[James P. Chandler, John D. Podesta. (Jun. 07, 1993). Third CPSR Cryptography and Privacy Conference included Stephen Crocker, NPR, ABC, US West, Ann Harkins, Ken Mendelson, Juan Osuna, Cathy Russell, Steven Wolff, James Chandler, IBM, HP, FBI, Mitre Corp, C.I.A., NSA, FBI, ACLU, Oracle, Deloitte, Qualcomm, NIST, Wilmer LLP, George Washington University, New York Times, MIT, Washington Post, Apple, Digital, AT&T. Judicial Watch FOIA No. 9403963. U.S. Dept. of State, U.S. Justice Department.]

p 65, 67
275

THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE

UNCLASSIFIED EXCISE

June 7, 1993

Carnegie Endowment for International Peace
2400 N. Street, NW
Washington, DC

8:30 **Coffee**

9:00 **Welcome and Introductions**

9:30 **Introduction to Cryptography**

David Kahn, a noted historian of cryptography, will provide an overview of cryptography and discuss the current trend toward use in everyday activities.

10:00 **Government Cryptography Policy**

In the past several years, law enforcement and intelligence agencies have attempted to restrict the public development and implementation of cryptography. This panel will discuss recent developments including the Clipper Proposal, the Digital Signature Standard and the roles of NIST and the NSA under the Computer Security Act of 1987.

Moderator:	Rick Weingarten, Executive Director, Computer Research Associates
Participants:	John Podesta, Staff Secretary, The White House David Sobel, Computer Professionals for Social Responsibility Ray Kammer, Acting Director, National Institute for Standards and Technology Dr. Steven Bryen, Secure Communications Technology

11:15 **Break**

11:30 **The Digital Telephony Proposal**

In 1992 the Federal Bureau of Investigation introduced a proposal to require that telecommunications manufacturers and service providers redesign their systems to facilitate wiretapping. This panel will discuss the implications of that proposal on privacy, security and the telecommunications network.

Moderator:	David Flaherty, Wilson Center/University of Western Ontario
Participants:	Janlori Goldman, Privacy and Technology Project, ACLU James K. Kallstrom, Federal Bureau of Investigation Dr. Dorothy Denning, Georgetown University William Murray, Deloitte and Touche

12:30 **Lunch (provided)**

UNCLASSIFIED

DEPARTMENT OF STATE IM/IPS/CR/IR Date
( ) RELEASE ( ) DECLASSIFY
(✓) EXCISE ( ) DECLASSIFY IN PART
( ) DENY EO Citations
FOIA Exemptions B5, B7E ( ) CLASSIFY as ( ) S or ( ) C OADR TS authority to
PA Exemptions ( ) DOWNGRADE TS to ( ) S or ( ) C

9403963

1:15 Debate - Encryption Policy, Privacy and Government Secrecy

Moderator: Professor Lance Hoffman, George Washington University

Participants: Whitfield Diffie, Sun Microsystems
Alan R. McDonald, Federal Bureau of Investigation

2:00 Export Controls

Currently, federal regulations restrict products that contain encryption from export. This panel will discuss the problems that these restrictions present and how they affect the use of cryptography within the United States.

Moderator: Roszel Thomsen, McKenney, Thomsen & Burke

Participants: Ilene Rosenthal, Software Publishers Association
Allan Suchinsky, Office of Defense Trade Controls, State Department
David Peyton, Information Technology Association of America

3:00 Cryptography in Everyday Use

This panel will look at the present and future applications of public key cryptography including Digital Cash, Privacy-Enhanced Mail, and Pretty Good Privacy.

Moderator: ~~Mikki Barry~~ Wayne Matson, Intercon Systems

Presenters: Phil Zimmerman, Pretty Good Privacy
Steve Crocker, Trusted Information Systems
David Chaum, DigiCash

4:00-6:00 Reception at Carnegie

Marc Rotenberg, David Banisar
CPSR Washington Office
202-544-9240 (voice),
202-547-5481 (fax)
rotenberg@washofc.cpsr.org
banisar@washofc.cpsr.org

CPSR Cryptography and Privacy Conference
June 7, 1993

Name	Organization
John Adams	IEEE Spectrum
Charlotte Adams	FCW
Michael Autrey	Privacy Times
Stewart Baker	NSA
Brian Baker	CUA Law School
James Bamford	ABC World News Tonight
David Banisar	CPSR
Mikki Barry	Intercon Systems
Jerry Berman	Electronic Frontier Foundation
Jim Bidzos	RSA
Denis Bieber	SecurTech
Jane Bortnick	Congressional Research Service
Martina Bradford	AT&T
Clint Brooks	NSA
Reese Brown	Jnl of Intel. and Counter-Intel.
Steven Bryen	SecurTech
David Burnham	TRAC
Jean Camp	IEEE
Karen Casser	
James Chandler	GWU
Dan Charles	NPR
David Chaum	DigiCash
John Cohen	House Judiciary Committee
Sarah Comley	
Dan Cook	Department of State
Steven Crocker	TIS
Colin Crowe	House Telecomm
Jim Dempsey	House Judiciary Commitee
Dorothy Denning	Georgetown University
Whitfield Diffie	Sun Microsystems
Mario Einaudi	CPSR
Woody Evans	US West
David Farber	University of Pennsylvania
Addison Fischer	Fischer International
David Flaherty	Wilson Center
Greg Frazier	House Committee on Intelligence
Bob Gellman	House Govt. Operations Comm
Frank Gilbert	
John Gilmore	Cygnus Support
Sol Glasner	Mitre
Janlori Goldman	ACLU
Harry Goodman	NPR
Tom Guidoboni	

UNCLASSIFIED

CPSR Cryptography and Privacy Conference
June 7, 1993

Name	Organization
Ann Harkins	Senate Judiciary Committee
Evan Hendricks	US Privacy Council
Ezra Herman	BNA
Lance Hoffman	George Washington University
Paul Hyland	CPSR
David Johnson	Wilmer, Cutler & Pickering
David Kahn	Newsday
Jim Kallstrom	FBI
Ray Kammer	NIST
Phil Karn	Qualcomm
Stuart Kern	Department of Treasury
Jack King	BNA Legal Report
Rob Kurz	House Govt. Operations
Steven Levy	MacWorld
Herb Lin	National Acadamy of Sciences
Steve Lipner	Mitre
Wayne Madsen	Computer Sciences Corp
Fred Mailman	HP
John Markoff	NY Times
Kate Martin	CNSS/ACLU
Alan McDonald	FBI
Kate McGee	Oracle
John McMullen	Newsbytes
Lynn McNulty	NIST
Brock Meeks	Communications Daily
Ken Mendelson	House Judiciary Committee
Ellen Messmer	Network World
John Mintz	Washington Post
William Murray	Deloite and Touche
Mike Nelson	OSTP
Juan Osuna	CRA
Bill Pauli	Apple Computer
Beverly Peterson	GAO
David Y. Peyton	ITAA
Harold Podell	General Accounting Office/OSI
John Podesta	The White House
Bill Poulis	Apple Computer
Bob Rarog	Digital Equipment Corp.
Mitch Ratcliffe	MacWeek
Harold Relyea	Congressional Research Service
Jeff Richelson	National Security Archive
Ilene Rosenthal	Software Publishers Association
Marc Rotenberg	CPSR

UNCLASSIFIED

CPSR Cryptography and Privacy Conference
June 7, 1993

Name	Organization
Debbie Rudolph	IEEE
Cathy Russell	Senate Judiciary Committee
Jeff Schiller	MIT
Wynn Schwartau	Inter*Pak
John Schwartz	Washington Post
Bob Smith	Privacy Journal
Olly Smoot	CBEMA
David Sobel	CPSR
John Sonderman	Department of State
Ross Stapleton	CIA
Gary Stern	ACLU
Allan Suchinsky	Department of State
Roszel Thomsen	McKenney, Thomsen & Burke
Lee Tien	
Peter Wayner	Georgetown University
Rick Weingarten	Computer Research Association
Danny Weitzner	Electronic Frontier Foundation
William Whitehurst	IBM
Steven Wolff	NSF
Phil Zimmermann	Boulder Software Engineering

UNCLASSIFIED

MEMORANDUM

TO: The Files

FROM: PM/DTC/CED: John Sonderman

SUBJECT: CPSR Cryptography and Privacy Conference
June 7, 1993, Washington, DC

The first speaker was David Kahn, author of The Codebreakers. He gave an overview of cryptography. He claimed cryptographic growth follows communication growth, as communications expand, cryptography expands. Governments want to prevent the growth of cryptography to maintain order and security. The government feels it must know what is happening in society. The U.S. government is trying to control cryptography through export controls and introduction of the clipper chip. Both help maintain the status quo and prevent privacy from advancing.

Kahn went on to state that privacy is good. A balance must be made between national security and privacy/profit. He claimed if you outlaw good crypto only the outlaws will have good crypto. Further, while the government wants to hold back technology, it can't, the government can only delay technology. He pointed out that even Iran is on the BITNET. Philip Zimmermann then stated trying to stop cryptography was "...like trying to stop the wind."

Zimmermann went on to state that the government was on the "...wrong side of the power curve... it may not be a choice of are we going to live in a world of unbreakable crypto, we can't stop it, we must find a way to adjust." Zimmermann claimed that while outlawing drugs and alcohol may have merits, outlawing cryptography had no basis. He claimed "cryptography doesn't hurt people."

Kahn concluded that there are three government proposals currently: CCEP, DSS, and Clipper. Each alone is innocuous, but all three together are something else.

UNCLASSIFIED

The next speaker was Ray Kammer, acting director of NIST. He addressed the Clipper initiative. He stated that Clipper is currently delayed do to problems finding key escrow agents and export control issues.

David Sobel, CPSR, spoke next on the Digital Signature Standard and the Computer Security Act of 1987. The act divided government cryptography into two categories, military controlled by NSA, and civilian controlled by NIST. Yet with DSS, of the documents CPSR obtained, 143 were from NIST and 1,138 were NSA. Sobel claimed NSA was running civilian cryptography, and that this was probably true in Clipper as well.

Dr. Steven Bryen, Secure Communications Technology, spoke on Clipper. He claimed Clipper was technology that will compete with his private sector products. Bryen stated that NIST/NSA had not identified the threat that clipper helps diminish. He also claimed Clipper was a domestic solution to an international problem. U.S. firms need secure communication abroad, and foreign governments might not allow Clipper in, or if they did demand the escrow keys.

Zimmermann then added a few comments. He said he was just back for Eurocrypt, and that he had learned that SHA hash algorithm was pretty good. He also stated:

> Clipper is voluntary for the moment until the other shoe drops... throw the baby out with the bath water, put the entire population at risk to catch a few criminals

Zimmermann continued stating that "...someday the government may change to a bad government... government has a history of abuse, there is a crying need for cryptography... not to employ cryptographic technology..." helps a police state.

John Gilmore claimed the counter reaction to the clipper proposal could be far more wide spread use of non-clipper encryption. Gilmore questioned how the intel community would interface with the escrow system.

During a break, Stephen Crocker of Trusted Information Systems approached me and expressed his frustration with DTC. He claimed he had sent several letters requesting permission to put his TIS/PEM product on his FTP server. Having received no reply, he went ahead and did it anyway.

Several FBI agents spoke on the merits of the FBI Digital Telephony Proposal. The main criticism expressed by the audience was that the FBI hadn't justified the need for the proposal.

John Podesta of the White House spoke on the Clipper proposal. He claimed clipper addressed three issues: (1) providing a higher level of security, (2) takes advantage of advances in technology, and (3) takes into consideration the needs of law enforcement.

David Peyton, Information Technology Association of America spoke first on export controls. He claimed government policy needed to get in touch with reality. Cryptographic technology was available outside the U.S. and current policy was a "unilateral give away" to Britain and Finland. U.S. vendors are kept at a "policy disadvantage." He wanted the U.S. to decontrol cryptography over the Internet and to adopt the rules agreed to at COCOM. Exports should be allowed to legitimate end users in friendly countries.

Ilene Rosenthal, Software Publisher Association, also addressed foreign availability. She stated that increases in foreign sales meant more customers want cryptographic functions in the software. Sophisticated customers want the best security including DES. Foreign cryptographic products now dominate the market with 143 foreign software manufacturers from 13 countries. She also claimed the Internet made cryptography widely available including PGP which has become a standard in Europe.

Alan Suchinsky and Dan Cook of PM/DTC spoke on current export restrictions. Glenn S. Tenney of Fantasia Systems, Inc. asked how many investigations into export violations for cryptography were ongoing. Suchinsky said he did not know but would find out. During questions about criteria for export Zimmermann added "how about common sense?"

Steve Crocker, of Trusted Information Systems (TIS) spoke on his companies implementation of Privacy Enhanced Mail (PEM). TIS/PEM, as it is called, provides security, confidentiality and authentication. Crocker said he has mounted TIS/PEM on his Internet FTP server for anonymous access, but he had implemented some controls to reduce international distribution. TIS/PEM uses MD2, MD5, DES and RSA.

Philip Zimmermann spoke on his software program called Pretty Good Privacy (PGP). Zimmermann said PGP uses RSA/IDEA for encryption, RSA/MD5 to sign messages, plaintext compression, pass phrases with MD5 form IDEA keys and a grass roots trust model for public key certification. Zimmermann said he plans to change the signature mechanism from MD5 to IDEA after Zimmermann learned of weaknesses in MD5 while attending EUROCRYPT '93.

UNCLASSIFIED

Zimmermann went on to state that PGP was published in June of 1991. Zimmermann claimed he did not know about the internet himself, but gave it to a friend that posted it onto netnews groups with a USA distribution set. He stated pgp was a "grass roots social phenomenon" and a matter of free speech. He claimed you "can't stop this."

UNCLASSIFIED

DRAFT

UNCLASSIFIED

[redacted]

MEMORANDUM

TO: ODUSD/DTSA/ML - Col. Richey

FROM: PM/DTC/CEB - Clyde G. Bryant, Jr.

B5
B7

UNCLASSIFIED

DRAFT

UNCLASSIFIED

United States Department of State

Washington, D.C. 20520
Bureau of Politico-Military Affairs

CENTER for DEFENSE TRADE

OFFICE OF DEFENSE TRADE CONTROLS

PM/DTC

Only UNCLASSIFIED Information may be transmitted by FAX

TO: S/A Robin Sterzer (Name) USCS (Office) 6/10/93 (Date)

FAX #: 408-291-4151

TEL #: 408-291-4162

FROM: John Sonderman (Name) PM/DTC/CEB (Office)

FAX #: 703-875-5663

TEL #: 703-875-5650

SUBJECT: CPSR Crypt & Priv. Conf; please call to clear on Memo to DTSA

Number of Pages Transmitted in this FAX: 11 incl cover

UNCLASSIFIED

--UNCLASSIFIED--

ENCRYPTION FAQ

FROM WWW.NIST.COM

NO

60

9403964

Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them.

In a multi-user setting, encryption allows secure communication over an insecure channel. The general scenario is as follows: Alice wishes to send a message to Bob so that no one else besides Bob can read it. Alice encrypts the message, which is called the plaintext, with an encryption key; the encrypted message, called the ciphertext, is sent to Bob. Bob decrypts the ciphertext with the decryption key and reads the message. An attacker, Charlie, may either try to obtain the secret key or to recover the plaintext without using the secret key. In a secure cryptosystem, the plaintext cannot be recovered from the ciphertext except by using the decryption key. In a symmetric cryptosystem, a single key serves as both the encryption and decryption keys.

What is authentication? What is a digital signature?

Authentication in a digital setting is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message. Authentication protocols can be based on either conventional secret-key cryptosystems like DES or on public-key systems like RSA; authentication in public-key systems uses digital signatures.

In this document, authentication will generally refer to the use of digital signatures, which play a function for digital documents similar to that played by handwritten signatures for printed documents: the signature is an unforgeable piece of data asserting that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient, as well as a third party, can verify both that the document did indeed originate from the person whose signature is attached and that the document has not been altered since it was signed. A secure digital signature system thus consists of two parts: a method of signing a document such that forgery is infeasible, and a method of verifying that a signature was actually generated by whomever it represents. Furthermore, secure digital signatures cannot be repudiated; i.e., the signer of a document cannot later disown it by claiming it was forged.

Unlike encryption, digital signatures are a recent development, the need for which has arisen with the proliferation of digital communications.

What is public-key cryptography?

Traditional cryptography is based on the sender and receiver of a message knowing and using the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is known as secret-key cryptography. The main problem is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, or a phone system, or some other transmission system to not disclose the secret key being communicated. Anyone who overhears or intercepts the key in transit can later read all messages encrypted using that key. The generation, transmission and storage of keys is called key management; all cryptosystems must deal with key management issues. Secret-key cryptography often has difficulty providing secure key management.<P>

Public-key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman in order to solve the key management problem. In the new system, each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. The need for sender and receiver to share secret information is eliminated: all communications involve only public keys, and no private key is ever transmitted or shared. No longer is it necessary to trust some communications channel to be secure against eavesdropping or betrayal. Anyone can send a confidential message just using public information, but it can only be decrypted with a private key that is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used for authentication (digital signatures) as well as for privacy (encryption).

Here's how it works for encryption: when Alice wishes to send a message to Bob, she looks up Bob's public key in a directory, uses it to encrypt the message and sends it off. Bob then uses his private key to decrypt the message and read it. No one listening in can decrypt the message. Anyone can send an encrypted message to Bob but only Bob can read it. Clearly, one requirement is that no one can figure out the private key from the corresponding public key.

Here's how it works for authentication: Alice, to sign a message, does a computation involving both her private key and the message itself; the output is called the digital signature and is attached to the message, which is then sent. Bob, to verify the signature, does some computation involving the message, the purported signature, and Alice's public key. If the results properly hold in a simple mathematical relation, the signature is verified as genuine; otherwise, the signature may be fraudulent or the message altered, and they are discarded.

What are the advantages and disadvantages of public-key cryptography over secret-key cryptography?

The primary advantage of public-key cryptography is increased security: the private keys do not ever need to transmitted or revealed to anyone. In a secret-key system, by contrast, there is always a chance that an enemy could discover the secret key while it is being transmitted.

Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. A sender can then repudiate a previously signed message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos secret-key authentication system involves a central database that keeps copies of the secret keys of all users; a Kerberos-authenticated message would most likely not be held legally binding, since an attack on the database would allow widespread forgery. Public-key authentication, on the other hand, prevents this type of repudiation; each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation.

Furthermore, digitally signed messages can be proved authentic to a third party, such as a judge, thus allowing such messages to be legally binding. Secret-key authentication systems such as Kerberos were designed to authenticate access to network resources, rather than to authenticate documents, a task which is better achieved via digital signatures.

A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method. But public-key cryptography can share the burden with secret-key cryptography to get the best of both worlds.

For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. The public-key system can be used to encrypt a secret key which is then used to encrypt the bulk of a file or message.

Secret-key cryptography remains extremely important and is the subject of much ongoing study and research.

Is cryptography exportable from the U.S.?

All cryptographic products need export licenses from the State Department, acting under authority of the International Traffic in Arms Regulation (ITAR), which defines cryptographic devices, including software, as munitions. The U.S. government has historically been reluctant to grant export licenses for encryption products stronger than some basic level (not publicly stated).

Under current regulations, a vendor seeking to export a product using cryptography first submits an request to the State Department's Defense Trade Control office. Export jurisdiction may then be passed to the Department of Commerce, whose export procedures are generally simple and efficient. If jurisdiction remains with the State Department, further review, perhaps lengthy, is required before export is either approved or denied; the National Security Agency may become directly involved at this point. The details of the export approval process change frequently.

The NSA has de facto control over export of cryptographic products. The State Department will not grant a license without NSA approval and routinely grants licenses whenever NSA does approve. Therefore, the policy decisions over exporting cryptography ultimately rest with the NSA.

It is the stated policy of the NSA not to restrict export of cryptography for authentication; it is only concerned with the use of cryptography for privacy. A vendor seeking to export a product for authentication only will be granted an export license as long as it can demonstrate that the product cannot be easily modified for encryption; this is true even for very strong systems, such as RSA with large key sizes. Furthermore, the bureaucratic procedures are simpler for authentication products than for privacy products. An authentication product needs NSA and State Dept. approval only once, whereas an encryption product may need approval for every sale or every product revision.

Export policy is currently a matter of great controversy, as many software and hardware vendors consider current export regulations overly restrictive and burdensome. The Software Publishers Association (SPA), a software industry group, has recently been negotiating with the government in order to get export license restrictions eased; one agreement was reached that allows simplified procedures for export of two bulk encryption ciphers, RC2 and RC4 (, when the key size is limited. Also, export policy is less restrictive for foreign subsidiaries and overseas offices of U.S. companies.

In March 1992, the Computer Security and Privacy Advisory Board voted unanimously to recommend a national review of cryptography policy, including export policy. The Board is an official advisory board to NIST whose members are drawn from both the government and the private sector. The Board stated that a public debate is the only way to reach a consensus policy to best satisfy competing interests: national security and law enforcement agencies like restrictions on cryptography, especially for export, whereas other government agencies and private industry want greater freedom for using and exporting cryptography. Export policy has traditionally been decided solely by agencies concerned with national security, without much input from those who wish to encourage commerce in cryptography. U.S. export policy may undergo significant change in the next few years.

[David Aaron. (Jan. 28, 1997). International Views of Key Recovery, Statement of Ambassador David Aaron, US Envoy for Cryptography, U.S. Dept. of State NIST FOIA-110-A-R. RSA Data Security Conference. Source: https://foia.state.gov/FOIALIBRARY/SearchResults.aspx]

P-110-A
R

Statement by Ambassador David Aaron
US Envoy for Cryptography

RSA Data Security Conference, January 28, 1997

International Views of Key Recovery

The first thing that I wanted to do in preparing for this assignment was to understand the concerns of industry and the general public.

I've had the pleasure of meeting with dozens of US and foreign industry leaders and representatives -- not only those in the encryption business per se, but others in the field of electronic commerce, telecommunications, finance and other industries for which secure communications are essential. They have all impressed upon me the crucial importance of robust encryption for the future of their enterprises.

- Businesses are increasingly reliant on private networks and the Internet for their communications and operations. As proprietary information and intellectual property is transmitted over these networks, it must be protected by strong encryption.

- Business is also increasingly multinational in nature. Thus, any system of encryption must be able to operate across national borders.

- Businesses are becoming more aware of the need to recover encrypted files. Companies simply cannot risk loss of access to their valuable intellectual property because of lost passwords, accidents or, a rogue employee.

I have also had the opportunity to meet with representatives of privacy groups. They point out that every day our citizens are electronically transmitting more and more sensitive personal data, including medical, health, and financial information. Such transactions require robust security afforded by encryption.

Earlier in my career, I had the experience of working on a Congressional investigation of Government violations of Americans' right to privacy. So I well understand the concerns of privacy advocates. When Americans' fundamental rights are involved, it is understandable that the public will be extremely sensitive and cautious.

To enable encryption to be used widely for privacy protection and electronic commerce, rapid development of a support infrastructure is needed. This infrastructure must provide the policies, product, and certificate services that will allow encryption to be used, and most important, used WITH CONFIDENCE. The Administration supports this requirement, as exemplified by its initiative announced in October to promote the development of an international key management infrastructure.

The Administration envisions an infrastructure that, if developed wisely, will offer greater privacy and confidentiality than ever before. It will provide for authenticated transactions, robust confidentiality services, and key recovery features. The latter will enable users, and law enforcement under proper legal authority, the ability to regain access to encrypted data.

This approach addresses needs of the user while ensuring the public safety is not placed in jeopardy. While this has been a controversial issue, the ability to protect the rights of Americans flows from successfully fulfilling the basic public safety obligations of government.

Already the Justice Department has encountered important examples of instances where encryption has been used by terrorist and criminals. For example,

- In the Aldrich Ames spy case, Ames was instructed by his Russian handlers to encrypt computer file information to be passed to them.
- Ramzi Yosef, recently convicted of conspiring to blow up 10 US-owned airliners in the Far East, and his co-conspirators stored information about their terrorist plot in an encrypted computer file. (Yosef is on trial for his role as the mastermind of the World Trade Center bombing.)
- In a child pornography case here in California, one of the subjects used encryption in transmitting obscene and pornographic images of children over the Internet.
- In a major international drug-trafficking case, the subject of a court-ordered wiretap used a telephone encryption device, significantly impacting the investigation.
- Some anti-government militia groups are now promoting the use of encryption as a means of thwarting legitimate law enforcement investigations.
- In several major hacker cases, the subjects have encrypted computer files, to conceal evidence of serious crimes. One of these, Kevin Lee Poulsen, recently pled guilty in Los Angeles and San Jose Federal Courts for among other things, breaking into and manipulating Pacific Bell telephone computers.

I cite these examples not in the spirit of argument, but to stress that in developing its policy on encryption, the government has made a good faith effort to balance the obligations and interests involved. And I want to stress that this policy in no way seeks to expand the powers of law enforcement nor reduce the privacy protections of individuals. The intent is to maintain, in the face of technological change, the current legal instruments it has and continues to require - instruments which Congress itself has determined are necessary in the interest of public safety.

Business leaders have also made clear to me, and to the Administration, that they believe there exists now a strong international market for robust encryption, and that American industry is in a leading position to respond. But, if American firms are not allowed to meet that demand in a timely way, they are deeply concerned that our leading position in information technology across the board could be jeopardized - even in product areas not incorporating encryption. Thus, industry asked for further export policy liberalization and streamlining of the regulatory requirements.

These concerns are being heard in Washington. The Administration has taken the following steps - many based on the direct recommendations of industry representatives:

- First, at the end of last year, jurisdiction for licenses of encryption exports was transferred from the Department of State to the Department of Commerce. Commercial encryption is no longer treated as a munition and thereby subject to various foreign policy embargoes. We hope this will both speed up and simplify the tasks of obtaining licenses.
- Second, and very important, the Administration will license the export of encryption products, of any algorithm and any key length, if they incorporate key recovery.
- Third, the Administration will also permit the export, over the next two years, of 56-bit DES and equivalent encryption products without key recovery provided exporters make commitments to develop key recovery products. I am pleased to report that already at least 4 vendors have formally filed key recovery commitments and several more companies are in the initial stages of dialogue with the Department of Commerce.
- And last, a point which is often lost in the debate, domestic use of key recovery will be voluntary as announced by the Vice President last October. All Americans will remain free to use any encryption system in the United States.

However, I must be frank with you. The Administration's agreement to allow the export of DES poses risks to national security and law enforcement, but these are risks that we are willing to accept to support the development of a key management infrastructure with key recovery.

In addition to export liberalization, the Administration is also taking other steps in partnership with US industry to hasten development of key management infrastructure:

- We have initiated ten US Government pilot projects to demonstrate the practicality of key recovery as part of a key management infrastructure. One pilot which may be of interest to this audience involves the electronic filing of patent applications with the US Patent and Trademark Office, incorporating digital signature and encryption.
- The Department of Commerce has convened a technical, private sector advisory committee to develop a Federal Information Processing Standard for a Federal Key Management Infrastructure with a focus on key recovery. We are encouraged by the high degree of industry participation in this activity, which will better ensure a successful outcome.
- The Administration will use a formal mechanism to provide industry, users, state and local law enforcement, and other private sector representatives with the opportunity to advise on the future of key recovery.

- Finally, the Clinton Administration will soon propose legislation relating to the provision of commercial key recovery services, including providing penalties for improper release of keys, and liability limitations. To this end, we will be consulting fully and broadly with Congress.

As part of this overall effort the President asked me to serve as Special Envoy for Cryptography. In accepting this assignment, I have been struck that everyone involved with the encryption issue, whatever their views, recognizes that the international reaction will determine the success or failure of their particular approach. With that common starting point, I thought I would share with you the results of my consultations with foreign governments thus far.

But before doing so, I think I need to describe my role. A recent publication labeled me the Czar for cryptography. I am not a Czar. For one thing I am mindful of what happened to the real Czar. More important, I report to an interagency group at the deputy Cabinet level. They, under the Vice President, are the real policymakers.

My assignment is to explain the US Government's position on this issue to other governments and get their views. My goal is an international consensus on the development of a global key management and key recovery architecture -- one that will foster robust and dependable security for the global information infrastructure while protecting public safety and national security.

My consultations also focus on the underlying requirements in building such an international infrastructure such as cross border certification of public keys and authenticated transactions, principles of interoperability, and key recovery criteria. One of my main messages is that while governments must provide the appropriate policy framework, the task of actually building an international key management infrastructure must lie with the private sector.

So far, I have held high level meetings with the governments of France, Great Britain, Germany, Belgium and Canada as well as with the Commission of the European Union. I have also had the opportunity to meet with the representatives of other governments of the OECD in the course of negotiations on cryptography policy guidelines about which I'll say more in a minute.

From San Francisco, I will go to Australia and Japan and then return to Europe for consultations with other governments there. Subsequently, I also plan to consult with emerging market nations in Asia, Africa and South America.

So, what I have to report is not a final tally of all governments' views, but I believe it is instructive nonetheless.

- All governments appreciate the importance of encryption for the future of their economies;
- All recognize the increasing need for privacy protection due to the explosion of electronic commerce;
- All governments recognize the need for international cooperation to create a KMI and certificate services to facilitate privacy and electronic commerce;

- All support the concept of lawful access by governments and the use of trusted parties and/or key escrow as a possible mechanism;
- Many governments, in the interest of public safety, want stronger controls than we have. They have, or are considering, domestic controls on the use of encryption within their borders.
- Virtually every government has expressed unhappiness with the US decision to release 56 bit non-key recovery products even with key recovery commitments. Several have criticized the absence of internal US controls.
- They are concerned that the increased availability of such products without key recovery could undermine their ability to protect the public safety within their borders.
- Also, many suspect that our policy is driven by a desire to obtain a commercial advantage.
- Nonetheless, all are willing to cooperate with us to work out the needed international arrangements for a global key management infrastructure.

In that context, two approaches to the encryption issue appear to be emerging internationally: one is market-oriented like ours, where governments provide the appropriate policies and regulatory framework to allow for and protect the voluntary use of key recovery. The other, which is not the U.S. approach, is based on government rules and strict controls, including domestic mandatory key escrow for communications. In either case, one of my primary objectives is to ensure that any requirements and limitations imposed in other countries do not discriminate against US companies.

An important element in getting to an international consensus on encryption issues has been the development of cryptography policy guidelines at the OECD. The discussions, which began in December 1995, among the 29 member countries, have included representatives from government and business, law enforcement, security, and privacy interests.

The guidelines, now in draft, outline basic principles for cryptography policy. They cover the issues of trust, choice, market-driven development and standards of cryptographic methods, as well as protection of privacy and personal data, lawful access, liability and international cooperation. As many of you know, we have included as many US business representatives as possible on the US delegation to the OECD meetings on encryption.

Though these guidelines are broad in nature and non-binding, our goal is their adoption and application by governments, businesses and individuals in safeguarding electronic transactions, communications and data storage. We expect final approval by governments in the Spring.

CONCLUSION

In conclusion, I want to underscore that every government I have consulted wants to protect the privacy of its citizens while also preserving lawful access to encrypted materials for public safety purposes. During the negotiation of the OECD Guidelines, delegates were specifically asked if their governments' wished to give up or reject their sovereign rights to lawful access. None did - not even the most ardent advocates of free choice, privacy and unfettered commerce.

So from what I can see at this point in my mission, the international encryption market will not be a wide open affair. As you in the encryption industry plan for the future, I would encourage you to take into account the likelihood that lawful access and key recovery will be a growing international requirement.

Many companies, including many represented in this audience, have announced efforts to search for key recovery solutions for their customers, and have provided useful ideas and feedback to the Administration. We are grateful to them and eager to hear more of your ideas and suggestions. I ask the rest of you to consider joining our efforts to develop the framework for an international key management infrastructure that will provide for robust encryption and key recovery for all users.

I believe the result of our cooperation can be a level of privacy and confidentiality never before available to both individuals and business. It can provide the security necessary to make electronic commerce and digital communications powerful engines of economic growth, improving the lives of us all.

And as I go forward in my assignment, I want you to know that I am committed to support the leadership role of American industry in the highly competitive international arena of information technology. I am eager to work with you and your representatives, and I look forward to seeing you all again.