerous in that someone could get hold of your private key and begin signing things. It is non-reputable. That is one of the reasons we hold onto the keys that are used to sign.

Mr. SHIMKUS. What if there is an issue on mail fraud and the government? I guess the Department of Treasury would want to address that. How would they get access to a key to follow information—or, would they?

Mr. ENGELBERG. Well, one of the motivations for the system, actually, was to combat mail fraud. Traditional postage meters are susceptible to fraud. You can crack into them and literally roll back the meters. So this was a way of stepping up the security of evidence of postage.

With regard to which government agency would conduct an audit, right now that exists within the Postal Service. The way they would do it would be by scanning any individual mail piece and checking the validity of the digital signature using a Postal Service Certificate Authority, which the Postal Service runs.

Mr. SHIMKUS. Okay. I think I still have some time, so I will go with Mr. Skogen, from Ford Motor Company. Would you please outline a few components of the transaction costs your company may incur if it is faced with 49 different State electronic signature laws? I don't know why it is 49. Probably 50 different signature laws are possible.

Mr. SKOGEN. Maybe I can respond to that from a little bit different side, and look at some of the things that we are looking at and doing today on the Internet that could be affected by it.

For instance, I see several opportunities for several applications for the Internet that we have already launched. For instance, company-to-dealer communications through a dealer Internet website, which enables us to communicate faster, on a more timely basis, from one central location. Some of the things that we would like to do on that website are going to require some type of electronic signature.

Ford Credit offers customer account access online, which provides 24 hours, 7 days a week secure account access for customers. Today we have roughly 170,000 Ford Credit customers that are using it on a monthly basis. Our purchasing organization is analyzing warranty repairs, via the Internet, along with our suppliers. They are pursuing a paperless purchasing process, which includes non-production purchases of several billion dollars a year. On the Ford supplier side, Ford has a Ford Supplier Network they can access through the web, which offers information and communications facilitating the engineering process, along with online training.

Everything that I have mentioned provides additional efficiency and convenience; but it would be more efficient and secure with electronic signatures.

Mr. SHIMKUS. And much more difficult if you had to comply with 49 or 50 different encryption possibilities.

Mr. SKOGEN. Yes, that is true, I guess. Whatever advances—is e-commerce the quickest? Whether we get it from the States, or whether we get it from the Federal Government, it has to be uniform and it has to be soon.

Mr. SHIMKUS. Mr. Chairman, I yield back. Thank you.

Mr. TAUZIN. I thank the gentleman. The Chair now recognizes the gentleman from Tennessee, Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman. Let me thank you, once again, for your tolerance in allowing a little flexibility here today.

As I had mentioned earlier, last year the House passed the Government Paperwork Reduction Act. I have introduced legislation to try to bring that to a head. That act required that, by the year 2002, the various Federal agencies would be able to communicate with electronic signatures with their constituents; but it has really set up no guidance. You could wind up getting into a situation where, because of interoperability within an agency, or between agencies, you could have even a more difficult time trying to communicate than before.

So what our digital signature legislation does is sets up, or dictates, or directs NIST, which is the National Institute of Standards in Technology, to establish some minimum, technologically neutral standards so that the different agencies will be able to by off-the-shelf products and have interoperability. That was the objective. I have vetted it extensively with the private sector, all on a positive basis, if anything they say goes beyond this in having authentication beyond just electronic signatures. I have tried to make this available to all of you. I don't know whether it has worked its way up through the food chain or not.

I am going to break the cardinal rule of a lawyer and ask a questions that I don't know the answer to. I will start with Mr. Pincus. The ones of you that have had an opportunity to review this, any kind of feedback that you might give, give please.

Mr. PINCUS. Certainly, Congressman Gordon. Let me say, first of all—maybe a little parochially—we are very proud of NIST at the Commerce the Department, and its expertise in the computer area, among many other areas. We think it does have a role to play.

I think our question involves how this legislation would interact with last year's, because we think last year's legislation is working. Agencies are moving forward with the process of moving online,

and adopting authentication methods that work for whatever their particular interaction with customers or constituents is. I think we would be interested in working with you to provide a way so that agencies, as Mr. Upson said, have access to the resources so they know what is out there in the marketplace.

Where we get concerned is the idea that there can be a single solution or set of solutions for standards problems in the government. Just like in the private sector, there are different kinds of authentication and different levels of security that may be appropriate for different kinds of government/non-government interactions. So we are leery of an approach under which there can only be one digital signature that you can use for all your interactions with the government, because that is not how the agencies are going. As I said, their missions and their various interactions may require different levels of security. Obviously, it is very high for Treasury in its dealings with financial institutions; and it may be much lower if it involves just filing an informational form that does not carry the same consequences if things are mishandled.

My overall reaction is that we would, obviously, be very happy to work with you in moving this forward.

Mr. GORDON. Well, our objective is not to look for one standard. Our objective is to, again, allow a minimum standard.

I know that at home we have 95 counties in Tennessee. We, some time back, tried to get them all to take their election commissions and get them computerized. Well, each election commission got the cheapest thing they could find. There was no interaction between them. We are having to start all over.

So, there are number of, I am sure, good products there. What we want is for agencies to know which ones can be interoperable and where you go out on-the-shelf and purchase them. Anyone else?

Mr. PINCUS. I should say that on the off-the-shelf point we are very focused on the idea that we shouldn't be looking to create special products or technologies for government. What government agencies should be doing is looking at what is out there in the marketplace and picking something that works for them.

Mr. GORDON. Trying to keep within our time. Anyone else?

Mr. UPSON. Just a quick observation. I am not real familiar with the legislation. As you describe it, there is also, under the Information Technology Management Reform Act that Congress created and the President signed, a chief information officer apparatus, where you have the agencies with the knowledgeable people. I forgot what the mechanism is in that bill, but they meet regularly as you know.

Mr. GORDON. I think it is the OMB.

Mr. UPSON. Yes. And each agency has a representative. That might be very useful.

Mr. GORDON. We are trying to work with them to, again, find that continuity.

Anyone else?

Mr. SIEDLARZ. Congressman, one other quick response. I wanted to make you aware of the fact that there is a significant movement within the industry to find application program interface standards

that all companies and all technologies can meet, up to a certain line, for a kind of handshake that would make them interoperable.

One of the most significant ones is an ad hoc organization called BIOAPI. Most of the major computer manufacturers, as well as significant participants in the biometric industry are involved in the development of those standards. Before the government steps in and attempts to adopt a standard, even a common denominator one—which I think is admirable—I think the product of those industry groups would be useful, first.

Mr. GORDON. If you could provide me with the name of that organization and how to contact them, it would be helpful. Thank you.

Mr. SIEDLARZ. I would be happy to do that.

Mr. GREENWOOD. If I may take a stab? I had an opportunity to review the legislation. One of the sections of it that I thought held a lot promise to be assistive was the panel. I think it was the last section. A number of States have been struggling with the same questions. How do we organize? How do we standardize? How do we ensure interoperability among our usages of electronic authentication; and in particular, the usage of certificate authorities, certificates, and digital signatures?

I would be happy to make available to the committee in part in response to your question a draft guidelines document which we came up with collaboratively with some Federal agencies, and mostly with some private-sector entities through the National Automated Clearinghouse Association. It is something called "The Certificate Authority Rating and Trust Guidelines." We opted in the end of the day for no central standards from any given organization, or even a consortium of organizations. But rather at this stage, since we are still in an early phase of development of the technology and the business model supporting the this technology; we opted to give some guidelines for bottom-up standards through watching best practices emerge: contracts, operating rules, and things of that nature.

The only other observation I make on the bill, which maybe deserves some more review, is that it does seem to have an underlying assumption that the usage of certificates will be part of a trusted third-party certificate authority model. Our review of this document in the natural organization seemed to indicate that the business models are developing more in line with a so-called "closed system," or a bounded system, where the organization issuing the certificates for use is actually one of the two parties themselves. So it may be that your bank is issuing you a certificate. It is not some third-party certificate authority. That is something that might bear some more analysis in your bill.

Mr. GORDON. I think within the Federal Government you are going to be dealing with constituents more than business. There is some business-to-business; but there are also going to be individuals that will not have that "in-house" ability.

Mr. SKOGEN. I would like to just make one quick comment here. We see H.R. 1714 as the first step in establishing acceptance of electronic signatures nationwide. We do support anything that advances uniform standards, such as H.R. 1572.

I mean, if the Federal Government can be used as a model for widespread usage, I think that is great. But we think that the in-

dustry-based standards for certification authorities would be better for business.

Mr. GORDON. Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman. The Chair is now pleased to recognize the gentleman from Oklahoma—who, in e-commerce jargon, may not have been much of a sender, but is one hell of a receiver—Mr. Largent.

Mr. LARGENT. Mr. Pincus, for many at the Commerce Committee, can you give us any idea what the number is in terms of dollars that is being conducted today in e-commerce in this country?

Mr. PINCUS. In my written testimony, I have some numbers. The projections are overtaken when we get to reality, so the projectors go up another notch.

The forecast that we are hearing is that online retail sales will be about $40 billion by 2002. And all e-commerce activity, including business-to-business which is obviously a much larger amount, could be up to $1.3 trillion, in around 2002-2003.

Mr. LARGENT. What would you estimate that it is in 1999?

Mr. PINCUS. I think in 1999, the online—the Christmas retailing—was in the $7 to $9 billion range. I am not sure what the number is for online business-to-business. It is many multiples of that. The business-to-business transactions are moving ahead much quicker than retailing.

Mr. LARGENT. So, $12 billion; $20 billion?

Mr. PINCUS. I think maybe in the upper range; around the $100 billion range.

Mr. LARGENT. One hundred billion. That is all electronic commerce? I am trying to compare your numbers. In 2002 you said $40 billion.

Mr. PINCUS. No. The all-in number was $1.3 trillion.

Mr. LARGENT. Right. Okay, that is right. So, $100 billion. We are anticipating that to grow by twelvefold in 2002.

Mr. PINCUS. I think the growth rates are very high.

Mr. LARGENT. Okay. Do we have any idea what kind of abuse has taken place today, because of the lack of verifiable or uniform electronic signature laws in this country? How much are people stealing—Visa Card numbers, and so forth? What kind of abuse is taking place today?

Mr. PINCUS. I don't think we know. I actually think that, even if we had a signature law, even if the Uniform Electronic Transactions Act were enacted today, that still would not provide a means of paying for most consumers goods. I think in the foreseeable future for consumer transactions, there is electronic money and perhaps other innovations that are a bit further off in the future. I think people anticipate that credit cards are going to be the method of payment for consumer transactions in the near and medium term.

Credit card companies, themselves, have been developing some kinds of security mechanisms to be sure that credit card numbers aren't misused. But as some people have pointed out, if you give someone your credit card in a restaurant, it passes through a lot of hands. The opportunity for people, if they have a fraudulent frame of mind, to get the number and misuse it is not that different from someone's catching the number electronically. A person

with fraud in mind, if they get into the stream, can obviously catch a lot more numbers and may have a bigger opportunity for fraud. But I think the credit card companies are very focused on this problem, since they bear the burden of the fraud and are figuring out ways to prevent it.

Mr. LARGENT. Do you hear from the States very often in terms of the dollars that are conducted through electronic commerce that escape State taxation, or even cities and municipalities?

Mr. PINCUS. I am privileged to be Secretary Daley's representative on the Internet Tax Commission. So in preparing for the first meeting of that Commission, which is going to take place in Williamsburg on the 21st and 22nd, I have been hearing a lot of information from States and localities about their concern that there may not be a tax collection mechanism; and what that might mean for their revenue base.

Mr. LARGENT. Yes. So I am asking that question, because one of the issues is States' moving forward with their own legislation on electronic signature. Would the fact that they are losing taxes, because of electronic commerce, be a sort of cold blanket on them out of wanting to move forward expeditiously within a 2-year window, or whatever, on doing something themselves? Do you understand what I am saying?

Mr. PINCUS. I understand what you are saying. I guess I haven't heard that. Because of the economic growth potential of electronic commerce for our country and for each State, I think there is much more of a policy and political imperative for States to do things that facilitate the growth of electronic commerce, even if it may, as you say if this other issue isn't solved, have an adverse revenue effect on them.

What we have heard is much more of an interest in doing things to help e-commerce grown, and then figuring out a way to deal with this tax issue.

Mr. LARGENT. That is what I hear, too. It does flow both ways. In other words, you can open up your own electronic shop in your State, and have people buying products from your State, as well.

Mr. Siedlarz, I just wanted to ask you a little bit about your company and how that works. What would I have to have to have on my laptop in order to do that iris deal? Everything that I would need, do I have it on my laptop right now?

Mr. SIEDLARZ. Pretty much, except that the only other peripheral that you would need, Congressman, is a small imager—a camera—that sends either the iris code itself, or the image for processing on the laptop, and resident software on the laptop that would do the processing and comparison.

Mr. LARGENT. Does that have to have that broad-band, high-speed Internet capacity?

Mr. SIEDLARZ. Well, it doesn't. There are two different version of it that we are working on now. One can send a very low bandwidth of 4 to 6 frames a second. Another version sends 30 frames a second, but you are doing the processing in the imager. So, it depends on where you are doing the processing.

Mr. LARGENT. Mr. Engelberg, my last question is to you. You were explaining, a little bit, about your electronic signature on your envelope. I have to tell you that I honestly did not understand one

word you said. Can you kind of just tell me what business you are in? What the heck do you do with this, Stamps.Com? I don't have a clue.

Who are your consumers? Do you just work with the general public? What would I buy from you? What is your business?

Mr. ENGELBERG. Yes. Our service is designed to provide postal convenience. We basically replace the postage meter. We make it possible for you to print postage off your desktop printer, using your laptop with nothing added; 24 hours a day, 7 days a week. We do it with a system of cryptographic keys on our servers that generate digital signatures to make each stamp unique. There is a digital signature in every barcode, in every stamp.

Mr. LARGENT. And the Postal Service has to read that digital signature?

Mr. ENGELBERG. The Postal Service can read it to audit the process to determine the authenticity of the stamp. When they read the barcode, they can pull out the digital signature and validate that with the public key they have on their Certificate Authority.

Mr. LARGENT. Okay, I got you now.

Mr. ENGELBERG. I will stop there.

Mr. LARGENT. Yes. Don't give me too much information.

Thank you, Mr. Chairman. I yield back.

Mr. TAUZIN. Otherwise you might go postal on us.

Thank you, Mr. Largent. The Chair is pleased to recognize the gentleman, Mr. Sawyer, for a round of questions.

Mr. SAWYER. Thank you, Mr. Chairman. Every time we talk about the electronic environment, one of the things that I try to do is to think back to the fundamental underpinnings of any process of law that might have preceded the environment that we are working in, and recognize that many of the protections that are offered in conventional environments really ought to apply in a more technological one.

Today we have been talking about interoperability and verification of signatures. We have touched a little bit on sanctions. But I am struck by the Virginia precept that suggests that, "Where any Virginia law requires a signature, or provides for certain consequences in the absence of a signature, that law is satisfied by an electronic signature." I would really like to ask you to talk a little bit about sanctions for falsification, or failure to perform as agreed over a legitimate signature at both ends of a transaction. I am particularly interested in the Federal law enforcement standards. We have talked about postal standards, but I am not sure about postal fraud: everything from bouncing checks and the IRS, and the way that has been used for enforcement.

So what I would like to ask each of you is, thinking in terms of both a multi-State and trans-national settings, are there special places that we ought to look for pitfalls that are unique to this environment in terms of enforceability and comfort levels with sanctions, and guarantees of privacy and security? It seems to me that if trust is at the core of a signature, that becomes particularly important when we are not only talking about the electronic environment, but the playing field, both multi-State and trans-national. Mr. Pincus? Mr. Upson? Special pitfalls that we need to look out for.

Mr. PINCUS. Well, I think one you mentioned is, certainly, privacy. We have taken the position that we should look for the private sector to lead the way on privacy protection. Certainly, one thing that we believe is important is that authentication providers have good privacy practices that are up to the level of the good online privacy practices that we have talked about elsewhere. I think that most of them do. That is clearly important. Because it is possible that with some forms of authentication, the authentication provider would have a lot of information about an individual's transactions that the individual might not want to be sold, or might at least want to exercise a choice about whether it could be marketed, or mined by data miners. Certainly, we think that allowing such choice is a good practice. We have not advocated government solutions to this problem, because we think the private sector is moving to do that. I think that is the right approach.

I think as a general matter, although electronic commerce technology is very different from that used in international commerce, it may be inappropriate to have special protections for electronic transactions differing from those we have in the physical world. We have general commercial contracting rules. We also have special consumer protection rules—unconscionability, and things like that—that apply to consumer contracts. You would certainly want to be sure that those things applied in cyberspace, as well.

There are some kinds of contracts in the physical world, with respect to which we require special formalities: wills, for example. One would certainly want to provide that is also true, to the extent that there will be electronic contacting, that there will be a form of authentication in that context that has special assurance, because we insist on that in the physical world.

I think as of now, we don't see the need——

Mr. SAWYER. I don't want to run out of time.

Mr. PINCUS. I am sorry. Other than translating current rules appropriately for the online world, we don't see the need for some special, overall new rules in electronic contracting, because we are concerned about how that might tilt the market.

Mr. SAWYER. Mr. Upson, would you be comfortable enforcing Virginia's laws based on signature in a multi-State or trans-national setting, based on the kinds of protections that you have available?

Mr. UPSON. Well, I guess I would look at from this perspective: I think that what we have tried to do in Virginia is not create any new laws, necessarily; except for unsolicited bulk e-mail, where we have a unique statute. Really, if it is fraud in the non-electronic world; it is fraud in the electronic world.

We have tried to ensure that our statutes do exactly what Mr. Pincus said: to ensure that our statutes recognize that fraud is fraud. If you falsify information electronically; once that is recognized, it is a crime. We actually have a program to train law enforcement professionals in cyber-crime. I guess that is the way to look at it. Really, we try to say that our whole premise is—I think it is yours, too, in this legislation—that crimes are crimes, whether they occur electronically or not.

Mr. SAWYER. I agree with that. I am looking for special circumstances that we ought to be particularly alert to.

Mr. UPSON. "Spam," I think we have looked at. We have attacked it. We have created a cause of action. There are companies that engage in spam as a matter of business and pay fines that are set up. We have made it very expensive now, in Virginia. That is unique to the Internet.

Mr. SAWYER. Mr. Skogen?

Mr. SKOGEN. Yes. I am really not the right person to respond to that question, but would be happy to get back to you.

Mr. SAWYER. Good.

Mr. GREENWOOD. In Massachusetts, one of the first things the Weld administration did in the early 1990's was to create a computer crime commission, which analyzed our entire body of statutory and common law crimes to see whether they were adequate for even what we were seeing then as our emergence into an information age. I think the results at that time really still hold true today. Largely, our existing body of laws was adequate to handle the types of crimes, fraud and other misdeeds, that we saw developing. The exception is that we have to keep asking the question.

So our approach is to remain on the lookout; to continue to have hearings like this; and continue to ask and make targeted reforms, as needed. I think we clarified a couple of things to just make it painfully obvious for our prosecutors as they made the case that larceny includes electronic property, and so forth. So we made a couple of small tweaks—arguably not even necessary.

Mr. SAWYER. Others? Thank you, Mr. Chairman.

Mr. TAUZIN. Thank you, Mr. Sawyer. The Chair is now pleased to recognize the gentleman from Illinois, Mr. Rush, for a round.

Mr. RUSH. Thank you, Mr. Chairman. Mr. Chairman, I want to also commend you for patience, and commend the witnesses for their patience. I know this has been quite a long hearing. I just have a couple of questions for Mr. Siedlarz.

This technology to verify someone's identity through their physical characteristics is pretty fascinating to me, and I am sure to others. You can accomplish this through the use of computers and other enrolled data?

Mr. SIEDLARZ. There is a broad range of technologies, Mr. Congressman, that do that. In fact, maybe 115 different versions are available in the world today.

Mr. RUSH. Who would take advantage of this type of technology?

Mr. SIEDLARZ. That question somewhat talks to the previous one from the Congressman about the issue of what we should be concerned about. The truth of the matter is that the new technology today has a capability of verifying an individual in a much more positive way that the previous signature—the human signature—ever did. To the degree that Federal law is not comprehensive enough to protect that from those who would attempt to steal and counterfeit even the electronic version of that today, we need to do something about that. As the business on the Internet increases and e-commerce increases, clearly, the threats against the electronic means of using technology to prove identity, or verification, or authentication are going to come under more serious attack. Anything made by man will ultimately be defeated by others.

Mr. RUSH. Is this technology aimed a particular, narrow group of people?

Mr. SIEDLARZ. No. The best biometrics whole purpose is to be absolutely useful in the general population. To the degree that segments would not be available, then the technology would be inherently flawed for use in electronic commerce.

Mr. RUSH. When you indicated that you can verify someone's identification through the pupil of the eye——

Mr. SIEDLARZ. The iris of the eye.

Mr. RUSH. Are you going to have that information? How would you gather and collect that information?

Mr. SIEDLARZ. That is a good question. Well fundamentally, an image of the eye is taken and it is immediately converted into a digital code. Then that is translated through a relatively sophisticated process into what we call an iris code and stored into the computer as 512 bytes of information. There is no way that if you take that hexadecimal code of 512 bytes that you could recreate the iris, or recreate anything that looks like that original image. That information is essentially, absolutely useless to anyone other than the system of crossing a firewall and liking that image to an identity code.

Even IBIA, as an organization, has taken a very strong stand in being proactive about privacy, the ethics of privacy, and the use of rules maintaining privacy within the biometrics industry.

Mr. RUSH. How would you collect it, though?

Mr. SIEDLARZ. Enrollment. You would look in a camera. The code is created.

Mr. RUSH. So you have consumers just lined up.

Mr. SIEDLARZ. It is a voluntary situation, exactly. There are tests going on now; pilots in banks both in Europe, the United States, and elsewhere, where people voluntarily submit to enrollment—to get a picture taken, essentially—using camcorder technology and to have that code created. It gives them a great convenience. It protects their accounts. It, frankly, protects their privacy in ways that it never did before.

Mr. RUSH. This is my last question. Are we approaching the day when there would be a national or international data base of pupils on file?

Mr. SIEDLARZ. Some of us might wish so from a business standpoint. I don't think that, practically, that any one technology is going to capture the world market or the world use. We think some are better than others. But the issue of interoperability is really what is important here. Whatever one you use, there is a way for them to ultimately speak to each other, and serve the purpose that we need in society.

Mr. RUSH. Thank you. I yield back, Mr. Chairman.

Mr. TAUZIN. Thank you, Mr. Rush. I think it is fair to say that before you have a contract, you have to see eye-to-eye, anyhow.

It will all work out, somehow. I apologize.

The Chair is pleased to welcome the very patient lady from Missouri, Ms. McCarthy.

Ms. MCCARTHY. I thank you, Mr. Chairman, for this hearing and your foresight. I would like to remark, in follow-up to Mr. Rush's comment on international, that last October I was sitting in the Dublin, Ireland, Silicon Valley area in the Gateway Facility there observing Prime Minister Ahearn and President Clinton sign a

trade agreement from their laptops with their secure id's. So there are huge international uses already for this technology of the virtual signature.

Mr. Chairman, the President noted that while he is somewhat new to the technology, this virtual signature could potentially lead to a "virtual president;" and thought we ought to probably debate larger, philosophical questions while we grapple with the practical issues today of State and Federal authority.

It is almost like being at the top of a really snowy hill. The toboggan is heading down. You know it would be a great ride, but you are not on it. You are running after it.

I feel a little be breathless about this whole conversation, because it is happening. We are today trying to grapple with how to do it well, so that it happens with the safety and security that we all seek.

I must confess to the panelists I am a product of State government: 18 years in the Missouri legislature before joining this august body. So the question of preemption of any State law is real to me. My State, Missouri, in 1998 did pass the Missouri Digital Signatures Act, that our Secretary of State is implementing. It is modeled after Utah law. I know a lot of States are grappling with this.

So in this issue of State preemption, H.R. 1714 would preempt any State law that is not consistent with the bill; even if the State law is passed within the 2 years that the National Conference of Commissioners is working in, as well as any laws that are already on the books, like in my State of Missouri. Do you believe there is any risk that the uniform law that you are contemplating could be construed as inconsistent with H.R. 1714, and thereby render this entire, intensive effort invalid? I know my State will have to reflect on its current law; look to the Commission's work; and adopt and make changes.

If we pass this law, H.R. 1714, what if the Commission's work is invalid? Mr. Greenwood, could you reflect on that? I would love to weigh-in anyone else's thoughts.

Mr. GREENWOOD. Thank you very much for the questions. It is very gratifying to see an alumna from the State legislature for so many years in this august body.

I think your concerns are really right on. There is clearly a need on the one hand to get a national baseline soon. However, that cannot rule to the exclusion of an equally important need not to unduly disrupt these areas of State law and the emerging State laws.

To zero in on your specific question, one of the areas that ought be looked at as this bill is honed through the process is section 102[b][1] and [b][2]. There are several areas, but let us talk about [b][1], for a moment. It would require that a State law that is enacted to basically revert the jurisdiction back to the State within this period of time must meet this requirement: that it not discriminate in favor of or against a specific technology, method, or technique of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

That sounds good in the sense that it is technology-neutral, which is what we want. I do believe the Uniform Electronic Transactions Act, which we are primarily talking about now, is largely

technology-neutral. However, in the particular implementation of many particular areas of law; you do have to start talking about specific technologies in a consumer protection stance, for example, as we start amending our lemon laws to allow people to buy their cars at home.

Right now, Massachusetts has a requirement that there be a disclaimer of various warranties, and other notices placed on the windshield. That is a paper requirement. It is based on a known business model, where a consumer goes into the lot. They see the notice, and so forth. It is a media-specific requirement.

As we start transforming our business models to allow these things to occur online, when you don't have a consumer walking onto a lot and looking at a windshield before they make a decision; at some point we are going to have to say something—some sort of equivalent language like, "Must appear on a screen," or something.

Similarly, with securities regulation and many other areas of law—banking and on down the line—where there is consumer protection and other media-specific protection for notices and conspicuous terms in place; at some point the State legislatures and law makers at every level of government will have to come up with equivalent types of standards. That is by definition; discriminating in favor of, or against, a particular implementation. The trick here is going to be making sure that you allow us to responsibly apply the same kinds of jurisdiction that we have over commerce and other areas of law now, in the information age, without having an inconsistent or an undue impediment to interstate commerce. I think that will be the trick.

Ms. MCCARTHY. Mr. Chairman, would you indulge me a follow-up question?

I thank you very much for those thoughts. I think they are right on point.

Mr. GREENWOOD. Thank you.

Ms. MCCARTHY. I would like to know from Mr. Skogen, Mr. Curtis, and Mr. Siedlarz, if your industry has been involved in the drafting of the Uniform Model Code?

Mr. CURTIS. No, we have not.

Ms. MCCARTHY. Oh, yes, Mr. Siedlarz?

Mr. SIEDLARZ. Same answer.

Ms. MCCARTHY. You have not. Mr. Skogen?

Mr. SKOGEN. Apparently, we do, in fact, have State representatives that have been involved in doing that.

Ms. MCCARTHY. Okay. Well, Mr. Pincus, are you concerned that your efforts in this area could be for naught if the model is effectively preempted?

Mr. PINCUS. Well, we have concerns, as I said earlier and laid out in my written testimony, that we not do anything that would lead to controversy about whether the UETA, once it is enacted by the States, provides the governing law; and that there not be a lot of controversy about whether its provisions are preempted. Obviously, such controversy creates the very uncertainty that everyone is trying to remove.

So that is why in our view, to the extent there is to be any intervening Federal law, the best approach is to design an interim gap-

filler until the States adopt the UETA. Then the Federal law would fade away. It literally would exist only to fill that gap to the extent that the subcommittee decided there was a gap that needed to be filled; it would not be a continuing Federal overlay on the State law that is eventually adopted.

Ms. MCCARTHY. Well, I think that makes a great deal of sense. In fact, there is language in H.R. 1320 that I think attempts to achieve what you just articulated with regard to this issue of preemption. I would hope that this subcommittee would take a look at this particular point. I know, Mr. Chairman, others before me have raised the concern that when we enter this arena, we do so with the most study and the most well-chosen words so that we don't find out at the end of the process that all was for naught, and we are back to square one. This technology is taking off without us, like that toboggan down that snowy hill.

Mr. Pincus, you expressed concern, in your testimony that I have before me, about the bill's provisions requiring electronic signatures to meet reasonable requirements. I think that is appropriate. How might this provision lead to problems in the interpretation that covers the impact of the viability of the model code, or the model bill?

Mr. PINCUS. Well, as I mentioned, the real model of authentication that businesses are using now are these closed systems that are set up contractually, in which people pick whatever authentication regime works for the level of business and level of security they need.

Our position, and it is also a position that has been adopted by the drafters of the model law, is that those agreements should be enforced. Therefore, if that authentication method is used subsequently, those contracts should be legally binding. Our concern is that the use of the word "reasonable" would provide a basis for a judge to say, "Well, I don't like the authentication method that these parties chose for their transactions; so none of them are legally enforceable."

Especially internationally, where there will be different domestic legal regimes, we think the contractual method is going to be the way cross-border transactions will be facilitated. We don't want to have a U.S. model that allows judicial second guessing or to have such a model adopted by other countries.

Ms. MCCARTHY. I appreciate your involvement in this process. I understand the National Governors' Association is engaged in it, as well, with the National Conference. I would hope the National Conference of State Legislatures would be included, because an awful of lot these States have measures already enacted. It is imperative that those voices be at the table as well.

Mr. Chairman, you have been so gracious and kind. I thank you for extending this time for me.

Mr. TAUZIN. Well, I beg to differ. I have never met anyone more gracious than you, Ms. McCarthy. I thank you for that.

Let me thank you all, in fact, for your patience and your kindness in educating us. I have always called this one of the best universities in America that we attend. We have a chance to do what Mr. Largent did, which is to say, "Do that again so I can understand it." We learn. You have taught us a lot today.

Let me point out, Ms. McCarthy, that one of the problems we have in this debate we are going to have over preemption is the fact that there are a number of States who have adopted "digital signature only," and authentification technology "certified by the State only;" which runs counter to the technology-neutral concept that is embodied in this bill. For example, the biometrics concepts of iris identification would not be allowed in a number of these State jurisdictions because of the fact that is not an authentication technology approved by the State. It is not a digital signature technology as required by the State.

So we are going to have a little difficulty in working that out. I think the best admonition is that we do it in a way that sets a national standard, but doesn't preclude improvements that the Uniform Code authorities eventually might want to bring to States and to the national government in the future, as technology continues to teach us that there are different ways to do things than the way we did it yesterday.

Let me finally say that it was a learning lesson for us that some of you asked that we e-mail our invitations to you to come to this hearing today. We had to—regrettably—inform you that we couldn't do so because we could not authenticate the source of that e-mail; and you might not, therefore, have been officially invited to attend here today. Next time, perhaps, when we invite you we will have a system in place where we can communicate with you; and in this e-commerce world, authenticate who we are. You can authenticate your identities to us. We can maybe establish a hearing in cyberspace where you will not even have to get through the traffic jams in Northern Virginia, as Mr. Upson did, to be with us.

Thank you very much for teaching us today. The hearing stands adjourned.

[Whereupon, at 12:10 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF THE BUSINESS SOFTWARE ALLIANCE

Introduction

The Business Software Alliance (BSA) appreciates the opportunity to provide our views on H.R. 1714, the "Electronic Signatures in Global and National Commerce Act" (E-SIGN). BSA's members represent the fastest growing industry in the world, and are leaders in the development of products and services that support electronic commerce and enhance consumer convenience. BSA's worldwide members include Adobe, Attachmate, Autodesk, Bentley Systems, Corel Corporation, Lotus Development, Microsoft, Network Associates, Novell, Symatec and Visio. Additional members of BSA's Policy Council include Apple Computer, Compaq, IBM, Intel, Intuit and Sybase.

Facilitating Electronic Commerce

Electronic commerce is the American success story of the decade. The value of commercial transactions taking place on the Internet is expected to double, even triple, annually as consumers and businesses grow to understand the vast communications and commercial potential of the Internet as a medium of commerce. According to Forrester Research Inc., business-to-business e-commerce is expected to top $1.3 trillion by the year 2003. Consumers are also increasingly purchasing goods and services online. Forrester Research estimates that consumers spent $8 billion in 1998 on the Internet, buying books, CDs, clothing and other items.

The growing electronic marketplace provides unparalleled opportunities for economic growth worldwide. However, the willingness of both consumers and commercial firms to engage in electronic contracting and other critical aspects of commerce online will depend, in large measure, on reliable, well-developed legal structures governing the formation of electronic contracts and the rights of parties thereto. It

is an unavoidable fact that parties will be deterred from contracting and fully utilizing the commercial potential of the Internet if the governing legal rules are uncertain and thus their risks unascertainable. This is especially true in the online world that knows no geographic boundaries. Such an environment places a premium on harmonious legal structures that do not depend on state or international borders, allowing parties to form electronic contracts without undue concern as to their validity and enforceability. The need for certainty in the governing legal rules of e-commerce goes well beyond the ability to "contract" electronically. For example, users of design and architectural software would gain tremendous efficiencies if professional engineers were able to electronically "seal" drawings by virtue of a digital signature. This would be the functional equivalent of placing a stamp on the physical drawing signifying that this person, with expertise, has signed off on the drawing. A consistent set of rules relating to electronic signatures is required for this to ever become a reality.

This goal is threatened by a dizzying array of state legislation governing electronic signatures. These state laws and policies range from highly detailed, prescriptive statutory regimes to very general enabling statutes. If parties are left with no alternative other than to navigate a maze of potentially inconsistent and inadequate state laws, the growth of a seamless and frictionless electronic commerce marketplace will be thwarted. Although the Uniform Electronic Transactions Act (UETA)—a long-running effort that seeks to provide a common model electronic signature law for the states' consideration—will receive final consideration at the July, 1999, meeting of the National Conference of Commissioners on Uniform State Laws (NCCUSL), the prospects for comprehensive, consistent and timely action by all fifty states with respect to UETA remains uncertain at best.

Federal legislation is therefore necessary to bring certainty and reliability to electronic transactions, thereby encouraging greater confidence in electronic commerce. This is not simply an important consumer issue; it is an important business issue. Consumers may be willing to conduct small transactions in the online environment despite the uncertainty regarding their legal rights and the effectiveness of their actions precisely because their transactions are of small value. Businesses, however, will be more reluctant to undertake large transactions online unless the rules governing their transactions are reasonably well developed and understood. In the end, online commerce has to encourage business-to-business transactions if it is to achieve its full potential.

The development of appropriate rules to foster online commerce in the United States has real import for the competitiveness of our economy. Europe, for example, is rapidly moving to put in place a detailed EU directive on electronic signatures, and the United States cannot afford to fall behind with respect to the development of a coherent, effective legal structure that supports and fosters online commerce. Electronic commerce will achieve its potential only if governments domestically and around the world create sound legal structures that bring certainty and predictability to electronic transactions so that electronic commerce can become a secure, ubiquitous and global marketplace.

Comments on the "Electronic Signatures in Global and National Commerce Act" (H.R. 1714)

BSA supports H.R. 1714, and views it as a very positive step forward in developing an effective legal structure for online commerce in the United States. H.R. 1714 is consistent with a number of basic principles, outlined below, that BSA considers essential to support electronic contracting. However, in two limited respects, BSA believes H.R. 1714 should be clarified to afford parties true flexibility in electronic contracting, and enable all forms of electronic signatures to thrive in business-to-business electronic commerce.

(1) **Technology Neutrality.** BSA considers it essential that federal electronic signature legislation be technology neutral. No one knows precisely how electronic signature products will develop. However, all agree that the market will demand a variety of products and services offering varying levels of cost and security, and that users will select the appropriate mix of cost and security based on the value of the particular transaction. To ensure that industry can provide electronic signature products and services that meet the whole range of consumer needs, the regulatory framework must be sufficiently flexible to permit and recognize new signature technologies so as not to stifle innovation. *H.R. 1714, which does not mandate or provide legal or other advantages to certain technologies, is consistent with this important principle.*

(2) **Non-Discrimination.** Federal electronic signature legislation should ensure that electronic signatures, and the contracts and records to which they are attached, generally are not subject to rules and requirements that are more onerous than

those applicable to traditional signatures and contracts. Any exceptions to this basic principle of non-discrimination should be narrowly drawn and clearly defined. *H.R. 1714 appropriately advances this principle, drawing narrow exceptions only for rules relating to wills, codicils or testamentary trusts, and to adoption, divorce or other matters of family law, all of which BSA finds acceptable.*

(3) **Market Driven Technical Standards.** Federal electronic signature legislation should not impose mandatory technical standards regarding electronic signature products or extend legal benefits only to signatures generated by products meeting certain prescribed technical standard. Although some standardization may benefit consumers, the information technology sector has been very successful in developing necessary technical standards through consumer choice and industry consensus. Such market-driven standards fully respond to consumer demand and avoid the rigidity of government-imposed, mandatory standards that would inevitably impede technological development, distort markets in electronic signature products, and ultimately restrict consumer choice. *H.R. 1714 is consistent with this principle in that it does not impose any technical standards for electronic signature products.*

(4) **Closed System and Limited-Use Certificates.** Federal electronic signature legislation should be drawn broadly enough to give legal effect to electronic signatures that are used in closed systems or that are accompanied by limited-use certificates. In both instances, a signatory is allowed to access information, utilize services or engage in particular transactions based on a preexisting relationship between the signatory and the recipient (*e.g.*, employment of the signatory by the recipient; signatory's membership in a buying cooperative operated by recipient). As a result, the signatory and the recipient are fully aware of the limited permissible uses of the electronic signature and any accompanying certificate. It is anticipated that the use of electronic signatures within closed systems and with limited-use certificates will be major component of electronic commerce, and therefore it is vital that electronic signatures be given full legal effect and recognition in such contexts. *H.R. 1714 is consistent with this principle in that its definition of electronic signature is broad enough to encompass electronic signatures used in closed systems or accompanied by limited-use certificates.*

(5) **Federal Preemption.** Federal electronic signature legislation should include a preemption provision that reasonably balances the interest of the states with the need to develop in a timely fashion, a coherent, harmonious set of rules to govern the use of electronic signatures and electronic records throughout the United States. Thus, in those instances where states have enacted rules that are not consistent with the basic principles established in federal legislation or where states simply have not acted to provide the necessary legal rules for the use of electronics signatures, uniform federally established rules would govern and facilitate the use of electronic signatures. *H.R. 1714 is consistent with this principle in that it provides a set of federal rules regarding the non-discriminatory recognition of electronic signatures, but allows the states a reasonable opportunity to legislate their own rules governing the use of electronic signatures so long as such rules are consistent with the basic principles reflected in the bill.*

(6) **International Harmonization.** Federal electronic signature legislation should be carefully crafted so as not to impose any legal rules that discriminate against, or preclude the use of, electronic signatures from other countries. Electronic commerce is truly borderless. Accordingly, federal legislation should provide equivalent treatment for all electronic signatures, whether generated within the United States or abroad. This is important not only to facilitate the use of electronic signatures within our borders, but also to encourage other nations to afford comparable treatment to electronic signatures generated in the United States. *H.R. 1714 is consistent with the principle in that it does not establish any federal rules that discriminate against electronic signatures generated outside the United States.*

(7) **Party Autonomy**. Federal electronic signatures legislation should expressly incorporate and support the principle of freedom of contract among private parties with respect to the terms and conditions on which they will accept and use electronic signatures and electronic records. Parties should be free, on an informed basis, to establish by agreement the terms and conditions (including choice of law rules and rules of liability) on which they will use and accept electronic signatures for purposes of contracting and otherwise. The ability to vary electronic signature rules by agreement will enable parties to be responsive to the needs and demands of the marketplace, and will thereby facilitate the growth of electronic commerce. *H.R. 1714 generally is consistent with this principle, although the language of the bill's party autonomy provision (*§ 101(b)) warrants limited revision to clarify its applicability to all terms and conditions on which parties will use and accept electronic signatures. BSA has attached suggested language to clarify this provision.

(8) **Electonic Agents.** Federal legislation governing electronic signatures should encompass signatures; generated by so-called electronic agents—that is, by computer programs that initiate or respond to messages without human intervention—in business-to-business transactions. Electronic agents already are in widespread use in systems where they effect transactions on behalf of principals, who have created such agents and authorized them to act on their behalf (*e.g.*, in online supplier and data exchange systems). As electronic commerce grows, the use of electronic agents is expected to become even more prevalent, for electronic agents facilitate more efficient conduct of online commerce. Within this context, if electronic commerce is to reach its full potential, electronic signatures generated by electronic agents must be given the same legal effect as electronic signatures generated by principals themselves. *It is unclear whether H.R. 1714 in its current form encompasses electronic signatures generated by electronic agents. BSA has attached suggested language to make clear that electronic agent-generated signatures are covered by the bill's provisions.*

CONCLUSION

H.R. 1711 appropriately recognizes that, for electronic commerce to achieve its potential, transparent and predictable legal structures must be established that support global business and commerce. BSA supports H.R. 1714, and appreciates the opportunity to provide its comments on this important piece of legislation. BSA's member companies and its staff stand ready to serve as a resource for the Subcommittee and its staff with regard to BSA's suggested revisions and any other issues relating to this critically important topic.