Should Our Government Control Encryption Technology?

A conference presented by
the Economic Strategy Institute and
Computer and Communication Industry Association
at The Hyatt Regency on Capitol Hill
Washington, D.C.
October 8, 1997
Panel 1: The Technology

Matt Blaze
Principal Technical Staff Member, Secure Systems Research, AT&T Laboratories
Art Goldberg
Co-Founder and Vice President, Entegrity Solutions
Philip R. Zimmerman
Founder and Chief Technology Officer, Pretty Good Privacy, Inc.

John Scheibel
Vice President and General Counsel, Computer and Communications Industry Association (moderator)

MR. SCHEIBEL: There is no shortage of interesting questions surrounding the technology of encryption. One of the most critical of these questions was posed by Congressman Peter Deutsch of Florida at the recent House Commerce Committee markup of H.R. 695, the SAFE encryption bill.

The committee was considering an amendment, offered by Mr. Oxley of Ohio, that would have prohibited the domestic manufacture, sale, and importation of any encryption product unless it gave the government immediate access to the plain text of communications and stored files without the knowledge of the user.

Mr. Deutsch asked Mr. Oxley whether the technology presently existed to comply with his amendment. Mr. Oxley never answered the question. The amendment was eventually defeated by a vote of 35 to 16.

Mr. Deutsch's question is extremely important to the encryption debate, and it raises a series of related questions. Does the requisite technology exist to implement key recovery on a scale that the Oxley amendment would have required? Can such a system be implemented so as to protect the confidentiality of sensitive information reliably? What problems are associated with the vast number of keys that would have to be created and retrievable immediately? How much would it cost to implement such a system, and how would the cost be borne? I look forward to having this panel address these and other questions.
Now, if I were cynical and not the objective, impartial moderator, I might say that the FBI, which inspired the oxley amendment, wants to require U.S. high-tech companies to make only a form of encryption for which a technology does not exist, and for which the consumer demand has not been demonstrated. However, because I am not a cynic and the objective, impartial moderator, I will not make such a statement.

If I were a cynic, however, my cynicism might not stop there. If you had told me, in the midst of this highly-charged, extremely contentious, take-no-prisoners encryption debate, that policymakers were going to be presented with a report by a balanced, thoughtful, highly expert blue-ribbon panel that has full access to all the relevant information, classified and unclassified, and that this report would make substantive recommendations, I would have told you that this report might change the debate and help them resolve the issue.

Amazingly, there is such a report. It was issued last year by the National Research Council. The panel was chaired by Ken Dam, deputy secretary of state under President Reagan. It included Benjamin Civiletti, former attorney general, and Anne Caracristi from the National Security Agency, among a large number of other experts.

The report reflects a consensus of the panel. It raises important questions regarding the technology of key recovery, and it finds that aggressive promotion of key recovery is not appropriate at this time, for several reasons. First, the panel found that the operational complexities of large-scale infrastructure are significant, especially in the international context of cross-border communications, and a prudent approach to policy would be to develop a basic experience that would guide policy decisions on how key-escrow encryption might work on a large scale in practice.

Second, the panel stated that it is not at all clear that escrow encryption will be a real solution to the most serious problems law enforcement authorities will face, because criminals – those most likely to have information to conceal – will be motivated to exploit technical circumvention of escrow encryption.

Third, the panel found that the parties whose needs may call for the use of escrow encryption will need confidence in the supporting infrastructure before they will entrust sensitive information to the safekeeping of others. The best way to convince users, the panel said, that these agents will be able to live up to their responsibilities is to point to a body of experience that demonstrates their ability to do so. To create such a base of experience, the panel urged the U.S. government to explore the viability of key escrow on its own systems.

Now, if I were cynical, I would say that, because these findings were unwelcome in some quarters, there has been an attempt to sweep this report and its recommendation under the rug.
Because I am not cynical, however, I assume that there is some other explanation for the administration's unwillingness to heed the advice of that blue ribbon panel.

Today, we have with us our own blue ribbon panel. I will introduce them at the beginning, and they will speak in the following order: Matt Blaze, from AT&T labs; Phil Zimmermann, the founder and chief technology officer of Pretty Good Privacy; and Art Goldberg, a cofounder and vice president of Integrity Solutions.

After these gentlemen have finished speaking, we hope to allow ample time for questions.

MR. BLAZE: Thanks. I'm Matt Blaze. I work as a research scientist in the area of computing and communications security. In particular, I study the use of cryptography to build large-scale, secure systems. By large scale, I mean the scale of the telephone system, for example.

Cryptography has become a hot topic. There are certainly people in this room who had not heard of cryptography as recently as a few years ago. Now, we find that this is an important issue for policymakers in Washington, who find it important enough to listen to technical people, like me, talk about how we think on this issue. This is certainly flattering for me, as a technical person, suddenly to find that people in places like Washington are actually interested in what the technical community has to say.

On this issue, I think it especially important that we do this, because cryptography is a deceptively simple issue. By that I mean that we often discover, in the research world, that many things that seem obviously true about cryptography turn out to be false, and many things that are obviously impossible turn out to be quite simple. Things are almost never what they appear to be at first blush.

The solution to the cryptography problem that has been posed by government has been variously called key escrow, key recovery, and trusted third-party encryption over the last few years. There have been technical differences between these systems but, fundamentally, they share the same important property, which is the provision of a secondary path that allows messages to be decrypted, possibly without the knowledge or consent of the parties to a message. This would be used, for example, by law enforcement or some other party who has reason to get to the clear text of a message, but does not have access to the original key with which it was encrypted, because they were not a party to the original communication.

The idea of key-escrow security is that we would store somewhere, possibly split among a number of parties, a copy of a secret that can be used to decrypt messages. Then, when we put this secret together, we can recover encryption keys. It sounds like a very promising solution to a very difficult public policy issue, which is: how do we allow access for law enforcement without allowing criminals and other bad people to
take advantage of the same mechanism that law enforcement would use to read encrypted messages? How can we allow access for law enforcement without also enabling new kinds of crime that cryptography would otherwise prevent?

Now, apart from the question of whether a key recovery or key escrow system is good public policy, the other important, fundamental question is whether this is a sound technical idea. Do we know how to do it? Do we know how to do it in a secure way? Do we know how to do it in an economical way? Do we know how to do it on the scale that would be required by the likely deployment of encryption in the near future?

Last fall, a group of eleven cryptographers and computer security researchers - Hal Abelson, Ross Anderson, Steve Bellovin, Josh Benaloh, myself, Whitfield Diffie, John Gilmore, Peter Neumann, Ron Rivest, Jeff Schiller and Bruce Schneier – formed a group to study this question narrowly, the question of whether key-escrow systems are feasible, based on the government's stated, and likely, requirements and objectives for them.

In May, we published a report, about twenty pages long. There are copies available outside, for those of you who have not seen it. It is excellent bedtime reading, and I recommend it to all of you. It dissects the question of what the technical implications of key recovery are. What risks are introduced by key-recovery systems? What will the economic landscape for implementing this technology look like?

Now, to understand our report, it is important to document the context in which encryption will likely exist during the very, very near future, the next one-to-five years. Paradoxically – and this is one of the first paradoxes of secure systems cryptography – technology is improving at an absolutely stunning rate, but almost all of the improvements come at the expense of intrinsic security. We have things like the Internet, and personal computing, and so forth, that would have been unthinkable a few years ago. We say that technology is doubling in its capacity about every eighteen months, and that is likely to continue for at least the foreseeable future. That is an exponential growth. Things evolve very quickly. Paradoxically, however, cryptography, the only technique we have for restoring security to communications and computing technology, is becoming fundamentally cheaper and faster and better, but it is also becoming less and less secure.

It is extremely likely over the next one-to-two years, therefore, that cryptography will cease to be something specialized, something available only to people with special security needs, such as governments and large corporations. Rather, it will become broadly integrated across things like the entire Internet, and across the telephone system. Cellular telephones are an obvious application, where we are likely to see a strong need for encryption very soon, in order to protect fundamental privacy issues. So, cryptography is intrinsically going to exist on a very large scale.
Now, we looked at the government's requirements for recoverability of keys in the context of cryptography that is being used broadly across the nation's entire information infrastructure. I will not try to go through all the details of our twenty-page report. It is beautifully written, I must say, but I can guarantee that it will put you to sleep. Let me just outline briefly what we concluded was inevitable.

Key-recovery systems are relatively easy to specify but extremely difficult to implement in practice. It is very difficult to design, even on a theoretical level, the complex interactions required to ensure access by a third party, who is authorized by a court, and prevent access by a fourth party, who is not authorized.

So, designing a secure system on a theoretical level is a difficult problem for which we have yet to see a strong solution.

On an engineering level, the problem becomes far harder. That is, on a theoretical level, we do not know how to solve the problem of key recovery. On an engineering level, the problem appears to be virtually intractable.

Key recovery intrinsically makes systems less secure, because it gives an extra path to plain text that would not otherwise exist, and that extra path has associated with it very complex requirements for when it can and can not be used. Controlling the extra copies of keys that have to exist far longer than the keys used for ordinary traffic, and the keys that exist without a key-recovery system, makes an intrinsically inexpensive technology into an intrinsically expensive one, requiring a great deal of external infrastructure.

Scale makes this problem harder, in that the number of potential entities that have to be identifiable quickly makes the problem one that simply cannot be reliably solved in the time constraints the government is talking about. Even if we imagine relaxing the government's requirements considerably, we still do not know how to engineer secure systems that implement key recovery.

I will leave you with the final word of our report, which is that we believe key-recovery systems, as envisioned by the government, are well beyond the current competency of the field of computer and communications systems. I would like to ask the policymakers in the audience to consider the question of whether it is wise to base public policy on the existence of a technology that does not appear feasible with the current state of the art.

Thank you.

MR. ZIMMERMANN: I am going to talk about something that is fairly controversial right now, because we just released a product that does message recovery. At least, we call it message recovery, but, in some ways, it resembles key recovery, in that it provides another path to get to the plain text. We just did this a few days ago,
and I have been answering some questions about it, so I will include that in my presentation here.

We looked at various key-recovery schemes that are in products, and some of them were designed that way in order to get export licenses, which means that they had to meet government requirements for government access to keys. We did not have that as our requirement, but, instead, we had to deal with the problem of companies getting access to messages, or files, when the person who controls the key may not be in the company any more, might be on vacation, might have gone down in an airplane crash, or is just otherwise not available.

Also, sometimes people forget their pass phrase. I get a couple of pieces of e-mail each week from people saying, "I forgot my PGP pass phrase. Is there some way you can help me? I would even be willing to forgo a couple of weeks of intensive computing on my pentium, if there is anything you can do." I just tell write back and tell them to contact psychic friends. [Laughter]

That is a sad thing to happen to an individual but, when it happens to a company, it could involve enormously valuable, intellectual property assets of the company. It could be all of the documents of a law firm. It could be something that could bring down the company and many of their clients. So, there must be a way for a company to get access to the plain text through keys that it controls. If this requirement is not met, it will not be feasible to get cryptography into corporate environments.

So, it was with that requirement that I came up with the scheme that involves message recovery requiring the consent of both parties. It is a sort of kinder, gentler approach. The way it works is that, when you generate your key, you have to give your consent to include a pointer to another key entitled to decrypt your messages. In fact, in order to make sure that you really are giving your consent, you are required to create a digital signature giving that consent with your own key that you just created.

Therefore, when you publish your key, it has embedded in it a pointer to another key, a message recovery key. That key is typically controlled by the corporation for which you work. Hopefully, it will not be controlled by a government. You really should not give your consent to something like that, unless you want to, and I do not know why anyone would want to.

So, you publish your key, and other people who want to use your key download it from a server and try to use it. When they do so, they discover that they need another key in order to use this key. They have to download the message recovery key as well, and, when they use our product, there is a window that indicates who is able to read the message. Both the name of the intended recipient and the name of the message recovery agent show up on the list of people who can read the message.
Now, we have a business version and a personal version of the software. If you are using the personal version, you can remove from the recipient list the extra recipient, the message recovery agent's key, thereby not participating in the scheme.

If you are using the business version of the software, it can be configured by your system administrator so that you cannot ignore it, so that you must adhere to it. On top of that, the message recipient who generated that key can have a kind of strictness flag that indicates whether or not it is okay with him for you to remove the key. If he consents to that, as kind of an advisory field, then you can still remove it. So, there is an escape route for a lot of circumstances, something you do not see in a lot of message recovery schemes or key-recovery schemes, certainly not in the clipper ship and not in any of the other software key-escrow schemes I have seen.

I think that, typically, in most business environments, for communications that involve intellectual property assets of the company or documents that are business documents, purchase orders, invoices, and what have you, people are going to use the feature, and companies will be able to have access to those documents, should somebody go on vacation or otherwise become unavailable.

However, if there are some particularly extraordinary circumstances, or perhaps personal communications, there are ways around it. Our customer response to this has been pretty positive. Particularly in the case of the business edition, it allows the administrator to specify that you have to use this all the time. This is a subject of some controversy, but there is no other way we could think of to meet business needs and still have a flexible system that fits our sense of social responsibility.

Now, it so happens that we started working on this quite a few months ago and just last week released the product. We did it on schedule, but we did not anticipate in our schedule a few months ago that last week would be the time when there would be so much controversy raging in Congress about message recovery or key-recovery schemes.

I do not know whether our product would scale on the level that Matt Blaze was talking about, on a nationwide scale. It is really intended just for little companies of maybe a few thousand employees, because those are our customers.

So, we have a scheme that is under customer control. It is not necessarily always under the end-user control, but under the customer control, the customer being defined in this case as the one who paid for the software, which means the company itself.

Now, there is one other observation I will share with you. I learned something about the politics of this. I found that it is really hard to try to do business in the field of cryptography. The reason, it seems, is that there is tremendous power in the technology of cryptography, and this power is being sought by different factions. There are end users, who want the power of their personal privacy. There is corporate America, or
any corporations, really, who want the power to conduct their business and get access
to their files and not to have their files encrypted in a way that they can not get to. Then
there is government regulatory pressure, because governments want to have access to
keys for law enforcement purposes. All of these competing interests, in some ways
mutually exclusive, are tugging the technology this way and that way.

Trying to build a high-technology business, to make a new disk drive or
something, is hard enough, but, when you are trying to build a business on a
technology that is being pulled by different market pressures or regulatory pressures, it
can be incredibly hard. I suspect that is why there are not very many successful
companies in this field. That is a lesson we have learned in this, particularly looking at
this message-recovery feature.

Thank you.

MR. GOLDBERG: For those of you I have not met before, my name is Art
Goldberg, and I am from a company called Integrity. It is not a household name, like
AT&T, and it is not written about as frequently as PGP, so let me spend a minute
telling you what our focus is and, therefore, why I have some background to speak on
the issues facing this group.

Integrity is bent on providing to the enterprise customer the capability to
integrate security capabilities into their applications, over a broad range of application
types and a broad range of issues that large enterprises, in particular, but also
enterprises in general, are dealing with. The first thing we did when we formed the
company was to acquire a Swedish company that, over the prior five years, had
developed a variety of encryption products and security products.

With that background, I would like to address some of the misconceptions I
heard discussed in the hall and declared from this platform and in other forums. The
first misconception is that the United States has the corner on cryptographic capability.
That is patently false. Cryptography is really mathematics, and mathematics is a pretty
universal language. Anyone who wants to know how to do encryption, if they are
intent on doing it, can buy Bruce Schneier's book. He publishes just about every one of
the most popular, and some of the less popular, encryption techniques, or encryption
formulas. Most first-year computer science students could do an implementation. They
might not necessarily do an effective or an efficient implementation, but they could do
an implementation of those cryptographic capabilities.

As it turns out, there are probably three centers of cryptographic expertise in the
world today. One is still in the United States. That is a residual the government is
trying to do away with. The second is in Sweden. We and several other companies
focused on security have principal development capabilities in Sweden. The third turns
out to be Israel, and a number of the commercial products that are coming to market
are coming out of Israel as well.
So, you can get strong cryptographic capability elsewhere in the world. It is easy to implement. Even in commercial products, it is inexpensive to implement. Therefore, you cannot control it by saying, "We are not going to allow it to be exported from the United States."

The second misconception is that bad guys are a greater threat using cryptography to promote their bad ways than they are in gaining inappropriate access to sensitive data, such as corporate secrets, trade secrets, design information, financial information, and other information of that sort. That is patently false. The real losses being suffered by corporate espionage are far greater than the exposures being realized by terrorists sending secret messages with cryptographic capabilities.

The third misconception is that the bad guys would actually adhere to a policy requiring that, if you are going to use cryptographic capability, you have to give someone else the vehicle to get at that information. That is patently false as well. That is like saying the bad guys should not own guns. They don't pay any attention to that. They are breaking the laws in the first place. It is nonsense to believe that they are going to adhere to, and pay any attention to, a law or requirement that they escrow their keys so that someone else can gain access to them.

That brings me to the fourth misconception, the one of greatest concern to me, and that is the misconception that this issue is a simple one. I heard John and others make that comment, but the fact of the matter is that this is not simple. It is a complex area, because cryptographic capability and cryptographic technology can be used for a large number of things, and how you apply it to do good things in a business context, or an institutional context, is not a simple task.

As proof, I will tell you about our efforts to trot our business plan around the venture capital community for second-round funding. Usually, these are reasonably intelligent people, but when we start explaining to them what security is all about and what the technology is to implement that security, we have seen more glazed-over expressions than I care to see in the rest of my lifetime. I notice some of those people here today.

So, I will spend the next few moments doing the impossible, which is what the folks from CCIA have asked me to do, and that is to explain this simple technology to you in eight minutes, four of which are already gone. I will just hit the highlights, then.

First of all, cryptography is not cryptography is not cryptography. There are different types of cryptographic capabilities. One type of cryptographic capability involves asymmetric key pairs and asymmetric encryption. Very simply, this means that the key with which you encrypt a message is different from the key with which you decrypt the message. In fact, they are paired. Hence, the term "key pairs." The one you use to encrypt the message is paired with a private key that you do not share with
anyone else, and with which you can decrypt the message. For example, if I generate a key pair for an individual, I publish what I will call the “public key.” I keep the other key hidden, and I will call that the “private key.” I can send a message to that individual encrypted in their public key, and only they, or anybody with access to the private key, will be able to decrypt that message. To everyone else, it will look like gibberish.

There are a number of public-key-pair techniques. One was developed by RSA. Another was developed by Diffy and Helman. A third one coming on the scene is called elliptic curve. They differ only in the mathematics used to generate the asymmetric key pairs, and the speed with which you can perform the actual function of encryption. In theory, elliptic curve can provide the same level of protection. That is, it is difficult to break the algorithm with fewer bits and, therefore, it is a more efficient algorithm. There are some benefits to RSA, some benefits to Diffy-Helman. The biggest benefit to Diffy-Helman is that it is in the public domain and, therefore, readily available to anyone who wants to implement that algorithm.

Asymmetric cryptography is really only good for encrypting small amounts of information. It is not very good if you take an encyclopedia and try to encrypt it. In essence, it is a very inefficient lock cipher, or streaming cipher. If you wanted to hide some really small information, then this public-key capability would be very, very effective. You can publish the public key of everyone, and only the individual with a private key can decrypt it. It is a very useful technique.

The second type of encryption is symmetric-key encryption, or secret-key encryption. Basically, this is an algorithm, a formula used to scramble information, with the same key being used to encrypt the information and decrypt the information. As a consequence, if I were to use it to transfer information from one place to another, I would have to ensure that the secret key for the symmetric algorithm is at both ends. This was the earliest form of encryption used. One example of it was something called the “Lucifer algorithm,” which was used in automated tele-devices made available by IBM back in the 70s. That, then, got picked up by the government and was published as DES, the Data Encryption Standard.

Basically, there are a number of other such encryption algorithms that are very good for encrypting large amounts of data. In many instances, they are streaming, so you put data in the front end and it comes out the back end, and you keep on putting information in the front end, so your delay in terms of the unencrypted version is minimized with the use of these algorithms.

In many instances, these two things are used together. For example, if I wanted to send you a large message, I might create a secret key, encrypt the message, then encrypt the secret key – or envelope it, if you will, using your public key – and then send you the secret key. You open the envelope, take out the secret key, and then you can decrypt the message.
The third type of encryption is something called hashing. Hashing is not really encryption, per se. It is a way of digesting a piece of information or block of data and getting a unique representation. The neat thing about hashing is, if you change the data being hashed, the result will be different. If nothing has been changed in the document, then the hashes will, in fact, match. The hashing algorithms are readily available. So, if I send you a piece of data or a letter, and I have hashed it, I send you the hash. You could hash that same thing and tell whether or not that document has been tampered with. It is a very, very useful capability.

It turns out encryption can be used for a number of other things, as well. Phil mentioned that it could be used for signing documents. If I were to send you a letter, I could hash it, and then sign the hash. By "signing," I mean that I actually encrypt it using my private key, okay? Since my public key is readily available, you can decrypt using my public key and verify that, in fact, it came from me and was signed by me. Then you can verify the hash and make sure that the document has not been tampered with or altered.

Another concept is public-key infrastructure. If it seems simple to you to generate public keys and hand them out, that is probably true. Actually, building an infrastructure for managing the distribution, revocation, and verification of public keys, and a document with which I can transport these things, is much, much more complex. First of all, you have to ensure the integrity of that chain within the public-key infrastructure. We are probably not going to issue keys in only one place. That would be totally unmanageable. So, you are going to have a distributed infrastructure where a variety of organizations and entities can issue keys. It is a very complex problem to find a way of verifying that, in fact, a key is a legitimate key, issued to a legitimate person, still valid, and has not been tampered with or absconded with.

Therefore, when the government of Singapore, for example, talks about implementing a public-key infrastructure for all the citizens of Singapore, it becomes a massive administrative problem and a massive systems problem, in terms of how you actually issue the keys in the first place, and then how you maintain and distribute information about those keys in a secure way over time.

One more concept is the token. Has anybody ever heard of a token? I can generate key pairs and distribute them with a bunch of other information, such as your name and affiliations, in something called a certificate. The thing in which I store that is called a token. A token could be something like the hard disk on your personal computer. That is not a very secure environment, because people can hack into it and, therefore, gain access not only to the public information in the certificate, but also to your private key pair.

You could also store it on a floppy disk that you remove from your personal computer when you use it. That is reasonably inexpensive and somewhat more secure,
but it still has the disadvantage that, if someone gains access to that floppy disk, it can be read and, therefore, someone could gain information necessary to decrypt other information sent to you using the public key.

There are two other alternatives. One is a plug-in card in a lap top, which might be a PCMCIE card on which the certificate is stored, or your key-pair is stored, but where the hardware capability, in essence, prevents you from actually reading that information once it is written onto the card. So, it is a write-only for portions of the card, and your private key, in fact, can be stored in there but not be retrieved and, therefore, compromised.

There is also a simpler version of that plug-in card, called a Smart Card, which, in essence, looks like a credit card and has a microchip on it, which, in fact, also has that same capability of storing this information, including your private key. Many of these chips have the capability of actually executing the encryption algorithms...[tape was turned over at this point]...hard, and never bring the private key out into any space, including your computer, where it might be compromised.

One other concept I want to talk about, because it seems to play into policy, is encryption strength. There is a myth going around that it is okay to have forty bits, but if you go to fifty-six bits, you had better tell someone else what you are doing. If you use anything more than that, then you are really strong, and that gives the government problems, because they really can not break it.

First of all, encryption strength is not a direct function of bit length. It is a function of two factors, the encryption algorithm and the bit length. So, for example, in the public key/private key, the number of bits you need to be secure when you use the RSA algorithm is different from the number of bits needed to gain that same level of security using elliptic curve algorithms.

The other thing is, in that study to which Matt referred, their conclusion was that anything short of ninety bits today, using the mathematical algorithm, is relatively insecure. What does that mean? It means that, with available technology, you could break that algorithm and, therefore, gain access to information that people believe to be safe.

So, hopefully, I have given you at least an understanding of some of the terminology and some of the technologies that are being used to implement encryption, and of the security products that are dependent upon having that encryption capability.

MR. SCHEIBEL: Thank you, Art. I think we have time for just a couple of questions. I have one question, and that is, has there been any use of third-party key-recovery on any sort of large scale? What is the largest scale we have experience with?
MR. BLAZE: Let me address that. Again, one thing that is important to understand is the distinction between key recovery as envisioned by the government and the key-recovery requirements that may exist within enterprises that are using encryption in general. Part of the difficulty here is that the applications of cryptography, when they do demand key recoverability, tend to require only very small-scale, limited key recovery. It is much easier to manage. These key-recovery systems still make the system intrinsically less secure, but they can be managed on a scale that limits the potential for damage, particularly in the choice of when keys are recoverable and when they are not, and when a recoverable key is to be destroyed.

In particular, the distinction between stored data and communications traffic is absolutely critical for understanding this issue. Obviously, stored data that is used for the operational records of a company, or the individual records of a person, such as financial or tax records, is associated with the trade-off between secrecy and continued availability. If I lose the key to my office, my company does not just wall up that section of the building. In similar fashion, if I lose the keys to my documents, I want some assurance that I can get to them at some point in the future. So, I might deposit a copy of my document keys with some corporate information officer, or with a trusted friend, or with my boss. Then, if I get hit by a truck, AT&T can still get access to my information, and discover what they were paying me for in the first place.

In the case of communications traffic, though, this need simply does not exist. Communications has a relatively interactive property. The sender of the message sends it, and the receiver receives it – immediately in the case of telephone calls, and relatively quickly in the case of e-mail – and discovers whether they have the correct decryption key. If they do have the decryption key, fine. They decrypt it, and they have the clear text. If they do not have the decryption key, the communication fails, and both parties suddenly discover that they no longer have the correct keys. If that happens, you just generate a new key and start over. You don't ever need to recover a key that was useful in the past, in the case of communications traffic.

So, the large-scale systems tend to be in the arena of communications, rather than storage. Stored data is an intrinsically small-scale problem, an intrinsically local problem, because even access to the cipher text tends to be localized. Communications, on the other hand, tends to be a much-larger-scale issue. However, because key recovery is not required by users of communications systems, we do not see large-scale key-recovery systems being proposed by anybody, because nobody wants them.

Now, the government is saying that it wants them, so there is some question of designing these systems.

So, that is probably more than you wanted to know.
MR. SCHEIBEL: Not at all. That was a great distinction. Are there any other questions? We have time for one more. Okay. Please join me in thanking this panel. This was just a wonderful explanation of the technology.
**SPEAKER AND MODERATOR BIographies**

Art Goldberg
Co-founder and Vice President, Sales and Business Development, Entegrity Solutions

Mr. Goldberg is a member of the founding team of Entegrity Solutions Corporation and is responsible for Sales and Business Development. Prior to joining Entegrity, Mr. Goldberg was Executive Vice President of HAL Computer Systems, responsible for all of Sales, Marketing Customer Support, Business Development, and Strategic Relations. He also was a member of the Board of Directors of SPARC International.

Previously, he was the President and CEO of Atherton Technology, a software company which developed and marketed CASE products. Mr. Goldberg spent 24 years at IBM holding many managerial and executive positions, including, Director of Workstation Strategy, and Director of Development Operations for the RS/6000 and AIX products. He is a graduate of Brooklyn College with a BS in mathematics, and did graduate study at the University of Chicago and City University of New York. He currently is a member of the Board of Directors of APM, ltd., a software and consulting company based in Cambridge, UK.

**Philip Zimmermann**
Chief Technology Officer and Founder, Pretty Good Privacy

Before founding PGP, Philip R. Zimmermann was a software engineer with more than 20 years of experience, specializing in cryptography and data security, data communications, and real-time embedded systems. Clients for his cryptographic services included Silicon Graphics, IBM, Sun Microsystems, TCI, Cable Labs, Reuters, Hewlett-Packard, Hughes, Allied Signal, First Virtual Holdings, FTP Software, Destron-Fearing, and others.

He has received numerous technical and humanitarian awards for his pioneering work in cryptography. Most recently, he received the 1996 Norbert Wiener Award from Computer Professionals for Social Responsibility for promoting the responsible use of technology. He also received the 1995 Chrysler Award for Innovation in Design, the 1995 Pioneer Award from the Electronic Frontier Foundation, the 1996 PC Week IT Excellence Award, and the 1996 Network Computing Well-Connected Award for "Best Security Product." PGP was selected by Information Week as one of the Top 10 Most Important Products of 1994. Time Magazine also named Zimmermann one of the "Net 50", the 50 most influential people on the Internet in 1995.
Zimmermann received his bachelor's degree in computer science from Florida Atlantic University. He is a member of the International Association of Cryptologic Research, the Association for Computing Machinery, Computer Professionals for Social Responsibility, the League for Programming Freedom, and the Union of Concerned Scientists.

**John Scheibel** - moderator
Vice President and General Counsel, CCIA

Mr. Scheibel brings to CCIA 18 years of experience in high level policy, legal, and management positions within the Executive and Legislative Branches of the United States Government. He has a proven record of achievement in Congress and regulatory agencies, and an in-depth knowledge of the legislative process including the ability to conceive, write and gain passage of complex legislation. Mr. Scheibel has knowledge in such high-tech issue areas as intellectual property, and telecommunications policy and he gained particular expertise in export controls and encryption serving as Chief Trade and Foreign Policy Advisor to Congressman Sam Gejdenson. He is also an experienced litigator in Federal court on Constitutional and statutory questions and has appeared before administrative tribunals in defense of agency technical standards.

His professional background includes positions as Minority Counsel (1995-Pres.) as well as Staff Director and Chief Counsel for the Subcommittee on Economic Policy, Trade and Environment, House Foreign Affairs Committee (1989-95); Staff Director and Chief Counsel for the Subcommittee on Oversight and Investigations of the House Committee on Interior and Insular Affairs (1987-89); Associate General Counsel of the Federal Emergency Management Agency (1983-87); and Assistant General Counsel of the Federal Emergency Management Agency (1979-83).

Mr. Scheibel is a graduate of George Washington University Law School and holds a BA in History from the University of Rochester.
Panel 2: Encryption's Uses and Values

Joel Lisker  
Senior Vice President of Security and Risk Management, MasterCard International  
Bill Poulos  
Director of Technology Policy, EDS Corporation  
Clint Smith  
Deputy General Counsel, UUNet  
Bill Wiedemann  
President and Founder, RedCreek Communications

Aaron Pressman  
Reporter, Reuters (Moderator)

MR. PRESSMAN: This panel of business people is scheduled between an earlier panel of technology people and a later panel of policy people, because whatever may be technologically feasible or politically desirable will still have to meet the market check of what people actually want to use and what they will pay for in the market.

As we all know, predicting the course of markets, or where the economy might develop, is a very difficult task. For instance, ten years ago, the Internet was not foreseen by most people as a mainstream phenomenon. Alexander Graham Bell, it is widely said, thought the telephone would be useful only for small business-to-business transactions, such as the telegraph was used for. When Xerox invented the copier in the 60s, they had a market research study that said there would be a total market in the United States for 5,000 Xerox machines, total.

Furthermore, a technologically preferable solution is not always the one the market chooses. We all know about the Betamax and the Macintosh, which are not the market leaders, although they were perhaps the technology leaders.

Unfortunately, policymakers in Washington do not always get this particular aspect of regulating technology. I was very moved when Sam Gageson spoke at the International Relations’ mark-up of the SAFE bill and pointed out several instances where restrictions on U.S. technology have simply pushed it all overseas.

Today, we will hear from four people who use and sell encryption. We will hear what customers want in their encryption and, more importantly, perhaps, what they are willing to pay for in their encryption.
We will also hear a little bit about that famous question of whether the genie is out of the bottle, whether the cow is out of the barn, et cetera. What is the competitive picture on encryption? When a company is seeking a product, to whom can they turn outside of the United States if they want?

On the panel today is Joel Lisker, senior vice president of security and risk management at MasterCard International; Bill Poulos, director of technology policy at EDS Corporation; Clint Smith, deputy general counsel of UUNet; and Bill Wiedemann, president and founder of Red Creek Communications. We will begin with Joel.

MR. LISKER: Thank you, Aaron.

Let me just say at the outset that my background is out of the FBI originally, and then with the Justice Department, in the internal security area. I go back to the time of the one-time cipher pads in the AFSAM-7, and to a much more primitive environment, an environment that we were all comfortable with, because it was pretty easy to bag those operations and recover whatever data we needed.

We are in a whole different world now. As has been said very well by the preceding panel, it is an extraordinarily complex world. Factually, it appears attractive for those who would look for a simple way to recover escrow, but, as I will try to explain, in terms of MasterCard's position, it gets very complex very quickly.

We place the highest priority on working with the federal government. Last year, MasterCard received the first Secret Service partnership award for its work with the Secret Service. We work closely with the Federal Bureau of Investigation. Both organizations in the United States are real allies in the fight against credit card fraud.

We also work with other services. We work with the German services, the Saudi services, the Israeli services, the French services, the Libyan services and the Iranian services. I realize that we have both friends and enemies in that list, from a political perspective, but there are no enemies in the ugly world of business. Everybody is a friend, because, potentially, they are a customer.

So, if you try to keep that perspective, you will understand that what the FBI or other law enforcement may be seeking to accomplish in the SAFE legislation, or similar legislation, would open the door to others who might share that concern and wish to engage in the same sort of recovery practice.

We use encryption in a variety of ways. First of all, we obviously use encryption in communications, to promote the integrity and ensure that whatever has been sent has not been altered.

In MasterCard's world, however, we use encryption to verify personal identification. Everybody has gone to an ATM. Everybody understands the fact that,
when you enter your PIN number at the ATM, assuming you remember it and you have not written it down on the back of your card, and there is no one holding a gun to your head and trying to extract it from you, that tends to identify you as the person authorized to access that deposit account.

We also use encryption as a card validation code. In 1994, fraud on MasterCard products was at 17 basis points. That is seventeen one-hundredths of one percent. It is now at 7.5 basis points. The reason for that success in reducing fraud is that we developed something called CVC, the card validation code, which appears in track one and track two of the mag stripe in the discretionary field. The card validation code is an algorithmically derived value based on the sixteen-digit account number, the expiration date and the card type, whether it is a domestic card or an international card. That is applied against a secret algorithm known only to the issuer and placed on the magnetic stripe.

For those who would do what we call dumpster diving, going into the trash and trying to extract copies of sales drafts, or recovering them at gas pumps or ATMs before truncation of the account numbers on the sales drafts, that was an easy way to counterfeit cards and engage in fraudulent transactions. Now, of course, with the Internet, with Credit Master and some of these other programs, a sixteen-digit account number and the check digits can be derived and put on a card. The problem for the crooks is that they do not know the CVC and there is no way they can get that off the Internet, or anywhere else, except by breaking into the secret code of the issuer. As a consequence, the counterfeiting has dropped like a rock.

So, in terms of the fraud that we were experiencing, in the whole world of fraud today there is probably a billion-and-a-half dollars. That sounds like a lot, but we are talking about MasterCard, Visa, Discover, JCV, Amex, and Diners outside the United States or Citibank inside the United States. This represents several trillion dollars worth of transactions, so the basis points are very, very low.

We use encryption for message authentication data. We have to settle our transactions daily, and ensuring the validity of the transactions is part of our day-to-day process. We are talking about tens of millions of transactions every day, just in the MasterCard world.

We use encryption for emergency card replacement. If you lose your card and you need a card, and you are traveling in Europe, we have to get it to you the next day. That information to the card replacement center is encrypted.

We use encryption for electronic commerce on the Internet. MasterCard and Visa are accelerating that process. Everyone, I think, has heard of SSIT, which is the Secure Standard for Internet Transactions, commercial transactions.
Finally, we use encryption for the chip that was mentioned earlier. Here I have the Chase card, which came out yesterday. This is a Mondex product. MasterCard owns fifty-one percent of this company in the United Kingdom. The cryptography on this card, in a nonfinancial application, would be illegal to export. This chip is made by Hitachi, and to get these chips in personalized form, back from Japan, was a major problem recently. We really needed Britain and the United States to sign off.

Well, you can not run a business that way. We just can not. The bureaucracy is great – I was part of it – but it is not relevant to the business world.

Now, the fact is, as I mentioned, this is pretty robust stuff. It is RSA, and it is DIS. There will be a billion of these things out there in the next two or two-and-a-half years. It does stored value. You can do cash exchanges, transfer of money to a child or a wife, or a wife to a husband, as in my case.

MR. PRESSMAN: I thought it was husband-to-wife in your case.

MR. LISKER: No, my wife gives me the money. It does not work the other way. She controls it.

The fact, however, is that, if we were going to try to escrow these keys, we are talking about debit, credit, and stored value. We are talking about loyalty applications, and coupon applications, because paper coupons are going to go away. We are talking about five-to-seven applications – including health care applications and, possibly, national security applications. That is five billion sets of keys. Who is going to manage this? Who is going to deliver these keys to the trusted third party, who will probably be buried by them?

As keys change, and as cards get lost, the fact is that the only place these keys exist is in the card. So, you are going to have to go back to your Colombian drug dealer (who hopefully is not using our product, but maybe Visa's) and get the card in order to get the keys, because we do not have the keys.

The whole idea of the global key center is to generate the keys in order that we can have signing authority on applications that work on what is called a multiple application operating system, or Multas, which will be available the first quarter of next year. This will be the basis for all of these products that I have described.

Well, who does the government think is going to manage all this? Who is going to pay for it? How effective will it be? How efficient will it be? What reliability will there be, so that, when the time comes to recover the keys, the mechanism will actually be in place to allow that to happen in an emergency situation?

There are a lot of questions. I do not have any answers to them. They are just good questions.
The other point that concerns me is that we talk about financial transactions being exempted under the SAFE bill. I like SAFE, because I thought we owned that word. We have something called the System to Avoid Fraud Effectively, which is our fraud reporting system, the acronym for which is SAFE. I think we probably could have copyrighted it and maybe have stopped this thing in its tracks. However, the fact is that financial transactions, to the best of my knowledge, are not clearly defined, and the transactions that we are talking about on the Multas operating system will not be purely financial transactions.

Does this mean, then, that the United States will not produce these cards? Does this mean that, when you travel abroad with one of these cards, you have committed some technical breach of U.S. law? I hope not. This would really set back the clock quite a bit for the United States, if the industries associated with the deployment of this technology have to move development overseas.

We have 22,000 members worldwide. We have about 60 million terminals out there. We have about 300 million cards, not counting these cards. So, add a billion or so to that. We have an unspecified number of ATMs, hundreds of thousands of ATMs. We have partners in Europe. EuroPay is our major partner in Europe. We rely on our membership, who are subject to laws separate and apart from anything in the United States, to deploy and promulgate our products. If the United States begins the process of encumbering the commerce associated with this technology, who is to say who will step up next? The British are not far behind. The Canadians are not far behind them.

We haven't even gotten to the Germans. When we had our fax machines in the old days, I had an encryption device on our fax machines. We could not import that encryption device for the fax machine, which was sold commercially in the United States, into Germany. It violated German law.

So, when we start to create these barriers for ourself, who is to say where it will end and whether, in fact, it will not bring down this revolution that we are trying to create, in terms of this technology?

Thank you for your attention, and I will be ready to respond to questions.

MR. POULOS: Hi. I am Bill Poulos, with EDS. ESI and CCIA have asked us the question: Should our government control encryption technology? EDS's response is "No." I will tell you why.

As we begin to understand the opportunities created by the incredible growth of electronic commerce, significant attention is being paid to the economic benefits of electronic commerce, and we all know that they are huge.
Electronic commerce is defined as nothing more than the commercial transaction of goods and services in electronic format, using computers and software and networks. In short, electronic commerce is just trade, in a new media. The technology that enables electronic commerce has the potential to revolutionize the business environment. It means using global networks.

What about the risks, however? What about the vulnerabilities? How can we reap the benefits of electronic commerce, especially for a company like mine, which is doing business in over forty-five countries, with revenue approaching fifty billion dollars, and operating in about fifteen major industries? How can we reap the benefits of the Internet and the rapid growth of electronic commerce while not unnecessarily harming national security and law enforcement?

These are not easy policy issues. If they were, we would not be here, having this forum, today.

Rather than attempting to engage in any technical discussion about which encryption is better, or which authentication system might work best, I want to focus on two important issues that I think have to be satisfied if electronic commerce is going to develop and flourish and be something that we can all use. Those two issues are user trust and user privacy.

It is widely accepted that industry's role is to develop the information infrastructure necessary to support electronic commerce. Electronic commerce requires the development of a globally harmonized, highly interoperable approach to providing confidentiality, authentication, reliability, and availability of information on networks.

As industry and government debate laws for the future, we would all be well served to keep an eye on our citizens, our users, our customers' needs. Users are the market. Users will determine if electronic commerce is useful to them. Users will determine if the Internet is safe enough to buy things. Users will decide if there is sufficient confidentiality for their information. Users will decide if individual and business privacy is being adequately protected.

In debating the issues on encryption, we have to recognize that users must be able to trust the encryption made available to them in the marketplace. If customers do not have trust in that encryption technology, they will not be quick to buy our computers, to buy our software, and to use our networks. It is that simple. Users, our customers, must have trust that their information, which is their property, can be protected.

Information is property, and users have the right to protect it. There is nothing inherently wrong with key recovery, the trusted third-party message recovery we heard about earlier. It provides the ability to recover valuable information by someone other than the party that originally did the encryption. It provides a measure of safety
that many businesses will need. However, it is certainly not appropriate for all applications.

As national policies are created in this area, we must ensure that we do not build a global system of interoperable, lawful access, that makes it easier for some governments to misuse the law and engage in commercial espionage against our companies. I maintain that the Oxley-Matton amendment would have done just that. It would have made commercial espionage easier, not harder.

The question is, will users trust a national or global information system that provides immediate access for governments to all digital information without the knowledge or cooperation of the user? I doubt it. The challenge for all of us is to create interoperable national policies that allow users to exercise their rights to protect their information property and prevent crime in the first place.

If EDS believed that national policies restricting our access to unbreakable encryption would prevent criminals from having access to unbreakable encryption, we would think seriously about supporting such a policy, but no one has been able to make that case. Restricting the user’s right and the user’s access to strong encryption that the user can control does not stop criminals from having access to it and using it.

So, ultimately, the confidentiality, the authentication, and the reliability of information become an issue of user privacy and user trust. Users want to be able to choose the type and strength of encryption products necessary to secure their information. Businesses, also, have an added responsibility to their shareholders to secure their valuable information.

This is particularly true in the case of my company. Most of the information that we move around on global networks to over forty-five countries does not belong to us. Companies hire my company to process and to build the information systems so that those businesses can do business. So, we have to be able not only to protect our own information, but also that of our customers.

Government policies that would restrict development, distribution, sale, import or export of the users’ choice are not likely to support the development of electronic commerce or to enhance user trust. Such restrictive policies are more likely to become huge trade barriers, all well-intentioned, to provide for law enforcement and national security.

Electronic commerce is a rapidly growing phenomenon. Government and industry need to continue working together to find a resolution for what is obviously a gridlock. This can best be done, I think, by establishing policies that provide for truly market-driven, industry-led development of encryption products and services that users want and will trust. The real issue in this debate is user trust and user privacy.
I want to put up a slide that focuses on this issue. This slide shows an ad that EDS recently ran on the Federal Page of the *Washington Post*, about two days before the House Commerce vote on the Oxley-Matton amendment. The focus of the ad is whether government should have access to everything in your computer without your knowledge? If you read the text, the answer is no. Copies of this will be available on the back table, should you wish to read it again.

Thank you.

MR. SMITH: I am Clint Smith, deputy general counsel of UUNet. I have been asked to talk about market demand for encryption, and I am going to talk specifically about our internal demand for encryption at UUNet, which is the world's largest Internet service provider, and a subsidiary of WorldCom/MCI, the telecommunications giant.

I am also going to talk about consumer demand, and what our customers are telling us they need encryption for.

So, let us begin on the subject of UUNet demand. UUNet is a global company. We have subsidiaries in Canada, in the United Kingdom, and all over Europe. We also have Internet hubs around the world. These are not necessarily companies that we own, but they are facilities in which we locate routers and splitters and switches and hardware.

Now, it is very important that our global network be secure. It is equally important that our global network be uniform, that we have consistent equipment around the world. In fact, the global network is managed in Fairfax, Virginia, on Route 50. From there, we can add new software to the switch in Singapore and fix our bugs in France. It is all done from Fairfax. It all must be uniform so we can administer it easily.

We are running into constant problems with export controls. At times, we can get permission to ship equipment, other times we can not, and, even if we do get permission, it is a very expensive and burdensome process. I ask the policymakers here, what is the benefit of adding cost and prohibiting a U.S. company like UUNet from having a backbone that is secure from hackers, and that secures the information of our customers?

Let us consider what customers are asking for. The first thing they are asking for is firewalls. UUNet started its company selling simple Internet access, and then customers came to us and said, "Well, thanks for the Internet access, but how are you going to protect us from the horrible jungle out there called the Internet?"
The answer to that was, "Well, we will sell you encryption firewalls." We did not have time to develop them ourselves, so we resell other companies' firewalls, like DES, and Checkpoint Fire Wall 1, another market leader. We are selling thousands of these encryption firewalls to U.S. customers, but we have a problem: we cannot sell them to foreign customers. Similar products are available around the world. We cannot sell them to a Swedish pharmaceutical company, but the Swedes can certainly buy it locally.

The other area where we see consumer demand is what we call Virtual Private Networks. Virtual Private Networks allow you to secure sites around the world, and also to secure communications with people who are roaming. UUNet has two new products called ExtraLink and ExtraLink Remote, and they use two components. They use a Cisco grounder of about 112-bit encryption. They also use the Checkpoint firewall and Checkpoint client software, 56 bit or 40 bit, so that a traveling salesman, a telecommuter, or anyone who is on business in a foreign company, perhaps doing mineral exploration, can communicate with their home gateway in a secure manner. There is huge customer demand for this. Can we sell it in the United States? Certainly we can. Can we sell it to U.S. multinationals who have foreign offices? We can with great burdens. Can we sell it to a Swedish pharmaceutical company or a Brazilian chemical producer? No, we can not. Potential here for lost sales, and that.

I said I would delve into policy. I will be direct. What is good policy sense? First, we should do something that should have happened three years ago. We should grant immediate export relief to sell 56-bit encryption to any reputable, corporate customer anywhere in the world. For example, why can't we sell a 56-bit company firewall to Mercedes Benz? That should be automatic.

Second, we should establish the foreign-availability test. If software can be bought overseas, without restriction, from a foreign supplier, a U.S. supplier, such as PGP or UUNet, should be able to sell that same encryption software.

Third, we need to minimize the burden on exporters. Even when one can get export approval, one has to hire a Washington lawyer to get it, and that is not cheap. I used to be one, so I can say that. You also have to follow up by submitting all sorts of regular reports. You have to worry about re-export problems. You have to ensure that foreign national employees do not use your product for other purposes. These are tremendous costs. We need to think about this, and possibly scale it out to the Customs Modernization Act, where the Customs Service says, "Okay. This is to comply. We trust you to comply with the new requirements, and we will audit once in awhile if we want to, but do all the final performance and all the paperwork. It is just too costly in an industry where that is a great burden.

Finally, we should stop using export controls as a way of trying to promote domestic use of key-recovery encryption. If we want domestic use of key-recovery encryption, we should pursue it directly. We should not punish U.S. companies trying
to sell abroad by using export controls as a hook to establish the standard product, both in the United States and abroad.

As for UUNet's position on key recovery, I agree with Bill Poulos and Phil Zimmermann: there will be a need for key recovery. The question is, who drives the demand? Is demand driven by market forces, by customers who want something and by entrepreneurs who think they can build it, or is it driven by government mandate?

I think the answer is fairly simple: there should be no government mandate for key recovery.

Now, you might ask, "Well, isn't this going to be damaging? Isn't this threatening law enforcement?"

I do not think so. If you would take a look at an article I wrote in the World Wide Web Journal – I think it was July 1997 – I argued that corporate employers and law enforcement have very similar interests in certain kinds of key recovery. They want to be able to recover important documents that are encrypted by employees. In some cases, they want to recover the material very quickly, say, with an hour's notice. They want to buy this service, and they want the potential to recover the documents for quite a long time, because they are valuable several years later. So, I think law enforcement will be well served by relying on market forces to develop the key-recovery industry.

I also said that we should give up on key recovery for real-time communications, such as communications between a Web browser and a Web server, because no one is going to be that fast. As for law enforcement, how would they be served? The communications are going to be in unencrypted form at either end, probably on the user's desk top and on the server owner's system, so we should give up on real-time communications. It is probably not feasible, and it is likely to be extremely expensive to implement.

Third, and I feel strongly about this one, we need to invest in alternative gates of access for law enforcement. Encryption is just one of many technologies that have made it harder for law enforcement to conduct electronic surveillance. Whether moving from copper to wire, or moving from analog to digital compression technologies, there have been many developments that have made it harder for law enforcement to tap your phone. The answer is not to have law enforcement design the telecommunications technology. That should be left to the market. The answer is to help law enforcement get better at decrypting messages that they have lawful authority to read.

Finally, we need to establish transparent government-to-government agreements. Bill talked about user trust. This fourth point is really in the government's interest. If we, as users of encryption, do not know the terms under which our data could be considered a threat to the Russian government, we are going to have zero trust
in that key-recovery system. If we have a publicly disclosed agreement, setting forth
the conditions under which that key will be released, we will at least be able to make
an informed judgment as to whether to use that system. If we want key recovery to
work, we can not have secret government-to-government deals.

My last slide deals with pending legislation. Let's go through it quickly. I am
talking about the bills that are coming out of the National Security and Intelligence
committees of the House. Inadequate or zero trust...I say that’s bad...mandatory key-
recovery encryption, again, is bad...trade...heavy regulation of key management: they
don't need it. Users will require a key management system that, by and large, will meet
law enforcement needs.

Fourth, addressing alternative access by creating a net center in the FBI, so that
the FBI has the resources to do surveillance and also to assist local police
departments....SAFE, the original bill, as well as the latest version, which came out of
the Commerce Committee...export relief? Yes. There's a reasonable amount of export
relief...foreign availability test going forward...no mandatory key recovery. The
market for key recovery, to the extent it developed, based on what users want and what
measures it will deliver...and fourth, develop an alternative means of access as well.

So, I am not a math whiz. That is why I had to go to law school instead of being
an engineer, but it looks to me like it’s four to one.

MR. WEIDEMANN: Thanks, Clint. Hi. I am the founder of Red Creek
Communications. We provide hardware and software-based security solutions to
corporate users, whether they be in the United States or abroad. We also supply them
to system integrators and to service providers. They secure connectivity between
remote and mobile offices and branch offices.

I founded Red Creek Communications because I saw two things happening
simultaneously. First, both the cost and the desire to interconnect remote users in
branch offices were increasing dramatically. This is evidenced by growth in equipment
providers, such as CISCO, 3 Com, and others, with which I am sure you are familiar.
There are literally thousands of companies that spend $100,000 to over a million dollars
per month interconnecting their branch offices and remote and mobile users, so this is a
very, very large marketplace and a growing marketplace, and the costs are growing
dramatically.

Secondly, I saw opportunities for companies to save on these costs by using
lower-cost, and more widely available, public networks, such as the Internet, or
networks available from companies that you heard about today. There are
opportunities to make it easier and less expensive for companies to interconnect their
branch offices and remote users.
I went out to customers and asked them why they did not use existing security solutions that were available? Their answers were that existing solutions slowed down the network. They were also too expensive, too difficult to use, and too bulky.

What we designed, and have been shipping for six months, are solutions that are small in size, low cost, and do not slow down the network. For example, we have a product that is approximately the size of a deck of cards, and it can encrypt data in a transparent manner, at what is called T-1 or E-1 rates, which is sufficient for approximately ninety percent of the connections that are done by corporate America today. If all of you were sitting at your company, and you took one of these products and put it inside your network, and I had one inside my network, any data that we chose to transmit between us would be transparently encrypted or scrambled, so that anybody that was looking at the transmitted data could not intercept it.

Possibly even more important than that, these encryption solutions, besides securing the data with encryption, also protect you from access control. Once you have this solution in your network, no one else can get access to your network unless you absolutely allow them to. So, there is the concept of encrypting or scrambling data, and also of preventing access through access control.

The difficulty we now face as a company is that the current debate in Washington is stifling the adoption of security products such as ours and giving unfair advantage to international companies that provide similar solutions. Quite simply, we cannot currently sell these products outside the United States unless we weaken the encryption, or unless we provide access to the encryption keys used for each communication.

Additionally, with some of the proposals, we may not even be able to sell our products in the United States unless we do these same things.

The difficulty we have with this is that our competitors outside the United States do not currently have these same restrictions. Companies in Canada, Israel, the United Kingdom, Australia, and Sweden – many, very prominent countries and prominent companies – are shipping products today that do not have this weakened encryption.

How do we address this? Well, we have included the capability in our products for our customers to field-upgrade these products while they are installed in the network, without having to take them out or take them down. Hopefully, then, if this debate gets resolved, we can stop stifling our industry. No matter which way the government debate goes, our customers can upgrade their products while in the network.

Now, I am not going to explain to you all the mathematics involved in encryption, or explain how public key and private key works, but I want to use a
simple analogy to show how easy it can be to understand what is currently happening in the government debate.

Let us say that U.S. law enforcement pursued a policy of allowing American car companies only to ship cars that could go no faster than forty miles per hour. This would allow U.S. law enforcement to catch the criminals. Of course, international car companies could sell cars that did not have this restriction. Then, let us suppose that the U.S. government realized that this was an unreasonable policy, so they decided to change the policy and allow car manufacturers in the United States to sell cars without this forty-mile-per-hour limitation, as long as they make a key available so that law enforcement can get access to your car any time they want. All the while, of course, car companies outside the United States would not have these same restrictions.

The effect of this never-ending debate is just as stifling to our industry, by giving opportunity to companies outside the United States. Even though we are a new and relatively small Silicon Valley-based company, I have dedicated a large amount of time visiting officials and representatives here, attempting to get this issue resolved, because it is so important to our success.

MR. PRESSMAN: Thank you. We have some time for questions. Are there any questions out there?

I have one question. I find it kind of confusing that the debate in Washington began over export policy, and now it is onto domestic restrictions on encryption. A number of people mentioned mandatory use of key recovery, but that is not quite what the proposals call for. They basically require manufacturers of encryption products to enable key-recovery-type solutions, but they do not require users to put their keys anywhere, or to use the features. Does that make a difference, in terms of the problems you have with the policy, or can you address that aspect of it?

MR. WIEDEMANN: Right. As I recall the language of the Oxley-Matton amendment, it did not define key recovery. The bill did not say you had to use key recovery. What law enforcement and national security want, and would have received in the Oxley-Matton amendment, had it been passed by the Commerce Committee, was lawful access to the plain text of encrypted information, without the knowledge or cooperation of the user. I think that is pretty close to a quote of the bill.

So, call it what you want. Lawful access without your knowledge is unacceptable in most circumstances.

Keep in mind, the FBI says this is not an extension of the wiretapping authority. Wiretapping, I think, was originally put in place to provide law enforcement with the ability to listen to telephone conversations. When that power was granted to law enforcement at every level, not just federal, all information was not digitized. In other words, we did not have global networks where we were trying to do business on a
daily basis, with both stored and transmitted information in digital form. However, that is what we have now. That is coming.

So, in fact, if we extend the wiretapping capability of law enforcement to stored information and communicated information, and we then provide lawful access without one’s knowledge, that is virtually access to everything. Every day that goes by, there will be more and more information in digital form, either stored or transmitted. So...

MR. SMITH: I would add, too, that I think the phenomenal growth of the Internet can, in part, be attributed to the fact that there has been so little government regulation. What is being discussed here, even if it is optional for the user, is a functionality that will require an extended and costly effort to build, and it is quite likely that nobody will want to use it. We survive by building products people will pay for, so spending time and engineering resources to build something that nobody wants is going to disadvantage us vis-à-vis our global competitors.

Finally, I think the exchange went something like this. One of the speakers that was pushing for mandatory key recovery mentioned that it would be optional to the users, that you could enable this feature or not, and a Senator responded, "Well, if we're going to do this, wouldn't you really want it to be mandatory key recovery?" The gentleman from law enforcement answered, "Well, obviously that's what want, but that won't get passed now, so we're willing to settle now for optional key recovery." Can't you tell what the outcome will be in the long term?

MR. WEIDERMANN: I don't think our government is a threat to U.S. industry in terms of industrial espionage. I do not think the FBI, or anyone else in the government, is attempting to access information belonging to my company or my customers. That is not the issue.

In the United States, we have a very sophisticated system of protections. Law enforcement has to go through so many hoops to be able to get a wiretap. They only do a few more than a thousand per year, on average.

The problem is that, when you are trying to do business globally, using global networks, the protections of the U.S. Constitution do not extend outside the borders of the United States. So, all a foreign power would have to do is show probable cause to the U.S. Justice Department and request that the U.S. Justice Department assist that foreign power in gaining access to the keys of my company or my customers. If the United States government wants lawful access without the knowledge of the user, then wouldn't any other government where we do business ask for the same right? We think they will.
So, we would end up with a global, interoperable system that provided immediate access to the information of all of my customers without their knowledge. I don't think they're going to pay for that.

MR. SMITH: In effect, we will be removing the marketplace for encryption products, because people will not buy those in a global environment.

MR. PRESSMAN: Are there any other questions out there? Okay. I have another question. The Congressional Budget Office did a study of the House Intelligence Committee's version of the SAFE bill, which has a requirement that all encryption products allow key recovery. Their estimate was that the total cost of this bill, to all U.S. companies in the entire United States, would be between 200 million dollars and 2 billion dollars. So, I want to start, perhaps, with Joel, and ask whether that cost estimate, for all companies in the United States to comply with that bill, is accurate?

MR. LISKER: I just can't imagine what that could be based on, because, as I mentioned with this Mondex product, we're talking about a billion cards, with two or three billion, or possibly as many as five billion additional applications, each with its own sets of keys. You would have to be fairly efficient, operating in less than nanoseconds, to be able to recover keys and still meet those budget targets. I can't imagine that that could be a valid number.

MR. PRESSMAN: Can you comment on cost?

MR. WEIDERMANN: It wouldn't matter if the cost were zero. It is unacceptable. If it were free, would you use a product that provided every legitimate government lawful access to your information without your knowledge? If it were free, would you use it?

MR. PRESSMAN: Any questions in the audience? Yes, Ken.

MR. PRESSMAN: The question is, how well do your customers understand this issue, and do they have the potential to be blind-sided by restrictions that might be imposed? How well do your customers understand it?

MR. LISKER: From MasterCard's perspective, we did a survey of a thousand customers. Security is the number one concern for customers. Now, many of those concerned talk about fraud, because they understand that cardholders will ultimately bear the cost of fraud. When we probed, however, it became much more significant than that.

For example, we are experimenting with digitized minutia extracted from the fingerprint, as a way to move from the PIN to identify, without flaw, the cardholder as the person authorized to extract money from an account or engage in a transaction.
This type of technology met with praise by this group of a thousand people, because they were looking for additional security.

The idea that there might be a back door, or a global access arranged by bilateral agreements, or some other enabling legislation to allow the Swiss to deal with the United States, or the Japanese to deal with the United States, or the Koreans, and so on, would only raise those people’s concerns to new levels, because they have already identified this in a much more conventional environment as the number one concern.

MR. PRESSMAN: Clint, what about your customers for UUNet?

MR. SMITH: Many of our customers are fairly sophisticated technology companies. So, I think the foreign government controls will represent the real surprises for them. Companies will come to us looking for a simple and total global solution, and I’m going to have to write a contract that says, "Well, we’ve got you this limited export approval, but..." there’ll be a long list of things they can't do, such as use it in Israel or France without getting a second set of solutions and a second set of permissions, and that is going to come as a big surprise to them.

MR. PRESSMAN: Joel?

MR. LISKER: Just recently, one of the first Mondex buyers was a non-financial institution, an Israeli oil company, and one of the concerns they had was whether or not the stream of data would be protected, or whether the U.S. government could somehow gain access to this data. That is just the beginning. We see this much more in an issuance to a non-financial institution. The bill really gives no relief from that, and I don’t know how in the world we can ever disseminate this product on the scale that we expect to disseminate it with those kinds of concerns in mind.

Anyone else on the foreign customers?

MR. SMITH: I guess I would just say that there are some solutions available from foreign companies. We have gotten a lot of excitement. Fortunately, we have been the last company in the marketplace to write any solutions, so we have a lot of advantages, and we have gotten a lot of excitement from foreign customers. They do understand that, today, the government does not mandate that you have access to these keys, but they do have to live with weaker encryption. So, they have to weigh whether or not they are going to go with other solutions that may have stronger encryption, that may be harder to implement, or solutions from us that have weaker encryption that might be easier to implement.

MR. PRESSMAN: Are there any other questions out there? Yes.
AUDIENCE QUESTION: Given the crime prevention problem, whether it's key recovery based or not, do you think law enforcement can meet its goals any other way through controls?

PANELIST: I really don't. I would turn the focus on what law enforcement needs to encrypt that message that's been encrypted with the user's choice of technologies. I would help out law enforcement.

PANELIST: A follow-on answer is, if I thought that restricting our access to 128-bit technology would keep it out of the hands of crooks, I would say that we would seriously look at it, but no one can make the case that restricting our access to that technology keeps it out of the hands of the Mafia, or the drug cartels, or any other crime crew.

MR. PRESSMAN: Bill?

MR. WIEDEMANN: I was going to say, even further, that the government should go farther and promote the use of these technologies, in order to secure our information infrastructure here in the United States, rather than to stifle the market, so that even the government has difficulty in finding reasonable solutions to secure our infrastructure.

MR. Poulos: Speaking to Bill's point, when you look at the balance, the risk far outweighs the discovery of sensitive information by those not authorized to have it than the reverse. When wiretaps first came in, and when Title III first came in, we essentially dealt with what we called la cosa nostra. Those people knew that they were subject to surveillance. They didn't have detailed conversations, even in code words. That was off-line somewhere. The recent success in New York with wiretap is only one out of thousands of cases. Most wiretap information is absolutely worthless.

That is the thing that we have to keep in mind. Cases can be solved by means other than breaking encryption. There are other sources of evidence. Informants still exist, payments can still be made, and stings can still be set up. There are lots of ways in which these crimes can be solved.

So if we incrementally add a penalty providing that possession of this sort of capability, once you have been identified as having committed a crime, gives you another hundred years in the slammer in Mexico, that's great. People wouldn't do it, because they're afraid they might go to jail.

PANELIST: If we are going to criminalize use of encryption in furtherance of a felony, I think the language that was in the Commerce Committee draft is probably better. It is very clear in saying that, when encryption is used to conceal evidence of a crime, that is criminal.
PANELIST: Yes. The way it was drafted earlier, it was much more serious for a corporation, for example, which might have had an employee encrypting something that violated a government statute, and corporate liability could have crept in.

So, if we are going to have to go for that, I would look carefully at the Commerce Committee language.

MR. PRESSMAN: Well, we have used up our extra five-minute dispensation. I want to thank the panel for enlightening us today.
SPEAKER AND MODERATOR

BIOGRAPHIES

Joel Lisker
Senior Vice President of Security and Risk Management, MasterCard International

Joel S. Lisker is Senior Vice President, Security & Risk Management for MasterCard International Incorporated. A native of Philadelphia, Mr. Lisker received a Bachelor of Science degree from the University of Pennsylvania, and a Juris Doctor degree from the Temple University School of Law.

In January 1987, he was selected to serve as Associate Counsel to the Senate Select Committee in Secret Military Assistance to Iran and the Nicaraguan Opposition. One of his major accomplishments in this assignment was to uncover the sources of funding for the arms purchases through the Swiss banking network. He continued to serve on the Committee until retirement from government service in September, 1987.

Mr. Lisker spent 25 years in public service with the Federal Bureau of Investigation, U.S. Department of Justice, the U.S. Senate Subcommittee of Security and Terrorism, and the Senate Select Committee in Secret Military Assistance to Iran and the Nicaraguan Opposition.

In 1987, he then joined MasterCard International in New York, as vice president for Security and Fraud Control. He was subsequently promoted to Senior Vice President, Security and Risk Management. In this capacity he is the company’s senior security representative, worldwide, with respect to matters relating to the fraudulent use of its numerous products. Mr. Lisker has led MasterCard’s efforts to develop a reliable cardholder verification methodology adaptable to the financial transaction environment. He has been responsible for various pilot efforts to progress the integration of the technology to the point of sale.

He is a member of the District of Columbia Bar and has been admitted to practice before the U.S. District Court for the District of Columbia, the Court of Appeals for the District of Columbia Circuit and the United States Supreme Court.

Bill Poulos
Director of Technology Policy, EDS Corporation

Bill Poulos is a representative in EDS’ corporate office of Government Affairs in Washington, DC. He is responsible for providing strategic business units with
information and advice on national and global technology policy issues relating to the “Information Superhighway” for the development of electronic commerce.

Mr. Poulos is currently the U.S. Chairman of the Electronic Commerce Committee of the Transatlantic Business Dialog. He has been very active in national and international policy development related to protecting critical infrastructures; global use of encryption technology; U.S. and global information privacy policy; protection of intellectual property and the associated liability for information service providers; policy concerning the control of undesirable content on global networks; and national policy regarding the harmonization of legal frameworks to support electronic commerce. From 1986 to 1994, Mr. Poulos was a Senior Manager of Corporate Government Affairs for Apple Computer, Inc., where he represented the Chairman/CEO and his senior executive staff to government officials at the Federal and State level.

He contributed to the writing of numerous Computer Systems Policy Projects (CSPP) reports on “Information Super Highways”, which helped national policy makers understand the potential of converging technologies. Mr. Poulos led a computer industry coalition related to national encryption and export control policy. He co-chaired an effort to secured from Congress access to a multi-billion dollar allocation of radio spectrum for the Personal Communications Service industry.

Before joining Apple Computer, Mr. Poulos had a distinguished 20 year military career in the U.S. Army. His assignments included combat in Vietnam and service in the Congressional Liaison Office, Secretary of the Army. Mr. Poulos received a B.S. in business from the University of Tampa and a graduate of the Armed Forces Staff College.

Clint Smith
Deputy General Counsel, UUNet

Clint Smith has recently joined UUNet as Deputy General Counsel. Prior to joining UUNet, Mr. Smith was an associate technology counsel in the Law and Public Policy Department at MCI Communications Corporation. In this capacity, Smith handled legal issues related to MCI’s Internet, encryption, and electronic commerce services. He has been heavily involved in the roll-out of encryption products and the development of MCI policy positions on government regulation of encryption.

Prior to joining MCI, Smith was an associate in the technology and international practice at the law firm Steptoe & Johnson in Washington DC.
Smith received his J.D. and an M.A. in political science from the University of California at Berkeley, studied banking law at the University of Geneva, and received his B.A. from Pomona College.

**Bill Wiedemann**

Founder and President, RedCreek Communications

Bill Wiedemann, founder and president of RedCreek, has become very active in the encryption debate during the 105th Congress. He has met with groups on both sides of the issue, from the Federal Bureau of Investigation to the Business Software Alliance, in an attempt to find a compromise solution. He has also met on Capitol Hill with the offices of Sen. Diane Feinstein, Sen. John Ashcroft, Rep. Bob Goodlatte and Rep. Ron Dellums. Finally, Wiedemann recently spoke at the National Computer Security Association’s conference on electronic commerce about the Administration’s encryption policy.

A seasoned marketing and sales executive with 17 years of high technology background, Wiedemann was Business Development Manager for Cylink corporation prior to founding RedCreek. Prior to Cylink, Wiedemann was Western Area Sales Manager at Anritsu Wiltron Sales. He holds a BS in Electronic Engineering and Technology from California Polytechnic State University at San Luis Obispo, CA.

**Aaron Pressman** - moderator

Reporter, Reuters

Aaron Pressman covers technology, electronic commerce and banking issues in Washington, D.C. for Reuters, the world's largest news service. Prior to his current assignment, Pressman wrote about financial derivatives for Reuters in New York and has also worked for the Bond Buyer and Investment Dealers Digest. His freelance work has appeared in Wired magazine. Pressman is a graduate of Columbia College in New York with a degree in American history.
Panel 3: The Pros and Cons of Administration Policy

Rep. Edward J. Markey
*Ranking Minority Member, Commerce Subcommittee on Telecommunications, Trade and Consumer Protection, D-MA*

William A. Reinsch
*Under Secretary for Export Administration, U.S. Department of Commerce*

Marc Rotenberg
*Director, Electronic Privacy Information Center*

Rory J. O’Connor
*Washington Correspondent, San Jose Mercury News (moderator)*

MR. O’CONNOR: I follow policy here in Washington for the *San Jose Mercury News*, a daily paper in Silicon Valley, and the encryption story was actually the first technology policy story that ever brought me to Washington, about four or five years ago. So, I have seen a lot of interesting things.

I am told that we have quite a bit of time in this panel for questions and answers from the audience, and I hope you will indulge us with them, because, otherwise, I will bore you with the saga of the house that I'm now buying, and we can discuss comparative interest rates, how to fax offers to sellers in the Netherlands, and things like that.

We are expecting Congressman Ed Markey, from Massachusetts, and I am told he left his office on the Hill a couple of minutes ago, so he should be here fairly soon.

We have our other two panelists here. First, on my left is William Reinsch, the undersecretary for export administration at the U.S. Department of Commerce. You all have his bio, I think. I look him up in my rolodex under "Encryption Czar." His job is to deal with this and other policies at the Commerce Department.

Next to him is Marc Rotenberg, a director of the Electronic Privacy Information Center, with whom I have been talking about this subject since I first came out to Washington, and he has asked me to plug his book shamelessly, which he will now hold up. I am shamelessly plugging his book on these very topics.
So, in the absence of the congressman, let me start out and we will talk about the pros and cons of administration policy. We are going to let the panelists give you a little opening statement.

I guess the one question that, as a reporter, I would love to have answered is: just what is it? I am still not quite sure what the administration policy is. I have been assured by many people within the White House that "it has not changed," so we have a starting point, at least, toward which we can work backwards, but this has certainly bedeviled the administration, as far as I can tell.

Obviously, there are different points of view, not only about what the policy should be from the outside but, as far as I can see, from the inside, as well. Depending on to whom I talk, I hear different things, so I am anxious to see where we are at this point, and why that might or might not make sense.

I do not know the make-up of this audience, but I suspect that at least a few of you probably disagree with the policy that has been followed for some time, in terms of not restricting domestic use. Recently, however, Louis Freeh, the FBI Director, has been testifying that he and the Bureau would very much like domestic control on encryption. This is the source of my inability to fathom right now exactly what the policy is, so I will be looking forward to hearing it. We will get a question-and-answer session going and maybe we can settle that up.

I see that the congressman is not here, so I will ask Secretary Reinsch to go first.

SECRETARY REINSCH: Well, thank you for having me. I have discovered that, if one talks really, really long, then there is no time left to answer questions, so I am not going to do that.

For those who are confused, let me try to articulate what the administration's policy is and what its rationale is, knowing that, in the time available, I will have to leave some things out, but I will be happy to take questions afterwards.

Rory is right: the administration's policy has not changed. We also think it is clear. Let me try to explain it and you can decide for yourself if it is clear. A lot of people have said it has not changed. A lot of people, beginning with the vice president and working down, have tried to articulate what it is, and I am going to do the same.

Keep in mind that we have tried to do two fundamental things. First of all, we have tried to look at encryption as part of the larger question of security, of which authentication is an equally important part. We can have the best encryption in the world, we can have unbreakable encryption, but, if we do not know with confidence where our message is going, and if we do not know with confidence who a message came from, or that it came from the person that it says it came from, and if we do not
know with confidence that the message did not have any mysterious intermediary stops along the way, then we really do not have good security, even though we have good encryption.

Therefore, for us, other things in the electronic commerce mix, like digital signature, are very important. They are also relevant to this part of the debate because of the infrastructure that will have to be created to sustain them. That does not have a lot of implications, in and of itself, for the encryption issues we will be debating today, but its very existence creates some opportunities for a key recovery infrastructure, which is where I am going with this, to latch on to some of the same people and some of the same service providers. You have to look at the issue in the context of larger security issues.

The second thing the president has been most outspoken about in this area is trying to pursue a policy of balance. Part of those inevitably competing equities are privacy, about which I am sure we will hear from Marc; electronic commerce, which you should have heard about already and you hear about frequently; but also national security and law enforcement. From the beginning, we have looked for a policy that tries to contain all those elements. If you are not interested in one of those elements, then you are not going to be interested in our policy, and we have a fairly fundamental disagreement.

Now, in order to develop a policy that reflects balance, we have tried to look at technologies that we believe provide opportunities for balance. The one we have ended up with, although we are always willing to listen about others, is key recovery.

I attempt to use that term generically. One of the frustrations in what I do is talking to people who construe key recovery as meaning third-party key escrow, and I want to make clear that that is not what we mean. In fact, the key recovery world that we envision and look forward to and think the market is going to create will consist, by and large, of private certificate authorities, private key-recovery agents, who are not affiliated with the government. Some of them may operate in the third-party category or capacity, but many of them will not, and these will operate essentially as agents of the entity that is running the piece of electronic commerce, whether it is an electronic banking network or something else that key recovery is a part of.

That is key to the point I am trying to make, because we see key recovery very much as a market-driven thing. Now, I am not sure the market is going to drive us to key recovery equally in all different sectors or segments of this market. However, looking at the ones where it is, which I think is particularly true of electronic commerce, we see companies, including financial institutions, wanting to engage in electronic commerce in a key recovery framework for their own reasons, which are commercial reasons, which are security reasons, or a variety of reasons that I can elaborate in Q and A if you want. We do not see them wanting to do this because of the government or because of law enforcement reasons, but we see them having their own interests in
being able to access and decrypt the encrypted records that they and their employees will inevitably be keeping. So, we see the market going in this direction anyway, certainly for stored data and certainly for electronic commerce and all of the transactional kinds of messaging that implies.

Now, we have tried to devise, on the part of the government, a set of policies that facilitate that movement. I will focus on two or three of these policies. The first is procurement. The federal government is always a powerful procurement agent. It always has been, and always will be, simply by sheer volume. We intend to go to a key-recovery system, we intend to have certificate authorities, and the whole nine yards, for our own use. If private parties want to enlist in that system and use those certificate authorities and make the same commitments, that is fine, but they will not have to do that. They can ignore it entirely.

The one time they will not be able to ignore it entirely is if they want to communicate with us in an encrypted manner. They will not have to communicate with the U.S. government in a cryptic manner but, if they want to do so, they will have to use our system.

I can speak from some personal experience with this. The Bureau of Export Administration is going to go online next year. I am sure this comes as a revelation to those of you in the export licensing business. We are going to permit people to file license applications through the net. I anticipate that people will want to file those applications with us in an encrypted fashion, because of the sensitivity of some of the information they will be providing us. We intend to set up a system that will permit them to do that, and it will be a key-recovery system. If they want to participate in that system, in order to communicate with us, they will have to do it our way. However, they do not have to participate in that system. They do not have to encrypt their data. They can continue to do paper filings or work through some other means.

The government, therefore, is going to use a key-recovery system, and the government is going to buy a lot of key-recovery hardware and software, and that will make a difference in the marketplace. There will be demand for those products. We think there is going to be demand for those products anyway. We see that happening through other elements of our policy, which I will get to in a minute, but we also see procurement being a powerful driver of the market in this area.

The other element of our policy, which has probably received the most comment, is the export control element of our policy. These items used to be controlled as munitions. The president decided they were dual use and moved them, and we are trying to operate an export control regime for these items. This is also designed to push the market a little bit in the direction of key-recovery products.

In that regard, we have said several things. The first thing we have said is that, if you are marketing a key-recovery product, you may export it without restraint,
except to certain states: Iran, Iraq, Libya, and North Korea. There does not seem to be much debate about that. In fact, people are marketing those products, and we are classifying their products. Once classified, they do not need to apply. That is happening.

The second thing we have said is that, if you will commit to make those products and submit a plan showing us how you are going to make those products over a two-year period, we will liberalize our export controls for you, with respect to non-key-recovery products, to the tune of 56 bits. So far, we have 39 plans, and we have approved at least 32 of them. We have not rejected any. I think this is a sign that the market is responding. People out there see a demand for this kind of product. They are investing R&D dollars, they are investing research time, they are investing intellectual resources in the development of these products, and I think it is because they see marketability, not simply because they see a government requirement.

We have also liberalized export controls on encryption items, particularly software that is going to banks and other financial institutions, because of the particular nature of those institutions. In the interest of time, I will not elaborate, but we are permitting exports well beyond 56 bits, under the circumstances we have prescribed.

Obviously, this policy is not going to succeed in the long run unless we can persuade or bring along, if you will, our trading partners in the same direction. That is why the president has appointed an ambassador for this purpose, David Aaron. That is why he is now getting in touch with upwards of twenty countries to discuss this issue. That is why we have developed a multilateral working group to try to develop some uniformity of policy in the encryption area.

We have discovered that every country we have dealt with is going through the same internal debate that we are. Every country's interior ministry or justice minister sounds an awful lot like Louis Freeh, and every country's trade minister or economics minister sounds an awful lot like Bill Gates. In some countries, like Germany, this is a very public debate. In other countries, it is not so public, but it is still going on. Countries that are well on their way through this debate have tended to end up in places not that dissimilar from where we have ended up.

There are elements of difference and there always will be. We have had a problem convincing some of our European friends that we do not intend to hold keys to their encrypted devices, and we do not intend to hold their keys and access their intellectual property. We have been making that case, but they have been slow to get the point. I was pleased, in a way, at an earlier seminar, when I got the reverse question from an American in the back row, who said, "You know, I don't want to go over to Germany and put my intellectual property at risk to their key-recovery system."

I said, "You know, the way we are proposing to do this -- which is not necessarily through third-party escrow but, oftentimes, through self escrow, and
through the prevalence of national law in each case -- you do not have a problem in that regard, except to the extent that you have a problem right now with protection of your existing records from the depredations of whatever police force or interior ministry you happen to be dealing with." In Germany, I think that is not an issue. There probably are some countries where it is an issue, but it is an issue now, and, if it is an issue now, it will be an issue then. It will not be an issue because of encryption, it will be an issue because of the nature of that society and the nature of that law, and we are also wrestling with that.

Our international group has set up two working groups. One is working on interoperability, which is very important. It would be interesting if the marketplace ended up with 840 different operating systems, none of which could communicate with each other, but that would probably destroy electronic commerce, so it is not in anybody's interest to have that happen.

At some point, standards, standard development and harmonization, must come into play. People do not always like to hear that, because, when one says "standards," one usually ends up saying "government" in the next sentence. However, there are positive roles governments can play in harmonization and interoperability. At the end of the day, everybody will want them to play that role, because German banks want to communicate electronically with banks, and vice versa, and we want to have systems all over the world that are going to facilitate that communication and not impede it.

Likewise, we have a working group trying to achieve some harmony on export controls. If we do not have export control harmony, then no country is going to be able to pursue its own national policy, unless their national policy is having no policy at all. So, we are working very hard to that end. There is a meeting of the senior level representatives next week. I think we are making progress. It is difficult, for the same reason it is difficult to pass legislation, and I suspect you will hear about that from Mr. Markey, among others.

On that point, let me say that we favor legislation to address some particular parts of our policy that we think are difficult to implement without it, the most obvious being liability for certificate authorities and key-recovery agents. We think legislation can also help on the carrot side, if you will, with some of our procurement proposals. There are some other things that we are certainly willing to have in legislation, clarifying the relationship between law enforcement and the terms of access for this kind of thing, with holders of keys or holders of information. It is a very important thing to do, there is a lot of precedent for it, and nobody seems to want to rock the boat in terms of raising or lowering that threshold, but trying to put the status quo into words has turned out to be difficult.

The legislation that comes closest, I think, to what we would like to see, although it is not quite perfect, is the Kerry-McCaín Bill, S-909, which we have been discussing with Senator Kerry. We hope the Senate will move on that. In the interest of time,
however, and in the interest of giving Congressman Markey a chance, I will refrain from making comments. In the interest of good taste and tact, I will also refrain from making comments on the House bills. We can discuss that during Q and A, and I would be happy to comment on them, as well.

Let me close with a subjective comment, if you will. The more I have looked at this, it seems that the way people break on this has a lot to do with what they think about the market, and the level of confidence they have in the market. If one has confidence that the market is going to get us where I have suggested we want to go, and if one has confidence that the market is going in the direction I have described, then the kind of encryption policy one looks to, either legislatively or administratively, is one that largely involves carrots, procurement, demonstration projects – which you are going to hear more about from us in about three weeks – and other things like that.

If one does not have confidence in the market, if one is not sure of the direction the market is going, or if one does not think it will produce a solution that is comprehensive enough (and nobody has ever suggested that we are going to get a comprehensive solution, even under the best of circumstances), then one must begin talking about some of the things Director Freeh has been talking about, which are domestic controls on manufacture, import, or whatever. So, where you divide on this depends a little bit on how you look at the marketplace, and that is an important question.

Frankly, there are some good arguments on both sides of that. The administration's view has been, and clearly is, to support a market-driven, market-reinforcing strategy. We have not proposed and, as far as I know -- I think I know, because I have been at most of the meetings on this subject -- we have no plans, as an administration, to propose domestic controls and the kinds of strategies that would not be market reinforcing. Thank you very much.

MR. O’CONNOR: Congressman Markey has joined us, and it was his compromise on this very subject that wound up passing the Commerce Committee in the House about a week or two ago. If that becomes the law of the land, I do not think there will be a domestic control issue to talk about. Congressman Markey.

CONGRESSMAN MARKEY: Thank you, Rory. What a great issue this is. We have forty-nine members of the Commerce Committee, and each one of them was coming over to me and saying, "I just got called by Bill Gates." Then they came back to me an hour later and said, "I just got called by Louis Freeh." Wow, what an issue, huh? We were getting calls from the wealthiest guy in the history of the world and the most powerful policeman in the history of the world. That’s quite a dilemma for members of the Commerce Committee to be presented with, because one would like to make friends with both of them, if you know what I mean. If there were any way humanly possible, one would like to be friends with both the wealthiest guy in the world and the most powerful policeman in the world.
That is the kind of dialogue we are now beginning, in discussion of these issues, because technology, in and of itself, is neither good nor evil. It is only as good or as evil as the human values that animate the technology and decide to what purpose it will be deployed. Automobiles going a hundred miles an hour do not serve society. We have to put limits on it. Each and every technology falls into the same category, including this technology. So, on the one hand, encryption software can protect data, safeguard personal privacy, foster electronic commerce, and preserve personal freedoms. However, an encryption software can also protect evildoers, hide criminal activity, and encourage electronic assaults.

Encryption is not innately good or bad. There is a Dickensian quality to it. It is the best of wires and the worst of wires at the same time. It is the best of encryption and the worst of encryption at the same time. It has a dual personality. It is like a nuclear power plant. It can generate electricity and have the unfortunate byproduct of plutonium. In the hands of a dictator, it can generate plutonium for bombs and have a wonderful byproduct of electricity. It all depends upon how we do it, how we control it, and what human beings decide to do in order to ensure that the technology serves mankind.

So, how will we deal with this issue? We hold up a mirror to our own society as we debate an issue of this nature. We are looking at ourselves and our values in every single one of these issues. Technology just can not be allowed to do whatever it wants in any area. There is no such technology. It always has to be ultimately circumscribed by what human beings want it to do for us. Do we want the technological innovation to be used for good or for evil?

So, law enforcement has identified a very serious problem in its efforts to solve crimes. It is, without a doubt, a very real problem, and it is good that Louis Freeh and the FBI have brought this problem to us, because it must be solved. No one denies that strong encryption can thwart law enforcement's ability to decode data and to do their job. It is a very big problem. Put it right on the table.

When I was chairman of Telecommunications from 1986 to 1994, we had to deal with the issue of something called CALEA, which really concerned the ability of police to gain access on digital wires to information that they have historically been able to gain over the copper wires. We had to work this issue out, and it took a couple of years on my committee to negotiate that issue. Again, there were very strong pressures on either side -- the telephone company and privacy people on one side, police on the other. We worked it out, but it took two years of trying to be respectful of all the values that are on the table at a time when such an important issue is being considered.

The problem with the debate over domestic use of encryption is that a solution to law enforcement's problem is electronically elusive. The solution proposed by the FBI and others in the law enforcement community comes to us with serious new
limitations on the individual rights of Americans, but also, in my view, it is a solution that does not effectively solve the problem. Until we find a solution that works, I do not believe it is wise to ask every American and every computer software maker or online company to reconfigure completely their data security software or their network protocols and, in the process, make Americans and American companies more vulnerable to crime, while in headlong pursuit of nefarious characters who, more than likely, will circumvent those controls anyway.

The Internet challenges us as policy makers, as Americans, to think in new ways about how we address common and historic policy issues. That was the lesson of the Communications Decency Act, and we will replay that drama with respect to tax policy, gambling laws, consumer protection issues, personal privacy issues, and law enforcement issues as we move deeper and deeper into this Internet era. It will invoke all of the old laws and all of the old principles that we have lived under in the real reality. As we move to the virtual reality, we have to ask ourselves how many of these old values we want to bring with us.

I would argue that we want to bring all of them with us, every one of them. We do not have to abandon the past in order to embrace the future of global competition and rapid technological change. The old values served us very well. We do not create a new formula by abandoning the old. We integrate the two new forces, global competition and technological change, with the old values and create a whole new formula. That is our test as a society. That debate has just begun on this issue.

The Internet challenges policy makers to think in new ways about how we do that. That was the lesson that ultimately had to be learned as we went through the Communications Decency Act.

By the way, we were in a room about a tenth of this side and, at that point, I was the lead Democrat, but the Republicans had the votes, because they had taken over the Congress. You should have seen the debate break out amongst the Republicans. There were the pro-business Republicans versus the Christian Right Republicans. I felt like a referee at an intramural squabble.

Ultimately, it came down to just one or two votes putting the Communications Decency Act on the books. Meanwhile, I was trying to tell them all that it was going to get struck down as unconstitutional in a nano-second, because we had already gone through these issues with Dial-A-Porn and other issues as a way of doing it, to offer protections to parents, and then there's another way of doing it, which is going to be clearly a violation of First Amendment rights. But you kind of get caught up in the momentum of the debate and the ideological polarity that can be created in terms of how you perceive the world. But ultimately we all had to be pragmatic and try to include very real considerations for parents -- that's blocking technology, with the desire for us to have this open, accessible, you know, vigorous discussion that goes on through the Internet technology. You can do both.
My hope is that, as the Rules Committee tries to reconcile all of the various perspectives coming out of the Judiciary Committee; the good perspective coming out of some of the other committees that voted on it, reflecting a narrower, more traditional security-and-law-enforcement perspective; and coming out of the Commerce Committee, which now has the Markey-White amendment as its prevailing sentiment; we can now begin the discussion. We have all the views on the table.

Everyone will now have to be cognizant of the fact that they will have to deal with paradox. They will have to deal with the other side's issues. How are we going to take care of it? We just can not do one thing and say, "Well, who cares about law enforcement?" On the other hand, we can not do something else and say, "Who really cares about whether or not you can sell computers or software overseas?" We can not have that be the end result, if that is the shootout. We must work this thing through the way we did with the Digital Telephony Act, being respectful of both sides of the issue.

So we have three problems. First, as the bill was framed coming into our committee, if we ban the encryption technology, the bad guys can download it from overseas, and if they are really bad guys and really sophisticated, and they really are going to do terrible things in America, then they are sophisticated enough to know how to get real encryption coming from overseas. So, that doesn't solve that problem.

Secondly, if we build a back door into every computer, software, and Internet technology in America, then we are never going to see the full growth in the commercial use of this technology. It will ultimately be stultified, because ordinary Americans are going to be saying, "I'm not going online. I'm not risking my privacy and my security. I'm not going to let that purple-headed, twenty-two-year-old that I see walking in and out of that apartment building across the street crack into my little world and find out what I'm doing, what I'm watching, and what transactions I've been engaged in. I'm going to be apprehensive about that."

That is the problem right now. You can get a certain generation of people to go online rather cavalierly, thinking it is a wonderful, wide world, but those are not the people with the money. Those people are not going to be banking with the big cash. Those people are not going to be buying the big items. Those people are not the customers to whom business people really want to have access. The desirable customers are not going online if they can not be confident that everything they do is going to be confidential, as it would be in a bank or a store, or in any traditional establishment. If we can not create that sense of community and that sense of historic values, then traditional Americans are not going to use it, and traditional Americans have the money. They work hard, they play by the rules, and they tend to make more money. Those are the people businesses want, and if we do not have proper encryption, proper security, and proper guarantees of privacy, they are not going to use it.
Thirdly, who in the world will be able to convince somebody in Germany or Korea or Indonesia, or wherever, to buy an American computer or American software, if a back door has to be built into it, and if a person can buy the same, exact technology, or a very close replica of it, from another country where such defects are not mandated by law?

So, we have these three problems, none of them solved, on the other side of the fence. As a result, the Markey-White Amendment did pass, 35-15 in the committee. It was an upset. We were probably going to lose it forty-eight hours beforehand. I think it was one of the very rare instances when the debate actually swung votes. The members actually had very powerful forces pulling them in opposite directions, and every member sat there throughout the entire debate, because, at the end of the day, they wanted to make the right decision.

So, as we hit the Rules Committee in the House of Representatives, we now have the beginning of the discussion, and it will not be short. This will not happen overnight. We just cannot force this like it is a decision to veto a pork-barrel military project or to increase the peanuts subsidies by 5 percent. This issue is not well understood by members of Congress. We are the committee that has jurisdiction over it, but members of ninety percent of the rest of the committees in Congress would not feel comfortable voting on it yet. It will be up to the public, up to the press, and up to lobbyists on these issues to meet with members and to bring them into this debate in a way that ultimately is going to forge a compromise.

So, we have to give the law enforcement community the tools to keep pace, and the Markey-White Amendment tries to do that, because it creates a new electronic technology center, the Net Center, to serve local, state, and federal law enforcement authorities by providing information and assistance regarding decryption technologies and techniques. The Net Center would serve as a center for industry and government entities to exchange information and expertise. In addition, the Net Center would facilitate law enforcement's access, in plain texts, to communications and electronic information, by investigating and researching new and merging encryption technologies. Our amendment is tougher on crime. We make the penalties infinitely harder than anyone else has ever even remotely thought about. Basically, I think, we have a good compromise, and that is why it won.

It is not the end of the debate, however, it is the beginning, and all of you should understand that your CEOs are going to have to be involved in this. The top person in your organization just can not delegate this responsibility.

I will give you my own perspective. We are debating fast-track authority for the administration right now. Essentially, the trade-off in fast track is that we are going to try to take down barriers in the rest of the world so that we can get our high-end products into those countries. In turn, we are going to let their low-end products, their beef or their coffee, whatever, come into our country, jeopardizing our low-end
workers. If you think about it, if we have a bill that is not sensitive to our high-end exports -- the computer, the software, the telecommunications, all the way down the line -- what is the whole point of fast track?

We are talking about creating a world where we can sell this stuff around the world, but who is going to buy it? In a lot of ways, even if there were no fast track but we had the right policy on encryption, making it possible to export this stuff overseas, that will be much more important, because people will move to quality, they will move to the best products. This should be the debate on the front page of the newspapers, not fast track. This should be the discussion in the high-tech community, not fast track, because, if we get this one wrong, fast track will not help us. No one is going to buy it. On the other hand, if we do not solve the police issue, we create a series of unintended consequences as well.

So, let the discussion begin. I thank all of you for your interest and attention to this issue. Without question, I think it will be critically important for our country to get this small handful of issues right over the next year, and I think you have a front-row seat in history. Thank you all so, so much.

MR. O'CONNOR: Last, but not least, let us call on Marc Rotenberg, and we can talk about whether there is a compromise out there somewhere. Is there?

MR. ROTENBERG: Well, let me say that you may be asking the wrong person, because I am not sure right now that compromise is what the user community is looking for. I am going to set out two perspectives that have not been discussed much today: the views of users, and also the views of what is happening around the world, which is absolutely critical to this debate.

Now, it would not surprise you if I told you that the civil liberties organizations and the privacy organizations like my own, of course, have emphasized privacy and talked a lot about whether or not it is appropriate to grant the FBI this type of authority.

More critical, in terms of understanding the user viewpoint, are the recent voices being raised in the scientific and technical community about the administration's policy on key escrow. Not surprisingly, the voices were heard first among the users and developers of the Internet. For example, it was the Internet Architecture Board, the Internet Engineering Task Force, and the Internet Society that, early in this debate, issued strong resolutions opposing the deployment of key escrow and key-recovery technology. That viewpoint is now spreading in the scientific community and, shortly before the vote that took place in the Commerce Committee, there were a dozen national scientific organizations, from the American Association for the Advancement of Science and the Association for Computing, to the American Mathematics Association, which all said, together, that a policy that intends to promote the widespread deployment of key-recovery encryption is ultimately mistaken and counterproductive.
This view was also expressed, as mentioned earlier, in the lengthy and comprehensive report produced by the National Research Council, and it is similar to the views expressed in Matt Blaze's report, which was done with a dozen leading cryptographers and security experts. So, when I say there is a strong sentiment in the user community against this policy – and it is a policy, as Mr. Reinsch has outlined, that tries actively to promote the development and use of key-recovery and key-encryption technology – I am not just speaking for the privacy and civil liberties organizations. I am reflecting a view that is widely held in the Internet community and among scientific and technical organizations.

To add another dimension as well, this view is also widely held by U.S. allies and trading partners, and this point is particularly important, given some of the things that have been said earlier.

Now, what is the basis for this conclusion? I can tell you that, during the past two years, I served on an OECD expert panel. It was established in December of 1995 for the purpose of creating an international framework for cryptography policy. It was clear that governments were pursuing different directions and different approaches to cryptography, and there was a desire to seek some type of harmonization, some type of common framework, some consensus viewpoint among the OECD member nations.

Now, if you know the OECD, you know that this is not an organization that operates either by the force of legal authority or on the ability to give out large grants and disbursements in support of programs. Its force, its credibility, derives from its expert assessment and its ability to seek a consensus position that can be supported by the OECD countries. The OECD came to the cryptography issue prepared to endorse key escrow and key-recovery encryption in a specific principle regarding law enforcement access, based, in part, on concerns that had been expressed by the United States government. If one looks at the early drafts of the OECD guidelines, one will see, in fact, support for the principle of law-enforcement access to encrypted communications, as well as support for such principles as voluntary, market-driven development of encryption products.

However, something very interesting happened over the period of time that the OECD met. I should tell you also that these were intensive meetings. They took place over the course of three or four days, several times in Paris, once here in Washington, and once in Australia. By the end of the process, the OECD had backed off the endorsement of law-enforcement access to private communications and had chosen, instead, to support privacy protection strongly, as a key element of an international framework for cryptography policy. If one looks at the final OECD guidelines released earlier this year, one sees many recommendations, eight principles – international cooperation, voluntary development, user choice – and it says, "these things shall be done, they shall be done, they shall be done." When one comes to lawful access, it says:
"This may be done." This was an acknowledgment that some countries may choose to pursue key escrow, key recovery, but the OECD was not prepared to back this.

I want to put a slightly finer point on this. Mr. Reinsch has not gone quite this far, but Ambassador Aaron has said, in fact, in public forums, that the United States has been pushed by other countries to adopt more stringent encryption controls than are currently in place in this country, and that the United States, in effect, has been trying to chart a middle course without pursuing the strong, draconian controls between absolute control over cryptography and no controls over cryptography. I think they used France and Russia, perhaps, as examples. I will tell you, this is simply not true. Only one country at the OECD was pushing for an international framework for key escrow and key recovery, and that was the United States.

When the United States put the proposal on the table and said, "We need endorsement for law-enforcement access to private communications," only one country of the twenty-nine members – France – supported it. Why did France support it? Not because they wanted an international framework for key recovery, but simply to protect their sovereign authority. Because France had already passed a national law establishing a TTP system, and they did not want the OECD or any other international organization telling them that their law was, in effect, void. France acted in that way to protect their sovereign authority.

Only the United States pushed the proposal to establish an international framework for key escrow, key recovery. It was rejected.

Since the OECD meeting this spring, the ministers of the European Commission reaffirmed this view at the Bonn Summit in June. Mr. Reinsch is correct that there have oftentimes been debates among European governments, between ministers of justice and ministers of trade and commerce, but those debates have been resolved in favor of commerce, in favor of trade. So, at the Bonn Summit, it was not the German minister of justice that was setting out the German position or the E.U. position. It was the German minister of commerce, who said, "We should have open availability of strong cryptography."

This is not just in Europe, either. It is true in Southeast Asia, it is true in Canada. We are seeing governments around the world moving toward open availability of strong cryptography. Even the two closest U.S. allies on this issue, which, admittedly, have been France and the United Kingdom, now seem to be backing off their earlier support for this position. France made clear, in just the past month, that they need to see good cryptography, in order for electronic commerce to go forward. The U.K. DTI proposal, which was put forward by the last government, by the non-Labor government, is now being put at a distance from the current government, and there are many questions about its future.
So, we are left today with a U.S. policy that is not supported by the scientific community, not supported by the user community, the Internet community, or by foreign governments. It is supported by this administration, and its aim is to force the use and deployment of key escrow, of key-recovery encryption.

I think this is a mistake, but, more importantly, I think it is a failed policy, a policy that has not taken hold. At this point, the direction needs to change. We need a policy that is more practical, more sensible, less costly, and less bureaucratic. Most importantly, we need a policy that engenders trust for users of new online services and of new products, trust for people in businesses and institutions and in the U.S. government, so that, when law enforcement does indeed exercise its necessary and important authority to pursue the bad guys and to conduct the criminal investigations, there will be public understanding and public support for those efforts, rather than resistance and opposition. I am afraid that is where we are heading today.

So, that is my quick take. I apologize, Rory. You asked the wrong person for compromise, but I think that, if you had asked some other people, they might have had a similar response. Thank you.

MR. O’CONNOR: I see there are microphones, so my presumption is that we would like people who have questions to come up to the microphones. I will exercise my prerogative and ask just two. The first has been on my mind for roughly six or seven weeks, since Director Freeh first came, I believe, to the Senate and said, outright, that the bureau favored domestic controls. Is he speaking for himself or is he speaking for the administration, and would the administration accept, or would the president sign a law of the type the director was suggesting if it were to come back up from the Hill? This is for Secretary Reinsch.

The corollary of that, for Congressman Markey is, how does the Hill view statements by the FBI director? Are they viewing this as the position of the administration or as an independent voice?

MR. REINSCH: Well, Director Freeh answered the first part of the question when he made these statements. In at least every forum where I appeared with him, and there were several, he made clear that he was speaking for the domestic law enforcement community. He made clear that he was not speaking for the administration, but he also made clear that he was speaking for more people than the FBI. In fact, he has received a series of letters from the International Association of Chiefs of Police, the Sheriffs Association, and a number of other law enforcement associations and groups in the United States, supporting the view that he has taken. So, I do not think there has been any ambiguity in his words about who he is speaking for and what he is representing.

To further that one more step, the FBI, in particular, and the law enforcement community in the United States, going back to J. Edgar Hoover, has a long history of
being forthright, certainly with Congress and, also, with the public, about what it feels it needs to do the job. Director Freeh is firmly within that tradition. That obviously has caused some confusion, given the question, but I do not think there has been any confusion in the way he has presented his views.

Now, to answer the second part of your question, it is telling that the House Intelligence Committee mark-up most closely reflected what the president had proposed, and the administration expressed opposition to that result. We said that we did not think that bill reflected the kind of balance the president was seeking, just as we said that the Goodlatte bill did not reflect that balance, so we opposed both of them.

CONGRESSMAN MARKEY: I think that is accurate. Not unlike the CDA, I think we are watching an intramural squabble in the Clinton administration. We realize that there are different points of view inside the administration and that there is no final winner yet, and that is why, in a lot of ways, as a prelude to the resolution of the issue within the administration, the Commerce Committee mark-up served as the end of the one-sided debate. The Congress and I think the same thing is ultimately going to happen, perhaps because of the vote of the Commerce Committee, inside the administration as well.

MR. O'CONNOR: I have a second question. It seems that we are trying to debate relative risk – right? What is the risk from criminal activity versus what is the risk to individuals, to privacy, commerce, et cetera? It is a risk assessment. I am familiar, as I am sure many people are, with the NRC report in which they did a risk assessment and said, "It is better that we have very, very strong encryption and prevent certain crimes and run the risk of having some get through." The FBI obviously is on the other end of this, painting very dire pictures of what might happen. So, I will ask you gentlemen, what do you believe is the relative risk here?

CONGRESSMAN MARKEY: The roll call has gone off over on the House floor. Do you mind if I ask Colin Crowell to sit up here for the next fifteen or twenty minutes and answer for the House of Representatives? Colin is my telecommunications guru, and he will be running telecommunications when the Democrats regain the House in another year, so he is my Luke Skywalker. Do you mind if we make that swap?

MR. O'CONNOR: If he can do the accent, sure. Marc, let me start with you. Talk about the relative risk issue, or is this a red herring?

MR. ROTENBERG: Well, I think it is obviously a real issue. Certainly I have never said that there are not going to be some circumstances where encryption will not, in some manner, frustrate a law enforcement investigation. We have always taken that issue very seriously. In fact, when the digital telephony proposal was before the Congress, we began a whole series of Freedom of Information Act requests in order to get the information from the field offices that justified this tremendous reworking of
the U.S. communications system. We wanted to know what was actually happening, what was creating a problem for law enforcement that would justify the legislation.

I can tell you there was nothing disclosed publicly, up to the vote on that bill, that would have justified the legislation. There were some private briefings. There was a document listing 183 incidences, and it was blacked out. It looked like something one of my kids might have done. Apparently, it was carried around the Hill and it led to a lot of votes in support of CALEA. So, as I said at the outset, I think the issue is a very serious one, and there will be instances where an encryption will cause problems.

On the other side of the issue, the reason why the scientific community’s view is so important in this debate is that we are creating a world in which vulnerability becomes the default, as Matt Blaze said, where we have another path to clear text that we did not need to have, and we put it there because, in some day and some circumstance, in the incredibly unlikely instance that a particular user becomes a target of a criminal investigation, we can get to it in real time. It is most interesting that Dorothy Denning, who was one of the early advocates and one of the most ardent advocates of this proposal, said in her most recent paper that we now have to consider the vulnerability of these key-recovery senders, given the nature of international organized crime. That is a lot of worry on the other side.

MR. O’CONNOR: Secretary Reinsch?

MR. REINSCH: Let me just make two comments. One of them is sort of irrelevant, but I can not resist. You referenced the NRC study, and I was amused, because, in the hearing before Mr. Markey’s subcommittee, I think, which was the last reference I have heard of the NRC study, one of the private-sector witnesses said that, of all the various policies on the table, the one closest to what the NRC had recommended was the one being pursued by the administration. I just think I should throw that out.

On the risk question, let me suggest a story I found interesting, because it illustrates to me the dual nature of the risks inherent here. I think it typifies the dilemma. I was struck that, in the same hearing, witnesses on opposite sides of this issue used exactly the same example to make their point. I thought that was telling.

It is the story about a guy in California who got arrested with 80,000 credit card numbers he had taken for nefarious purposes. One of the witnesses representing the private sector – I am not sure whether he was a computer witness or a privacy witness or whatever – was essentially making the point: "If we had good encryption in commerce, this would not have happened, because that guy would not have been able to get all those numbers." I think his argument is true.

Director Freeh actually made the point first, however, and he said, "When we arrested that guy, all those numbers were encrypted, and we were only able to decrypt
them and get the evidence with which to charge him because we had a cooperative witness. We did not have the capacity to decrypt. Therefore, we need key recovery."

Well, to me, that summarizes one of the dilemmas here. I think they are both right. They both have a point. The president is trying to thread his way through that by reflecting a policy that tries to take into account the risks on both sides.

MR. O'CONNOR: Colin?

MR. CROWELL: I will just comment briefly. When we had our committee mark-up, the general assessment broke down 40 to 11, and that was not an easy assessment for members, because, politically, the threat of a terrorist bombing or a publicized kidnapping or some heinous crime really is where nitro meets glycerin on this issue. No member of Congress wants to vote for something and then have it turn around and be alleged that that vote allowed a certain crime to occur, and that was part of the debate before us. That was certainly part of the series of arguments that proponents of the alternative were proposing before us, that we needed to do this for law enforcement, because there was a great risk.

However, the final assessment from the committee and the membership was that they did not think the solution solved the problem, and that, even if they were to have endorsed what the FBI and other law enforcement entities were proposing, it still might not avert the heinous crime -- a World Trade Center bombing or what-have-you. Those things might still occur, and we might still have folks getting hold of what they need to hide their tracks electronically. Asking American citizens and American companies to do technological backflips does not really solve the issue of getting after the characters we are most hopeful of putting behind bars.

MR. O'CONNOR: Did you have a question, sir, please?

MR. POULOS: My question is for Mr. Reinsch. I am Bill Poulos, with EDS. My question regards key-recovery crypto for communicated information. Would you please clarify the administration's policy for us. In earlier panels, we heard from both technical experts and business representatives that there was little or no demand for key-recovery encryption for communicated information. Is it the administration's policy to impose key-recovery crypto requirements for communicated information?

MR. REINSCH: Well, you haven't got the vocabulary quite right, Bill. The administration's policy is not to "impose" key recovery in any situation. It is to encourage and promote it. I want to be clear about that.

Having said that, we have not yet made a distinction between communication and stored data, which is not to say that we will not. However, I would suggest that, if we were to make such a distinction, and it is something we chronically think about, the distinction is really between stored data, e-mail, and other Internet communication, and
voice communication. The statement about the absence of a market for key recovery has been made most frequently with respect to voice communication in the marketplace, and I think it is probably the most accurate there. I would probably contest that statement if it were made about either of the other two segments.

To answer your question, however, we have not yet made a distinction in that regard, and, because we are not imposing or compelling, I am not sure we need to. It is something we continue to look at closely. In particular, we are looking at the voice communication issue, which is the most difficult piece of the puzzle, both from a law enforcement perspective and from a privacy and encryption perspective.

MR. O’CONNOR: I have an ISDN line at home. I make phone calls on it, and I have Internet traffic going out on it at the same time. I presume that my voice and my data are going out in the same packet stream. What is the difference? If you are trying to pick off voice, you are also trying to pick off data.

MR. REINSCH: In that particular mode, there is not necessarily a difference, but there are means of voice communication other than the one you identify.

MR. O’CONNOR: That is true, but we would seem to be going to a marketplace where we would go in more of a packet data for voice, as well.

MR. REINSCH: Yes.

MS. DROLTE: I am Angela Drolte, with the Bureau of National Affairs. Secretary Reinsch, you mentioned that there is going to be a meeting next week of senior representatives, to deal with the issue of harmonization of export controls. Can you elaborate on that? Who, exactly, is going to be meeting? Can you tell us a little bit more about the working group and what issues you might be talking about?

MR. REINSCH: I do not want to elaborate too much. This is a regular meeting. This is not something special. It just happens to be next week, because the last one was...

MS. DROLTE: Is it just administration officials, or representatives of other countries?

MR. REINSCH: It is representatives of other countries. That is what Ambassador Aaron does. As I said, he has talked to over twenty countries. I can not remember them all, but he has been all over the place. We have spent the greatest amount of time, for a lot of reasons, with Canada, Japan, the United Kingdom, Germany, France, Sweden and the Netherlands. The eight of us have gotten together in a series of periodic meetings that began in the spring, and we have continued, at different levels and different times, to discuss different topics. As I indicated in my remarks, two working groups have developed out of that group at lower levels.
Periodically, some more senior representatives, at Ambassador Aaron's level, get together to talk about where things stand, progress, work programs, what they want to do in the future, and so on. That is the meeting I was referring to.

MR. ROTENBERG: Rory, I just got some news that actually may save the ambassador some time.

MR. REINSCH: I know what you are going to mention.

MR. ROTENBERG: You do? Well, let me share it with everyone else. There was a news item this morning in the Wall Street Journal indicating that the European Commission is expected today to reject a U.S. plan that would allow law enforcement to monitor Internet communications. Moreover, I have just now received a copy of the “European Commission Policy Framework for Security on the Internet,” which was released today in Brussels. It is a short document, so maybe we can make copies available. Among the highlights: "Encryption is often the only effective and efficient way of protecting confidentiality. Regulation of encryption would probably not be very efficient, because nobody can be prevented from using encrypted data." There is more: "Widespread availability of encryption can also prevent crime. As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not, however, prevent criminals from using these technologies."

Now, this strikes me as a lot of common sense and good policy. It seems to be the direction in which the European Commission is firmly committed. So, my question is: why does the United States not move in this direction?

MR. REINSCH: I need to be tactful on this point, and I will end up saying what was quoted in the article you referred to, namely, that we always welcome what the Commission has to say, just as we welcome what the OECD and other multilateral organizations have to say, but our contacts and work on this effort are bilateral efforts with individual countries and their governments.

MR. O’CONNOR: I know what that means. Does everyone else here know what it means?

MS. OLMER: I am Jody Olmer, from the U.S. Chamber. Regarding the last point, there has been a lot of concern in the business community that the administration is, frankly, not carrying the private sector's view into international fora. I can say that the U.S. Chamber would hope that the views discussed and the positions taken would be given very serious consideration by the administration, taking into full account the private sector's views on this issue before positions are advanced on behalf of the United States.
I want to beat up on Bill Reinsch a little bit, since he is here today, speaking for the administration. I feel somewhat comfortable in beating up on him because he is so widely respected in bipartisan circles for his fine career, both in Congress and now in the Department of Commerce.

The business community is very troubled when we hear statements like: "The government is going to buy products with key-recovery capabilities." I respectfully call that sort of thing "bullying" tactics, and I think that setting a de facto standard is very troubling. We believe that government is spending taxpayer dollars and, therefore, it has a responsibility to interact fully with the private sector on such important and contentious issues.

With the implementation of the Information Technology Management Reform Act and the Government Performance Results Act, there will be much more information technology work, currently being performed in the public sector, that will be shifted to the private sector, making such de facto standards questionable. Moreover, it would impose a great cost on the business community. If they were doing business or communicating with the government, surely they would opt to have two systems rather than to buy into a key-recovery system that is not supported at this point. So, we would hope the government has not decided to run off and purchase key-recovery products or, if they have, we would hope they would reconsider that position. If you have any comments about where they are on that, of course, we would like to know that, too.

MR. REINSCH: Well, I am a little surprised by your preamble about the United States paying attention to the private sector and carrying its message to the international fora. First of all, if you listen to Mr. Rotenberg, it sounds like no one believes anything the United States government says in international fora anyway, but they do believe what the private sector says. So, I am not sure you need more help from us to get your message across in international fora. From his point of view, I think you have gotten it across very effectively.

I can assure you that you have gotten your message across to us. I have spent a lot of time on this, and I think you would be hard-pressed to find people who believe that the Commerce Department, at least, is giving people short shrift and has not been willing to pay attention to them on this. We have tried very hard to listen. That does not mean that, at the end of the day, we always agree, but we all understand that problem.

I am a little surprised at your comment. You are the first person in a long debate that has ever suggested that the federal government ought not to be able to buy what it wants to buy, and I confess that I am a little confused by that. We are going to follow all federal procurement rules. It is going to be bid, and agencies are going to make judgments based on RFPs and submissions that people make, and so on and so forth. It
is going to be competed. I suppose there is always the possibility that nobody is going to want to sell us anything, in which case we would be hard-pressed to implement the policy you want, but it goes rather far to suggest that the federal government should not have the right to decide what it wants for its own use. For example, are you going to complain if we decide to buy Chryslers rather than Fords?

MS. OLMER: No, but is not the issue, in terms of this procurement, that the administration would seek to use its market power, in effect, to create the market for...

MR. REINSCH: We can not help it. When we buy automobiles, it has the same effect.

MR. OLMER: That does not make it right.

MR. REINSCH: People buy Chrysler, it helps them. I can not do anything about that.

MR. O'CONNOR: Well, let me just say there's a little bit of relevant history here, because the standard did not come about through a whim. In 1994, a proposal was issued for the escrowed encryption standard, which was FIPS 185, the standard that was proposed for federal agencies. The Department of Commerce, Mr. Reinsch's department, solicited public comment on the standard. There were more than 300 detailed comments in opposition. There were only a handful in support. These were comments coming from businesses, users, technologists. The proposed standard was widely rejected by the user community, and still the Commerce Department went forward.

So, it is not quite the same situation as when you are talking about Fords or Chryslers. You are talking about standards, where there has been a solicitation of public viewpoint, and that viewpoint was provided and then was largely ignored. That is really an issue of whether or not it makes sense to go forward with key recovery, never mind the fact that the National Research Council just finished saying it would be a mistake for the government to promote this technology actively at this point in time.

AUDIENCE MEMBER: Two issues. First, the government spends $200 billion every year on business services, and they do have a responsibility to buy very competitive products. If the private sector does not want to spec the system, but those products are not out there, and the government is the only one buying, then they are suppressing market forces. If they have to go outsource the system in the private sector and that has to be done by other specifications to accommodate key recovery, then that is going to cost more.

This is very different from when the United States government set the standard for transportation infrastructure. The U.S. government said, "Here are the standards for our highways all across the nation," and they set those standards because military
trucks would be going down the highways. In case you do not know this, the right shoulders must be built more steady, so that the trucks can roll on the side, but the government paid for that. They have paid for that infrastructure, and this is very different. This is a product that the government would be using and that the private sector would be forced to interact with, so on Rory's point, market forces could create a de facto standard.

MR. REINSECH: Do you want to keep going or do you want...I think we disagree fairly fundamentally, both about the purpose of government as well as a lot of other things.

MR. O'CONNOR: I would also be curious on the other side of this, out of this $200 billion, how much of it is going to be spent on encryption?

MR. REINSECH: You got me. I have no idea. There are many, many examples, mostly in the defense and national security area, but that is also one of the equities I mentioned in this case, of the government setting up special, if not peculiar, procurement requirements for its own use and trying to promote the development of products that do not have broad applicability, because we think we need them. Most people don't complain. Most of the time, they are defense products. I guess I'm just surprised.

MR. O'CONNOR: I am sorry, but I have been asked to stop here for a five-minute break. I want to thank every...

MR. REINSECH: Ed's question.

MR. O'CONNOR: That's right. I'm sure Ed will get his question in at some point.

PANELIST: Oh, I will do it real quick. I get that prerogative. No, it should follow up what went on with Secretary Reinsch, because he has been very forthright here, in testimony about the need for this administration policy to work, to have multilateral agreement and acceptance. Marc also made some very compelling points, I think, about the difficulty he as perceived in getting that consensus, and that coincides with a lot of private communications we have had with different embassies and governments.

I realize that Bill can not nail us down to an exact timeframe, but the question I want to ask is how long is long enough to get multilateral agreement? Six months? A year? Two? Five? You said it is essential that it be there for the administration policy to be viewed as successful, so there has to be a point at which you say, "Okay, we are going to get that support or we are not," and you stop saying, "Well, we are talking and we are hopeful."
MR. REINSCH: Well, I will say two things. First, every prediction I have ever made about when we were going to finish anything turned out to be wrong, so I am increasingly reluctant to make predictions. Somebody asked a similar question this morning, and I ended up saying, "The one thing I'll guarantee is that it will take...." Well, I'm not going to say that, because you will disagree.

PANELIST: Give it a try.

MR. REINSCH: No, no. "Soon" was what I said. In some respects, though, I think the answer is that it is going to be driven or decided as much by the market as it is by negotiations. That is, if we do not get moving and come to some kind of closure, market developments and widespread availability, as well as use of non-key-recovery technology, is going to overrun the effort to develop multilateral policy. I think that is moving faster. It is really a question of how fast that is moving and when you think it will reach that point.

Now, I know there are plenty of people in the hardware and software communities who believe we are already there. As you know, from having suggested it to me in the past, I do not agree that we are there, but I think we are going to be there in a short time. As far as we are going here, we have to pull some things together and create foundations in six months to a year.

I hope that, if this is not working, we will be smart enough to figure that out and retool but, at this point, I do not agree that it is not working.

MR. O'CONNOR: There is a strange sense of deja vu. I think I was on a similar panel with Mike Nelson, about four years ago, and similar predictions were being made.

MR. REINSCH: That's why I don't make predictions.

MR. O'CONNOR: Yes. Well, okay. We've got about six months to a year, as I remember. I want to thank the panel very much, and I thank Secretary Reinsch, especially, for coming to get beaten up.
SPEAKER AND MODERATOR BIOGRAPHIES

Congressman Edward J. Markey
Ranking Minority Member, Commerce Subcommittee on Telecommunications, Trade and Consumer Protection

Edward J. Markey represents the 7th Congressional District of Massachusetts. He serves on the House Commerce Committee, where he is the highest ranking Democratic member of the Telecommunications, Trade & Consumer Protection Subcommittee. He is also a member of the Energy and Power Subcommittee and the Finance and Hazardous Materials Subcommittee. In addition, Rep. Markey is the second ranking Democrat on the Resources Committee and is a member of the Commission on Security and Cooperation in Europe.

Rep. Markey's post on the Telecommunications Subcommittee, a panel he chaired from 1987 through 1994, is one that holds particular interest for him because of its vital importance to Massachusetts workers and the Commonwealth's economy. Issues such as high-technology job growth, telecommunications, financial services and consumer protection are major concerns of the Subcommittee. Also, as a senior Member of the House panels that set energy policy, Rep. Markey plays an influential role in energy efficiency issues that are important to the New England states.

Ed Markey was born in Malden, Massachusetts, on July 11, 1946. He attended Boston College (B.A., 1968) and Boston College Law School (J.D., 1972). He served in the U.S. Army Reserve before completing his legal education.

William A. Reinsch
Under Secretary for Export Administration, U.S. Department of Commerce

Bill Reinsch currently serves as the Under Secretary for Export Administration in the U.S. Department of Commerce.

As head of the Bureau of Export Administration (BXA), Mr. Reinsch is charged with administering and enforcing the export control policies of the U.S. government, as well as its antiboycott laws. In addition, the Bureau is part of an interagency team helping Russia and other newly emerging nations develop effective export control systems and convert their defense industries to civilian production. Through its Office of Strategic Industries & Economic Security, BXA is also responsible for monitoring and protecting the health of U.S. industries critical to our national security and defense industrial base and assisting in domestic defense conversion efforts.
From 1991 through 1993, Mr. Reinsch was a senior Legislative Assistant to Senator John D. Rockefeller IV, responsible for the Senator’s work on trade, international economic policy, foreign affairs and defense. From 1977 to 1991, Mr. Reinsch served on the staff of the late Senator John Heinz as Chief Legislative Assistant, focusing on foreign trade and competitiveness policy issues. Prior to 1977, Mr. Reinsch was a Legislative Assistant to Representatives Richard Ottinger and Gilbert Gude, acting Staff Director of the House Environmental Study Conference, and a teacher in Maryland.

In addition to his legislative work, Mr. Reinsch has serves as an adjunct associate professor a the University of Maryland University College Graduate School of Management and Technology since 1990, teaching a course in international trade and trade policy. He is also President of the Saint Mark Elderly Housing Corporation, a non-profit corporation that runs Saint Mark House, a home for the frail elderly in Rockville, Maryland.

Mr. Reinsch received a B.A. degree in International Relations from The Johns Hopkins University and an M.A. degree from The Johns Hopkins School of Advanced International Studies. He lives in Bethesda, Maryland, with his wife and two sons.

Marc Rotenberg

Director, Electronic Privacy Information Center

Marc Rotenberg is Director of the Electronic Privacy Information Center (EPIC) in Washington, DC and former head of the CPSR Washington office. He was counsel to the Senate Judiciary Committee specializing in technology and the law. He teaches information privacy law at Georgetown University Law Center and has testified before Congress on many issues, including access to information, encryption policy, computer security, and communications privacy. He debated Senator Exon on CNN when the Communications Decency Act was introduced and FBI Director Sessions on ABC Nightline when the FBI wiretap bill was proposed. He helped organize grassroots campaigns against Lotus Marketplace and the Clipper encryption scheme, and is now coordinating the Internet Privacy Coalition. Marc is secretary of Privacy International, an international human rights organization. He is a graduate of Harvard College and Stanford Law School and a member of the bar of the United States Supreme Court.

Rory J. O’Connor - moderator

Washington Correspondent, San Jose Mercury News

Rory J. O’Connor, Washington Correspondent/Technology for the San Jose Mercury News, has covered the encryption controversy extensively since 1992. In his 18-year career as a journalist, he has followed the development of the personal computer
business in Silicon Valley, where he worked as a reporter, editor and columnist from 1981 until his transfer to Washington in 1995.

As the senior member of the Mercury News technology staff, his current beat focuses on technology policy and has taken him from the White House to Capitol Hill to the Supreme Court for stories concerning telecommunications reform, export controls, technology in education, computer crime, the application of high-technology in the Congress, immigration and technology transfer programs.

His work has been awarded prizes by the Associated Press News Executives Council, the California Newspaper Publishers Association and the Software Publishers Association. He was part of the 300-person newsroom staff awarded the Pulitzer Prize for its coverage of the 1989 Loma Prieta earthquake in Northern California. O’Connor lives in Takoma Park, Md. with his wife, Irene Fuerst, and their two children.
Keynote Speaker: The Prospects for Political Compromise

Senator John Ashcroft

Member of the Senate Commerce, Foreign Relations and Judiciary Committees

I. The Future of Internet and Electronic Commerce

A. Privacy

The need for and protection of privacy in an electronic world cannot be overstated. If we are to operate at our highest and best in the information age, U.S. citizens should have the same rights and protections on the Internet as they have in other forums.

To date, we have heard a great deal about the needs of law enforcement and not enough about the privacy needs of the rest of us. Without the protection of privacy, the Internet is doomed to the status of an international party line or an international broadcast device and will never become a useful means of commerce, communication, and entertainment.

As we work to provide law enforcement with some necessary amount of access, let us do so in a manner consistent with the Constitution, as we have done in the past with telephone lines and computer hard drives.

While we need to revise our laws to reflect the digital age, one thing that does not need revision is the Fourth Amendment. The Founding Fathers crafted the Constitution to protect our most basic liberties. Those protections have kept Big Brother from intruding into our private lives for over 200 years. Removal of these protections is now being advocated, which would leave citizens open to the invasion of their privacy, for the sake of security.

I am deeply troubled by the Administration’s insistence that we should turn over the keys to our individual privacy to federal agents. In recent weeks, we have heard blood-chilling tales of abuse of innocent citizens by the IRS. Only a few months ago, the nation was shocked to learn of snooping in tax returns by IRS employees. Before that, we discovered that the FBI had handed over hundreds of sensitive private files to political operatives in the White House.
The outrages against privacy committed by federal law enforcement agencies means one thing: Now, more than ever, we must protect citizens’ privacy from the excesses of an arrogant, overly powerful government.

Law enforcement is using advances in digital technology as an excuse to insist on intrusions into privacy that were never allowed in the pre-digital era. For example, I doubt the Founding Fathers would have ever required every citizen to provide the government a key to their homes, bank accounts, medical records, investments, or their diaries.

Law enforcement officials tell us that a key recovery system will make it easier for law enforcement to do its job. But it would also make things easier on law enforcement if we repealed the Fourth Amendment. But that is not the American way. The way to fight crime is to get tough with criminals, not to take away the privacy rights of innocent citizens.

B. Commerce/Communications

The Internet is the most participatory form of communications ever developed and offers the potential for a low cost means of commerce for everything from clothes to real estate to software.

Electronic commerce has not reached its full potential. Many areas must be examined in order to actually conduct business, including a legally binding signature.

We must also make improvements with respect to the availability of robust encryption. Business must be able to protect their transmissions from hackers -- those with malicious intent or who are out for a lark.

Stronger encryption clearly exists on the world market, and foreign competition is clearly outpacing our domestic industry. We cannot afford to forfeit our edge in high tech industry, an industry in which the U.S. has always been dominant.

Although government clearly can make matters worse by imposing inefficient export restrictions, government does not have a monopoly on the solutions to the challenge of maximizing opportunities for commerce on the Internet. Private industry must take the lead on many issues related to the Internet and find solutions, including self-regulation.

II. The Importance of Encryption

Encryption is the most important issue to the future of electronic commerce. If we are to promote the integrity of the Internet, we must have secure means of communication, domestically and internationally.
Fundamentally this debate is about the relationship of our citizens to our government. We must take steps to ensure that their rights are not violated. Our citizens should be able to communicate privately, without the government listening in.

We must focus on allowing trustworthy parties to use robust encryption -- not necessarily only allowing the sale of encryption -- but also to allow the use in private transactions and in the development of software and hardware.

A. Export

We must allow your industry to compete in an international market where robust encryption already exists. The technology industry in the country, and the software industry in particular, is a world leader. Other countries are seizing ground because our outdated export law is not in sync with technological realities. (e.g. Siemens)

The recent procedure of permitting 40 bit, and 56 bit with special permission has already been relaxed by the Administration to allow 128 bit for specific financial and banking systems. At the same time the Administration still prohibits the export of encryption to compete with others.

The Administration’s export restrictions not only hurt the competitiveness of American industry, but also needlessly anger our allies. Many of our allies recognize the superiority of American technology and resent America’s unwillingness to share its best encryption technology. Today’s Wall Street Journal quotes a European Commission official as saying that, “they treat us as if we were Baghdad even though we fought on the same side in the Gulf War.”

B. Domestic issues

Currently, the Administration and the FBI are demanding language that would allow the FBI real-time access to all domestic Internet communications.

Although the Administration has not yet demanded mandatory domestic key recovery, they have rejected every alternative. For example, Director Freeh has been candid about the limits of any form of non-mandatory key recovery. He has emphasized that criminals are unlikely to opt-in to a non-mandatory system.

If you sort through the Administration’s position and decrypt it, it is clear that mandatory domestic key recovery is among the Administration’s goals - a move we must resist.

The Administration has focused on national security concerns. But the Administration seems to ignore the fact that national security is compromised when we make policy that forces U.S. companies to transact business outside the U.S. without the
benefit of encryption. Under the terms of the Administration language there are no exceptions, so presumably even enterprises that do defense contract work for the U.S. would have to broadcast their plans to the world as they use e-mail.

I am far from alone in criticizing the Administration’s encryption policy. Today’s Wall Street Journal reports that the European Commission is expected to issue a policy paper today strongly critical of both the Administration’s export restrictions and its advocacy of mandatory key recovery systems. Commission officials are convinced that a key recovery system will compromise security on the Internet and may be incompatible with European data privacy laws. The Wall Street Journal quoted a European encryption specialist as concluding that, “Nobody will trust the security of U.S. encryption products. People just assume they are insecure because of the U.S. policy to build in a back door for law enforcement.”

The forthcoming European Commission report provides further evidence of what everyone in this room has long understood: We must rethink the Administration’s approach to encryption.

C. Legislative Approach

We must promote a sensible, reasonable alternative to the current Administration policy that can attract the support we need to win. We need an approach that builds on and improves the PRO-CODE approach reflected in Senator Burns’ Commerce Committee bill.

Any encryption bill must address both the international and domestic aspects of the encryption issue. As for the international dimension of the problem, we must ensure that our export policy reflects the realities of the international marketplace.

With respect to domestic encryption issues, we need an approach that protects the legitimate interests of law enforcement but does not ignore the privacy interests of individual Internet users or the public interest in expanding electronic commerce.

As the encryption debate moves from the Commerce Committee to the Judiciary Committee, I will continue to work for a comprehensive approach to encryption. Senator Lott has assured me that a balanced approach to encryption is one of his priorities.

I have already conferred with Representative Goodlatte, and I think there is much in his bill that should be incorporated into Senate bill. Senator Leahy’s proposal provides a solid move towards a comprehensive approach that addresses both the international and domestic aspects of the encryption problem. These two proposals provide significant guidance for a bill that can be passed in the Senate.

In closing, I want to thank you once again for your work on the important issue
of encryption. I look forward to working with you to come up with workable legislation in the Senate. And once that legislation is finalized, I hope I can count on you to work with me to ensure its passage.
Biography

Senator John Ashcroft
Member of the Senate Commerce, Foreign Relations and Judiciary Committees

John Ashcroft of Missouri was elected to the United States Senate in 1994, winning 60 percent of the vote and carrying every county in the state. Prior to his election to the Senate, he served Missourians as their governor for two terms, winning reelection in 1988 by 64 percent, the largest percentage of any Missouri governor since the Civil War.

In the Senate, Ashcroft has taken a leading role on key issues. In the 105th Congress, he is a principal sponsor of three of the “Top Ten” legislative priorities: new scheduling flexibility for workers striving to meet the needs of job and family; comprehensive action against violent juvenile crime; and reform of the civil justice system, by updating laws on product liability.

Ashcroft presently serves on three Senate committees, Judiciary; Commerce, Science, and Transportation; and Foreign Relations. He is the chairman of subcommittees on the Constitution, Consumer Affairs, and Africa, respectively.

Ashcroft also is widely recognized for his innovative use of technology and the Internet. He conducted the first-ever congressional on-line petition for an issue before Congress (term limits), and has taught students in Missouri and across the country about using the Internet and on-line information as a tool of citizenship.

Ashcroft was born on May 9, 1942. He attended public schools in Springfield, Missouri, and graduated with honors from Yale University in 1964. He met his wife, Janet, at the University of Chicago Law School where they each received law degrees in 1967, and later co-authored two college textbooks. They have three children, Martha Patterson, Jay, and Andrew.