

HEINONLINE

Citation: 2 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 i 2002

Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Sat Apr 20 11:22:17 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at <http://heinonline.org/HOL/License>

-- The search text of this PDF is generated from
uncorrected OCR text.

**SECURITY AND FREEDOM THROUGH ENCRYPTION
(SAFE) ACT**

HEARING
BEFORE THE
SUBCOMMITTEE ON COURTS AND INTELLECTUAL
PROPERTY
OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
FIRST SESSION
ON
H.R. 850

MARCH 4, 1999

Serial No. 34



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

62-507

WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

ISBN 0-16-060600-4

COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, Jr.,
Wisconsin

BILL McCOLLUM, Florida

GEORGE W. GEKAS, Pennsylvania

HOWARD COBLE, North Carolina

LAMAR S. SMITH, Texas

ELTON GALLEGLY, California

CHARLES T. CANADY, Florida

BOB GOODLATTE, Virginia

STEPHEN E. BUYER, Indiana

ED BRYANT, Tennessee

STEVE CHABOT, Ohio

BOB BARR, Georgia

WILLIAM L. JENKINS, Tennessee

ASA HUTCHINSON, Arkansas

EDWARD A. PEASE, Indiana

CHRIS CANNON, Utah

JAMES E. ROGAN, California

LINDSEY O. GRAHAM, South Carolina

MARY BONO, California

SPENCER BACHUS, Alabama

JOHN CONYERS, JR., Michigan

BARNEY FRANK, Massachusetts

HOWARD L. BERMAN, California

RICK BOUCHER, Virginia

JERROLD NADLER, New York

ROBERT C. SCOTT, Virginia

MELVIN L. WATT, North Carolina

ZOE LOFGREN, California

SHEILA JACKSON LEE, Texas

MAXINE WATERS, California

MARTIN T. MEEHAN, Massachusetts

WILLIAM D. DELAHUNT, Massachusetts

ROBERT WEXLER, Florida

STEVEN R. ROTHMAN, New Jersey

TAMMY BALDWIN, Wisconsin

ANTHONY D. WEINER, New York

THOMAS E. MOONEY, SR., *General Counsel-Chief of Staff*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

F. JAMES SENSENBRENNER, JR.,
Wisconsin

ELTON GALLEGLY, California

BOB GOODLATTE, Virginia

WILLIAM L. JENKINS, Tennessee

EDWARD A. PEASE, Indiana

CHRIS CANNON, Utah

JAMES E. ROGAN, California

MARY BONO, California

HOWARD L. BERMAN, California

JOHN CONYERS, JR., Michigan

RICK BOUCHER, Virginia

ZOE LOFGREN, California

WILLIAM D. DELAHUNT, Massachusetts

ROBERT WEXLER, Florida

MITCH GLAZIER, *Chief Counsel*
BLAINE MERRITT, *Counsel*
VINCE GARLOCK, *Counsel*
DEBBIE K. LAMAN, *Counsel*
ROBERT RABEN, *Minority Counsel*
EUNICE GOLDRING, *Staff Assistant*

CONTENTS

HEARING DATE

March 4, 1999	Page 1
---------------------	-----------

TEXT OF BILL

H.R. 850	1
----------------	---

OPENING STATEMENT

Coble, Hon. Howard, a Representative in Congress from the State of North Carolina, and chairman, Subcommittee on Courts and Intellectual Property	1
---	---

WITNESSES

Davidson, Alan, Staff Counsel, Center for Democracy and Technology	94
Denning, Dorothy E., Professor, Computer Science Department, Georgetown University	91
Gillespie, Ed, Executive Director, Americans for Computer Privacy	131
Lee, Ronald D., Associate Deputy Attorney General, U.S. Department of Justice	47
McLaughlin, Craig, Chief Technology Officer, Privada	80
McNamara, Barbara, Deputy Director, National Security Agency	43
Norquist, Grover, President, Americans for Tax Reform	86
Parenty, Thomas, Director, Data & Communications Security, Sybase, Inc.	71
Reinsch, William A., Under Secretary of Commerce for Export Administration, U.S. Department of Commerce	37

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Coble, Hon. Howard, a Representative in Congress from the State of North Carolina, and chairman, Subcommittee on Courts and Intellectual Property: Prepared statement	7
Collingwood, John E., Assistant Director, Office of Public and Congressional Affairs, U.S. Department of Justice: Letter to Hon. Howard Coble dated March 3, 1999	19
Conyers, Hon. John, Jr., a Representative in Congress from the State of Michigan: Prepared statement	18
Davidson, Alan, Staff Counsel, Center for Democracy and Technology: Prepared statement	96
Denning, Dorothy E., Professor, Computer Science Department, Georgetown University: Prepared statement	93
Gillespie, Ed, Executive Director, Americans for Computer Privacy: Prepared statement	132
Goodlatte, Hon. Bob, a Representative in Congress from the State of Virginia: Prepared statement	11
Lee, Ronald D., Associate Deputy Attorney General, U.S. Department of Justice: Prepared statement	49
Lofgren, Hon. Zoe, a Representative in Congress from the State of California: Prepared statement	16
McCurdy, Dave, President, Electronic Industries Alliance: Prepared statement	137
McLaughlin, Craig, Chief Technology Officer, Privada: Prepared statement	82
McNamara, Barbara, Deputy Director, National Security Agency: Prepared statement	45

IV

	Page
McNamara, Barbara, Deputy Director, National Security Agency—Continued	
Letter to Hon. Zoe Lofgren dated July 30, 1999	68
Norquist, Grover, President, Americans for Tax Reform: Prepared statement ..	88
Parenty, Thomas, Director, Data & Communications Security, Sybase, Inc.:	
Prepared statement	73
Reinsch, William A., Under Secretary of Commerce for Export Administration, U.S. Department of Commerce: Prepared statement	40
U.S. Department of Justice, Office of Legislative Affairs: Letters to Hon. Zoe Lofgren dated April 14, 1999 and May 21, 1999	59

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

THURSDAY, MARCH 4, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS AND
INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 2226, Rayburn House Office Building, Hon. Howard Coble [chairman of the subcommittee] presiding.

Present: Representatives Howard Coble, F. James Sensenbrenner, Jr., Bob Goodlatte, Edward A. Pease, James E. Rogan, Mary Bono, Howard L. Berman, John Conyers, Jr., Zoe Lofgren and William D. Delahunt.

Staff present: Mitch Glazier, Chief Counsel; Vince Garlock, Counsel; Joseph Gibson, Chief Antitrust Counsel; Eunice Goldring, Staff Assistant; and Bari Schwartz, Minority Counsel.

OPENING STATEMENT OF CHAIRMAN COBLE

Mr. COBLE. Good morning, ladies and gentlemen. The subcommittee will come to order. The subcommittee will hear testimony on H.R. 850, the Security and Freedom through Encryption Act, sometimes popularly referred to as the SAFE Act.

[The bill, H.R. 850, follows:]

106TH CONGRESS
1ST SESSION

H. R. 850

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 25, 1999

Mr. GOODLATTE (for himself, Ms. LOFGREN, Mr. ARMEY, Mr. DELAY, Mr. WATTS of Oklahoma, Mr. DAVIS of Virginia, Mr. COX, Ms. PRYCE of Ohio, Mr. BLUNT, Mr. GEPHARDT, Mr. BONIOR, Mr. FROST, Ms. DELAURO, Mr. LEWIS of Georgia, Mr. GEJDENSON, Mr. SENSENBRENNER, Mr. GEKAS, Mr. COBLE, Mr. SMITH of Texas, Mr. GALLEGLY, Mr. BRYANT, Mr. CHABOT, Mr. BARR of Georgia, Mr. HUTCHINSON, Mr. PEASE, Mr. CANNON, Mr. ROGAN, Mrs. BONO, Mr. BACHUS, Mr. CONYERS, Mr. FRANK of Massachusetts, Mr. BOUCHER, Mr. NADLER, Ms. JACKSON-LEE of Texas, Ms. WATERS, Mr. MEEHAN, Mr. DELAHUNT, Mr. WEXLER, Mr. ACKERMAN, Mr. ANDREWS, Mr. ARCHER, Mr. BALLENGER, Mr. BARCIA, Mr. BARRETT of Nebraska, Mr. BARRETT of Wisconsin, Mr. BARTON of Texas, Mr. BILBRAY, Mr. BLUMENAUER, Mr. BOEHNER, Mr. BRADY of Texas, Mr. BRADY of Pennsylvania, Ms. BROWN of Florida, Mr. BROWN of California, Mr. BURR of North Carolina, Mr. BURTON of Indi-

(1)

ana, Mr. CAMP, Mr. CAMPBELL, Mrs. CAPPS, Mr. CHAMBLISS, Mrs. CHENOWETH, Mrs. CHRISTIAN-CHRISTENSEN, Mrs. CLAYTON, Mr. CLEMENT, Mr. CLYBURN, Mr. COLLINS, Mr. COOK, Mr. COOKSEY, Mrs. CUBIN, Mr. CUMMINGS, Mr. CUNNINGHAM, Mr. DAVIS of Illinois, Mr. DEAL of Georgia, Mr. DEFAZIO, Mr. DEUTSCH, Mr. DICKEY, Mr. DOOLEY of California, Mr. DOOLITTLE, Mr. DOYLE, Mr. DREIER, Mr. DUNCAN, Ms. DUNN, Mr. EHLERS, Mrs. EMERSON, Mr. ENGLISH, Ms. ESHOO, Mr. EWING, Mr. FARR of California, Mr. FILNER, Mr. FORD, Mr. FOSSELLA, Mr. FRANKS of New Jersey, Mr. GILLMOR, Mr. GOODE, Mr. GOODLING, Mr. GORDON, Mr. GREEN of Texas, Mr. GUTKNECHT, Mr. HALL of Texas, Mr. HASTINGS of Washington, Mr. HERGER, Mr. HILL of Montana, Mr. HOBSON, Mr. HOEKSTRA, Mr. HOLDEN, Ms. HOOLEY of Oregon, Mr. HORN, Mr. HOUGHTON, Mr. INSLEE, Mr. ISTOOK, Mr. JACKSON of Illinois, Mr. JEFFERSON, Ms. EDDIE BERNICE JOHNSON of Texas, Mrs. JOHNSON of Connecticut, Mr. KANJORSKI, Mr. KASICH, Mrs. KELLY, Ms. KIKPATRICK, Mr. KIND, Mr. KINGSTON, Mr. KNOLLENBERG, Mr. KOLBE, Mr. LAMPSON, Mr. LARGENT, Mr. LATHAM, Ms. LEE, Mr. LEWIS of Kentucky, Mr. LINDER, Mr. LUCAS of Oklahoma, Mr. LUTHER, Ms. MCCARTHY of Missouri, Mr. MCDERMOTT, Mr. MCGOVERN, Mr. MCINTOSH, Mr. MALONEY of Connecticut, Mr. MANZULLO, Mr. MARKEY, Mr. MARTINEZ, Mr. MATSUI, Mrs. MEEK of Florida, Mr. METCALF, Mr. MICA, Ms. MILLENDER-MCDONALD, Mr. GEORGE MILLER of California, Mr. MOAKLEY, Mr. MORAN of Virginia, Mrs. MORELLA, Mrs. MYRICK, Mrs. NAPOLITANO, Mr. NEAL of Massachusetts, Mr. NETHERCUTT, Mr. NORWOOD, Mr. NUSSLE, Mr. OLVER, Mr. PACKARD, Mr. PALLONE, Mr. PASTOR, Mr. PETERSON of Minnesota, Mr. PICKERING, Mr. POMBO, Mr. POMEROY, Mr. PRICE of North Carolina, Mr. QUINN, Mr. RADANOVICH, Mr. RAHALL, Mr. RANGEL, Mr. REYNOLDS, Ms. RIVERS, Mr. ROHRBACHER, Ms. ROS-LEHTINEN, Mr. RUSH, Mr. SALMON, Ms. SANCHEZ, Mr. SANDERS, Mr. SANFORD, Mr. SCARBOROUGH, Mr. SCHAFFER, Mr. SESSIONS, Mr. SHAYS, Mr. SHERMAN, Mr. SHIMKUS, Mr. SMITH of Washington, Mr. SMITH of New Jersey, Mr. SOUDER, Ms. STABENOW, Mr. STARK, Mr. SUNUNU, Mr. TANNER, Mrs. TAUSCHER, Mr. TAUZIN, Mr. TAYLOR of North Carolina, Mr. THOMAS, Mr. THOMPSON of Mississippi, Mr. THUNE, Mr. TIAHRT, Mr. TIERNEY, Mr. UPTON, Mr. VENTO, Mr. WALSH, Mr. WAMP, Mr. WATKINS, Mr. WELLER, Mr. WHITFIELD, Mr. WICKER, Ms. WOOLSEY, and Mr. WU) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Security And Freedom through Encryption (SAFE) Act".

SEC. 2. SALE AND USE OF ENCRYPTION.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 123 the following new chapter:

"CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

"2801. Definitions.

"2802. Freedom to use encryption.

"2803. Freedom to sell encryption.

"2804. Prohibition on mandatory key escrow.

"2805. Unlawful use of encryption in furtherance of a criminal act.

"§ 2801. Definitions

"As used in this chapter—

"(1) the terms 'person', 'State', 'wire communication', 'electronic communication', 'investigative or law enforcement officer', and 'judge of competent jurisdiction' have the meanings given those terms in section 2510 of this title;

"(2) the term 'decrypt' means to retransform or unscramble encrypted data, including communications, to its readable form;

“(3) the terms ‘encrypt’, ‘encrypted’, and ‘encryption’ mean the scrambling of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information;

“(4) the term ‘key’ means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire communications, electronic communications, or electronically stored information, that has been encrypted; and

“(5) the term ‘key recovery information’ means information that would enable obtaining the key of a user of encryption;

“(6) the term ‘plaintext access capability’ means any method or mechanism which would provide information in readable form prior to its being encrypted or after it has been decrypted;

“(7) the term ‘United States person’ means—

“(A) any United States citizen;

“(B) any other person organized under the laws of any State, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

“(C) any person organized under the laws of any foreign country who is owned or controlled by individuals or persons described in subparagraphs (A) and (B).

“§2802. Freedom to use encryption

“Subject to section 2805, it shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

“§2803. Freedom to sell encryption

“Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

“§2804. Prohibition on mandatory key escrow

“(a) GENERAL PROHIBITION.—Neither the Federal Government nor a State may require that, or condition any approval on a requirement that, a key, access to a key, key recovery information, or any other plaintext access capability be—

“(1) built into computer hardware or software for any purpose;

“(2) given to any other person, including a Federal Government agency or an entity in the private sector that may be certified or approved by the Federal Government or a State to receive it; or

“(3) retained by the owner or user of an encryption key or any other person, other than for encryption products for use by the Federal Government or a State.

“(b) PROHIBITION ON LINKAGE OF DIFFERENT USES OF ENCRYPTION.—Neither the Federal Government nor a State may—

“(1) require the use of encryption products, standards, or services used for confidentiality purposes, as a condition of the use of such products, standards, or services for authenticity or integrity purposes; or

“(2) require the use of encryption products, standards, or services used for authenticity or integrity purposes, as a condition of the use of such products, standards, or services for confidentiality purposes.

“(c) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall not affect the authority of any investigative or law enforcement officer, or any member of the intelligence community as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a), acting under any law in effect on the effective date of this chapter, to gain access to encrypted communications or information.

“§2805. Unlawful use of encryption in furtherance of a criminal act

“(a) ENCRYPTION OF INCRIMINATING COMMUNICATIONS OR INFORMATION UNLAWFUL.—Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution—

"(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and

"(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.

"(b) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant."

(b) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 123 the following new item:

"125. Encrypted wire and electronic information

2801".

SEC. 3. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979.—Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection:

"(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

"(1) GENERAL RULE.—Subject to paragraphs (2) and (3), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

"(2) ITEMS NOT REQUIRING LICENSES.—After a one-time, 15-day technical review by the Secretary, no export license may be required, except pursuant to the Trading with the enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

"(A) any computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

"(i) that is generally available;

"(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

"(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which—

"(I) includes encryption capabilities which are inaccessible to the end user; and

"(II) is not designed for military or intelligence end use;

"(B) any computing device solely because it incorporates or employs in any form—

"(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

"(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

"(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

"(D) any computing or telecommunication device which incorporates or employs in any form computer hardware or software encryption capabilities which—

"(i) are not directly available to the end user; or

"(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

“(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

“(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

“(3) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a one-time, 15-day technical review by the Secretary, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for non-military end uses in any country—

“(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such computer hardware or software or computing devices will be—

“(i) diverted to a military end use or an end use supporting international terrorism;

“(ii) modified for military or terrorist end use; or

“(iii) reexported without any authorization by the United States that may be required under this Act; or

“(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

“(4) DEFINITIONS.—As used in this subsection—

“(A)(i) the term ‘encryption’ means the scrambling of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information;

“(ii) the terms ‘wire communication’ and ‘electronic communication’ have the meanings given those terms in section 2510 of title 18, United States Code;

“(B) the term ‘generally available’ means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

“(i) computer hardware or computer software that is—

“(I) distributed through the Internet;

“(II) offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

“(III) preloaded on computer hardware or computing devices that are widely available for sale to the public; or

“(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

“(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

“(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

“(II) select from among options contained in the computer hardware or computer software; and

“(iii) with respect to which the manufacturer of that computer hardware or computer software—

“(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has supplied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

“(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer;

"(C) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data;

"(D) the term 'computer hardware' includes, but is not limited to, computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, and printed circuit board assemblies;

"(E) the term 'customer premises equipment' means equipment employed on the premises of a person to originate, route, or terminate communications;

"(F) the term 'technical assistance' includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

"(G) the term 'technical data' includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

"(H) the term 'technical review' means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented."

(b) **NO REINSTATEMENT OF EXPORT CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.**—Any encryption product not requiring an export license as of the date of enactment of this Act, as a result of administrative decision or rulemaking, shall not require an export license on or after such date of enactment.

(c) **APPLICABILITY OF CERTAIN EXPORT CONTROLS.**—

(1) **IN GENERAL.**—Nothing in this Act shall limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act of 1979, to—

(A) prohibit the export of encryption products to countries that have been determined to repeatedly provide support for acts of international terrorism; or

(B) impose an embargo on exports to, and imports from, a specific country.

(2) **SPECIFIC DENIALS.**—The Secretary may prohibit the export of specific encryption products to an individual or organization in a specific foreign country identified by the Secretary, if the Secretary determines that there is substantial evidence that such encryption products will be used for military or terrorist end-use.

(3) **DEFINITION.**—As used in this subsection and subsection (b), the term "encryption" has the meaning given that term in section 17(g)(5)(A) of the Export Administration Act of 1979, as added by subsection (a) of this section.

(d) **CONTINUATION OF EXPORT ADMINISTRATION ACT.**—For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

SEC. 4. EFFECT ON LAW ENFORCEMENT ACTIVITIES.

(a) **COLLECTION OF INFORMATION BY ATTORNEY GENERAL.**—The Attorney General shall compile, and maintain in classified form, data on the instances in which encryption (as defined in section 2801 of title 18, United States Code) has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States.

(b) **AVAILABILITY OF INFORMATION TO THE CONGRESS.**—The information compiled under subsection (a), including an unclassified summary thereof, shall be made available, upon request, to any Member of Congress.



Mr. COBLE. As you all know, encryption is the process of encoding data or communication in a form that only the intended recipient can understand. Once the exclusive domain of the national security agencies, encryption has become increasingly important to persons and companies in the private sector concerned with the security of the information they transmit. H.R. 850 seeks to provide a means of ensuring protection for confidential communications

transmitted in this information age. It also seeks to lift restrictions on the exportation of advanced encryption so U.S. information companies will remain the world leader.

This matter has consumed abundant time and energy on this subcommittee as well as the full Judiciary Committee, over the last few years, and it is time that it becomes law.

While I am ever mindful of the concerns of law enforcement and national security agencies, I believe the reforms contained in H.R. 850 are critical to ensure that the United States will continue as the leader in information technologies as well as guaranteeing protection from intrusions to free speech as new information technology develops.

I once again want to publicly acknowledge the contribution of the gentleman from Virginia, Mr. Goodlatte, for his work in this area and introducing this very important piece of legislation, which I support. I might mention that this bipartisan bill currently has over 200 cosponsors, including both Republicans and Democratic leadership.

I see the gentlelady from California has just come in. I refer to Zoe Lofgren and Bob Goodlatte as the two leading gurus on this subject. Howard, you may be one as well.

Mr. BERMAN. No, no.

Mr. COBLE. But Zoe and Bob have been the lead dogs on them. I commend each of them.

[The prepared statement of Mr. Coble follows:]

PREPARED STATEMENT OF HON. HOWARD COBLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA, AND CHAIRMAN, SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

The Subcommittee will come to order.

Today the Subcommittee will hear testimony on H.R. 850, the "Security and Freedom Through Encryption (SAFE) Act." As all of you well know, encryption is the process of encoding data or communications in a form that only the intended recipient can understand. Once the exclusive domain of the national security agencies, encryption has become increasingly important to persons and companies in the private sector concerned with the security of the information they transmit. H.R. 850 seeks to provide a means of ensuring protection for confidential communications transmitted in this information age. It also seeks to lift restrictions on the exportation of advanced encryption so U.S. information companies will remain the world leader.

This matter has consumed abundant time and energy of this Subcommittee and the Full Committee over the last few years, and it is time make sure it becomes law. While I am ever mindful of the concerns of law enforcement and national security agencies, I believe the reforms contained in H.R. 850 are critical to ensure that the United States will continue as the leader in information technologies, as well as guaranteeing protection from intrusions to free speech as new information technology develops.

I once again commend the gentleman from Virginia, Mr. Goodlatte, for his work in this area and for introducing this very important piece of legislation which I support. I might mention that this bipartisan bill currently has over 200 cosponsors including both Republicans and Democratic Leadership. I would like to ask the Ranking Member, Mr. Berman, to make an opening statement and will then ask Mr. Goodlatte to further explain his bill.

Mr. COBLE. I would now like to recognize the Ranking Member, the gentleman from California, to make his opening statement.

Mr. BERMAN. Thank you very much, Mr. Chairman. They are very good dogs indeed.

I congratulate you on having this hearing and for your decision to get to the issues underlying this legislation very quickly in the

beginning of this Congress. The issues surrounding encryption are very complex, and it remains one of the most serious and complicated issues that our subcommittee will address this year, and I want to join you in commending both Mr. Goodlatte and Ms. Lofgren for their leadership in considering these problems and in developing their legislation.

I have discussed the issue not this year, but in past years with the Administration officials and with supporters of the bill, and everyone agrees that effective encryption of electronic communication is absolutely necessary. None of us want our personal information susceptible to interception, and to the extent the current policy restricts the ability of U.S. industry to maintain its leadership position in the international marketplace, this is another reason to have our current policies re-examined.

And at the same time we do want reasonable means to meet the vital needs of law enforcement, and I—it is only fair to say while I supported this bill last year and hope to support it again, I do have some concern that the availability of stronger encryption products freely and without limit might have the ability to impede some of our legitimate efforts to safeguard national security from terrorists, rogue nations, countries developing weapons of mass destruction, and effective National Security Agency ability to intercept legally certain types of foreign communications essential to the security of the United States.

Clearly the ability of strong encryption products will to some extent impair NSA's ability to intercept foreign communications. Some would argue such capability has already been seriously weakened by the wide availability of strong encryption products on the Internet and from other more permissive countries. One of the witnesses on the first panel here, Secretary Reinsch, I remember going around with him back in the early 1980's on this whole issue of foreign availability. When you are dealing with national security control, and that is what we are talking about really here, not foreign policy controls, full foreign availability of the same quality product sort of eliminates the logic of export control. And I think Mr. Goodlatte points that out frequently as well. So this is an important issue established for the record.

Simply because something is available on the Net or is available from other sources doesn't automatically mean that the Government should reject all efforts to constrain trade in items that might have an effect on national security. These circumstances would not alter our responsibility to recognize and support the appropriate legitimate needs of the National Security Agency and the needs of the United States and national security law enforcement areas. The question that remains, however, is availability so extensive and so similar in quality that it renders export controls worthless in preserving national security and law enforcement interests. If that is the case, then we probably in all fairness ought to just come to terms with it, admit it, move on and have our policies reflect that reality.

U.S. policy has matured in the several years that we have been considering this issue. The Administration has made substantial changes in their policy, and I appreciate their efforts to find a balance between the need for national security and the need to pro-

mote privacy and security for individuals in business and electronic commerce. As I understand it, the Administration now opposes H.R. 850, and the Administration, although not supporting a broad mandatory key recovery system any longer, believes that H.R. 850 might impede the development of a voluntary key recovery system and opposes the statutory prohibitions with regard to controls on domestic use and sales in H.R. 850.

The Administration is concerned that immediate encryption de-control will deprive the NSA of the opportunity to review encryption products prior to their export. Another concern is H.R. 850's decontrolling extends to all destinations, even regions of political instability, and the NSA observes that H.R. 850 would preclude the U.S. Government from an opportunity to conduct a meaningful review of a proposed export to assure that it is compatible with national security interests.

Finally, the Administration has pointed out that Wassenaar nations agreed unanimously in December 1998 to control strong encryption products reflecting an agreement that export control is appropriate. I hope that there is a way to bridge the differences that remain regarding the honest concerns raised by each of the sides of this debate, and I hope we will be able to take what we learn in implementing the current Administration's policy and work to responsibly resolve their remaining issues in a manner satisfactory to everyone. Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Berman.

Traditionally we restrict opening statements to the subcommittee chairman and the subcommittee Ranking Member, but in view of the extensive work that Mr. Goodlatte and Ms. Lofgren have done on this bill, and we also have the Ranking Member of the full committee here, I am going to depart from tradition and recognize Mr. Goodlatte for an opening statement.

Mr. GOODLATTE. Thank you, Mr. Chairman. First let me thank you for your support for this legislation and for holding this hearing on what I view as a very, very important issue. Two years ago I held the committee and the panelists and the audience in rapt attention for a full 10 minutes while I read my opening statement, and today I will ask that it just be submitted for the record and comment on a few things.

Mr. COBLE. Without objection, that will be done.

Mr. GOODLATTE. I would hope there would be no objection.

First of all, I would like to note the significant progress we have made in building support for this. When we introduced this legislation 2 years ago, we had 55 original cosponsors. When we introduced it last Thursday, we had 205 original cosponsors and a very bipartisan alignment of support. I am especially grateful to my colleague, Ms. Lofgren, for the outstanding work she has done these several years with me as we push this legislation forward and in the work to line up cosponsors. We have 114 Republicans and 91 Democrats. We almost have a contest here between who can raise—

Ms. LOFGREN. I was sick for a week.

Mr. GOODLATTE. We have the Majority Leader Mr. Armey, the Minority Leader Mr. Gephardt, Majority Whip Mr. Delay, Minority Whip Mr. Bonior, the Conference chairmen on both sides of the

aisle, and a great many other very respected Members of Congress, and I am hopeful that we will be able to move this legislation to the floor this year.

It is vitally important because, quite frankly, when legislators attempt to deal with something that involves technology of this nature, we tend to fall behind the curve, and that is exactly what is happening both in the Congress and in the Administration. While there have been some steps taken by the Administration, which I applaud, to move our policy toward a more enlightened direction, the technology itself and the industrywide standard has moved forward at a much more dramatic pace. When we introduced this legislation a few years ago, the industry standard was 56 bits, and the Administration was holding on to 40 bits. Today in most areas, although they have moved further ahead in some, the Administration is at 56 bits, but the international industry standard is 128 bits. That is not just a little more than double 56 bits. That is trillions of times more powerful than 56 bits because we are talking about 2 to the 128th power.

This is vitally needed because of the security that is needed on the Internet and in wireless communications, and it is vitally needed to protect and create American jobs because this is something that can be done anywhere in the world. We are not talking about something that is very suitable for export controls, such as jets or bombs or even mainframe computers under certain circumstances, because those are manufactured in a few places, going to a few places and our border can be an effective choke point for them. We are talking about little ones and zeros going through millions of wires all across the world, going wireless through the air.

There are, I suspect, millions of American citizens who violate our export control laws every single day because of the fact that they have loaded encryption onto their computers, and when they send a message overseas to somebody or share some software with somebody overseas, they inadvertently violate our export control laws if that piece of software has more than the Administration standard for encryption.

While I was in Europe recently, I found that the situation there is changing dramatically. The French Government, which has been cited by our Government many times as being a leader in strong controls on encryption, has taken a complete about-face. They are going to pass legislation shortly that will not include domestic key recovery. It will set a domestic standard of 128 bits, and with regard to exports, there is no doubt in my mind that they are moving in that direction, as they are all across Europe, to challenge an industry that we dominate today with software products that contain strong encryption and will continue, as they have been in the past, to use our export controls as a lever against our industry when they compete for customers.

In Belgium, the Deputy Chief of Mission there told me a personal story that had changed his point of view regarding this. He said that he works with the FBI and with national security on these issues, and he shares their concern, as I share their concern, regarding the need to be able to handle encryption in some fashion. But he said when he purchased a \$1500 PC from the United States and had it shipped to him in Belgium, and then was told by the

manufacturer that they couldn't send the software because it violated American export control laws, and he went down the street to a shop in Brussels and bought that software from European vendors, he got a little enlightenment about how behind the times we are in terms of trying to control this.

I have serious doubts whether tens of thousands of different pieces of software sold to tens of millions of customers potentially involving—if we were to follow the route of the FBI—tens of billions, if not trillions of keys will ever be a workable system that any administrative body can keep up with in this highly competitive environment. And for those reasons, I would urge the committee to pass this legislation when we have an opportunity to mark it up. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF VIRGINIA

Mr. Chairman, I would like to thank you for holding today's important hearing on legislation I have introduced H.R. 850, the Security And Freedom through Encryption (SAFE) Act of 1999 to encourage the use of strong encryption.

This much-needed, bipartisan legislation, which has 205 original cosponsors, including a majority of the Republican and Democratic leadership, a majority of the members of the Judiciary Committee, and all but two members of this Subcommittee, accomplishes several important goals. First, it aids law enforcement by preventing piracy and white-collar crime on the Internet. Several studies over the past few years have demonstrated that the theft of proprietary business information costs American industry hundreds of billions of dollars each year. The use of strong encryption to protect financial transactions and information would prevent this theft from occurring. With the speed of transactions and communications on the Internet, law enforcement cannot stop thieves and criminal hackers by waiting to react until after the fact.

Only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment. As the National Research Council's Committee on National Cryptography Policy concluded, "If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States."

Second, if the Global Information Infrastructure is to reach its true potential, citizens and companies alike must have the confidence that their communications and transactions will be secure. The SAFE Act, by allowing all Americans to use the highest technology and strongest security available, will provide them with that confidence.

Third, with the availability of strong encryption overseas and on the Internet, our export controls only serve to tie the hands of American business. Due in large part to these export controls, foreign companies are winning an increasing number of contracts by telling prospective clients that American encryption products are weak and inferior, which is robbing our economy of jobs and revenue. In fact, one noted study found that failure to address the current export restrictions by the year 2000 will cost American industry \$60 billion and 200,000 jobs. Under the current system, America is surrendering our dominance of the global marketplace.

The SAFE Act remedies this situation by allowing the export of generally available American-made encryption products after a 15-day, one-time technical review. Additionally, the bill allows custom-designed encryption products to be exported, after the same review period, if they are commercially available overseas and will not be used for military or terrorist purposes.

Removing these export barriers will free U.S. industry to remain the leader in software, hardware, and Internet development. And by allowing our computer industry to market the highest technology with the strongest security features available, America will lead the way into the 21st century Information Age.

This bipartisan legislation enjoys the support of members and organizations across the entire spectrum of ideological and political beliefs. The SAFE Act enjoys this support not only because it is a common-sense approach to solving a serious problem, but also because ordinary Americans' privacy and security is being assaulted by this Administration.

Amazingly enough, the Administration wants to mandate a back door into peoples' computer systems in order to access their private communications. In fact, the Administration has stated that if people do not "voluntarily" create this back door, it may seek legislation forcing them to give the Government access to their information, by mandating a "key recovery" system requiring people to give the keys to decode their communications to a Government-approved third party. This is the technological equivalent of mandating that the Government be given a key to every home in America.

The Administration is proposing an Industrial Age solution to an Information Age problem. The SAFE Act, on the other hand, prevents the Administration from placing roadblocks on the information superhighway by prohibiting the Government from mandating a back door into the computer systems of private citizens and businesses. Additionally, the SAFE Act ensures that all Americans have the right to choose any security system to protect their confidential information.

With the millions of communications, transmissions, and transactions that occur on the Internet every day, American citizens and businesses must have the confidence that their private information and communications are safe and secure. That is precisely what the SAFE Act will ensure. I urge each of my colleagues to support this bipartisan legislation, and I look forward to hearing from the witnesses who will testify before us today.

"As more and more businesses conduct e-commerce on the Web, conversations need to be held about balancing privacy and security. We have woken up a conversation on these two issues, which needed to happen," Alfis said.

But even those who have worked closely with Intel in the past agree that the company has badly damaged itself.

"I think they would have done better had they laid out a white paper," said **Jim Bidzos**, president of RSA Data Security. Their intent was to facilitate secure content delivery, but they ended up creating a fear of Big Brother stamping everyone with the mark of the beast."



- by Drew Clark

Encryption

Relaxing in Europe

European Union officials are examining whether to relax controls on the export of encryption products within the borders of its member states, an EU official said.

While discussions are in the early stages, officials are considering some liberalization of policies on dual-use products, those that have both military and commercial value, according to **Gerard de Graaf**, first secretary to the European Union's Washington delegation. A proposal could be made before the summer, he said.

"The EU has always taken a liberal approach on encryption," de Graaf told *National Journal's Technology Daily*. "We feel in many instances, restrictions are not always the best way of protecting national security."

The Clinton Administration is concerned that increasing the availability of encryption technology, which scrambles data or communications for privacy, will lead to its broader use, hampering law enforcement and intelligence gathering.

A significant liberalization in EU encryption rules could undermine U.S. efforts to create an international regime in the more restrictive U.S. mold. It would bolster industry's argument that the United States cannot control the spread of robust encryption, and that controls on the export of U.S. products will only lead to a loss in market share for American companies.

"To the extent that they lessen restrictions on exports and adopt standards that were seeking to adopt here in the U.S. that would be helpful," said Rep. **Rick Boucher** D-VA, co-chairman of the Congressional Internet Caucus. He introduced H.R. 850 last week with Rep. **Bob Goodlatte** R-VA, legislation to ease U.S. controls on encryption exports.

The European Union has resisted U.S. efforts to gain international support for key-recovery, de Graaf said. He noted that an announcement earlier this year by France that it plans to ease controls on encryption within that country brings the French more in line with the rest of Europe.

One notable exception is Great Britain, which has floated a proposal for establishment of a voluntary third-party key escrow system. The proposal calls for licensing key-escrow agents who would hold a "key" needed to unscramble encrypted data or communications.



- by Juliana Gruenwald

Trade

Quote of the Day

"Their intent was to facilitate secure content delivery, but they ended up creating a fear of Big Brother stamping everyone with the mark of the beast."

— RSA Data Security President **Jim Bidzos** on Intel

On The Right Track?

Microsoft Chairman **Bill Gates'** call for the renewal of presidential fast track negotiating authority is unlikely to provide the necessary spark to jump start debate over legislation that has been killed twice in the last two years.

Gates issued a vocal appeal for Congress to pass legislation to renew fast track authority for trade pact negotiation during a speech in before the Washington [State] Council on International Trade in Seattle Friday. Gates said e-commerce would not reach its full potential unless "there are new trade agreements that eliminate the prospect of tariffs on electronic transfers and guarantee free market access for e-commerce providers."

"The significance of these issues makes it important that the president have fast track negotiating authority," said Gates, co-chairman of the host committee for the World Trade Organization's ministerial meeting in Seattle, which starts Nov. 30. Gates is hoping fast track will be reinstated before the WTO meeting begins.

Fast track, which expired in 1994, allows the president to submit trade deals to Congress for an up-or-down vote within 90 days. Lawmakers are not allowed to offer amendments. Without fast track, other countries are reluctant to negotiate new trade agreements because of concerns that Congress could alter the pacts, supporters say. But efforts to reinstate fast track in the last two years have been defeated, first by an organized labor drive in 1997, and then by Democrats, including the administration, who saw a Republican revival of the bill last year as an attempt to divide Democrats prior to the congressional elections.

But despite Gates' push for renewal of fast track, many supporters are still skeptical about its chances in the 106th Congress.

"I just think too many other factors are going against it," said **B. Timothy Bennett**, senior vice president for international issues at the American Electronics Association. In particular, he noted that even though President Clinton called for renewal of fast track in his State of the Union speech, the administration has not given any indication that it is high on its agenda.

Senate Finance Committee Chairman **William V. Roth Jr.** R-DE is expected to introduce an omnibus trade bill in a few weeks that will include a provision renewing fast track authority, a spokeswoman said.



- by Juliana Gruenwald

Education

The Three R's And The Three W's

Most of America's public schools now have Internet access, and more than half of classrooms are hooked up to the World Wide Web, according to a study by the National Center for Education Statistics.

The study, "Internet Access in Public Schools and Classrooms between 1994 and 1998," shows that 89 percent of all schools have Internet access, up from 78 percent in 1997. Approximately 51 percent of classrooms, computer labs, school libraries, media centers and other facilities have Internet access, up from 27 percent in 1997 and just 3 percent in 1994.

The study also showed schools in low-income areas are bridging the gap with wealthy school districts in gaining Internet access. In 1997, only 63 percent of schools in the lower income districts were connected to the Web, compared with 88 percent of wealthy schools. That gap is "no longer significant" in 1998, says the report.

Still, teachers lag in training on how to use the computers to teach, with only 20 percent of teachers surveyed feeling they are "well prepared" to use the technology.

"That is why Congress should support my \$800 million educational

Mr. COBLE. Let me recognize the gentlelady from California. John, if you have an opening statement, I will come to you after.
Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. I also have a written statement that I would like to submit for the record and spare the crowd its reading.

Mr. COBLE. Without objection it will be done.

Ms. LOFGREN. I would just like to add my voice of thanks to Mr. Goodlatte for the work that he has done, and for the leadership role that he has played in bringing this bill forward. It has been a great partnership. I think we have terrific support here on both sides of the aisle for this important measure, and I am hopeful that by working together we can finally put this over the goal line this year.

I recognize that all Administrations, including the current one, have concerns about the use of encryption, and I am not hostile to the concerns that have been expressed over the years. Certainly law enforcement has a legitimate interest, when properly authorized to obtain information, to be able to do that. The plain fact is, however, that technology has moved past where we can control the use of encryption.

Last night I went on the Internet to see what you could download that is strong encryption. It is wonderful to see how technology develops and how widely it is distributed. To say that we can control the export of encryption when any one of us can go across the hall and download what we are prohibiting, I think, is preposterous.

So what we need to do is to organize ourselves with the help of the private sector so we provide as much information as possible to our much valued law enforcement agencies. Certainly we have able representatives here today. We know the NSA has been the prior employer of practically every cryptographer I have ever met. So they are certainly a capable agency. They probably don't need the help of private industry. But I think additional efforts to assist the FBI and State and local law enforcement agencies is something we need to monitor and industry needs to be a part of that. I am from Silicon Valley and know that industry is more than willing to act as an advisor and to assist in this regard.

I understand this is just the first hearing of many, but we are going to move very quickly this year, and I think that is important. I believe that we will have a terrific vote on the House floor soon. I have already been in touch with our colleagues on the Senate side—at least on the Democratic side of the aisle. They are eager to move this forward. So I am hopeful we can get this resolved once and for all for the benefit of our economy, and of our security.

Much has been said recently about our vulnerability to attack by terrorists and by rogue individuals, by those who would harm our Nation. One of the best ways to protect our system of information, our computer system is basic infrastructure is through strong encryption. So I am hopeful we can get past this together, for the benefit of both law enforcement and our economy. Having said that, I am eager to hear today's witnesses. It seems like I can never get away from Bill Reinsch, who often visits us in the valley. I credit him for being out and listening to industry and trying to

work with them in a productive way. Thank you and thank you, Mr. Chairman, for recognizing me.

Mr. COBLE. I thank the gentlelady.

[The prepared statement of Ms. Lofgren follows:]

PREPARED STATEMENT OF HON. ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF CALIFORNIA

I would like to thank the Chairman for holding this prompt hearing on H.R. 850, the Security and Freedom Through Encryption (SAFE) Act. Our national encryption policy is an extremely urgent matter and Congress must act promptly to avoid further damage to our national, economic, and personal security.

I have heard the Administration's call for a "balanced" encryption policy and I appreciate the steps they have taken thus far. I also understand their concerns regarding the potential impact that wider use of strong encryption could have on the ability of law enforcement and national security agencies to collect information important to their missions.

As a Member of the Judiciary Committee, which has oversight jurisdiction over Federal law enforcement agencies, I am certainly sympathetic to the difficulties that investigative and security agencies face in combating crime, terrorism, and espionage. However, I am convinced that current Administration encryption policy will not go very far in addressing these concerns. Indeed, I believe it will continue to do much to damage an industry that is of critical importance to the strategic and economic interests of the United States.

It is important to note that this is not the first Administration to advance controversial and onerous controls on digital software and hardware products. Unfortunately, the Executive Branch has an extensive history of almost unrestrained efforts to monitor electronic communications and data. Perhaps the most infamous example of this has been the notorious "Clipper Chip" proposal, authored by the Bush Administration.

The problem with the Administration's position is that the "balance" they seek to achieve—guaranteed access to the plaintext of any communication or data file—is simply impossible to achieve. The world's foremost experts in the field of cryptography and computer security, and we're privileged to have a few of those experts here with us today, have examined at this problem and have determined *unanimously* that such a system is beyond the experience and current competency of the field. Nor do they anticipate that such a scheme could be developed in the future either. The Administration is asking for industry to pull a rabbit out of a hat, but there's only a hat—no rabbit.

Furthermore, even if such a system could be developed, no sophisticated criminal or terrorist would ever use such a product; it's foolish to think otherwise. Therefore, for any mandatory access scheme to have any chance of achieving its intended goals, non-conforming encryption software must be unavailable to any criminal or terrorist, as well as every honest businessman or government.

Strong encryption products and knowledge about the science cryptography do not exist exclusively within the borders of the United States. It is very widely available on the Internet. We have recently seen numerous reports of such programs being developed by teenagers in Europe. Therefore, if the U.S. continues to pursue its current course, our law enforcement and national security interests will gain virtually nothing, and our nation will lose a lot. Our domestic workforce, American industry, and the U.S. Treasury will suffer unnecessary and irreparable damage (some estimates have projected losses of 200,000 jobs and \$96 billion over the next five years). Furthermore, our country will also lose our current lead (I have been told we have already lost about a third of the market) and along with it the concomitant expertise in the field of cryptography. If the best cryptographers are overseas, we as a nation will not only be less productive, but we will also be more vulnerable to strong encryption from a law enforcement and national security perspective.

I am also very disturbed that our current encryption policy has the perverse effect of making all Americans' digital information and communications more susceptible to hackers, terrorists, and thieves. In the name of promoting greater investigative ability for law enforcement, all Americans are more exposed than ever to illicit or surreptitious access to our computer files, phone conversations, and personal information. The former Speaker was just one victim of these unfortunate circumstances.

I recognize that the days of cracking strong codes are nearly gone. Unbreakable codes (256-bit key algorithms can generate more possible solutions than there are particles in the known universe) are already widely known. Private security experts and sophisticated hackers realize this and have begun to develop ways to attack

data at vulnerable points before and after it is encrypted (i.e., on the sender's hard drive or at some "good-guy" recipient such as a bank). I suspect that law enforcement and national security experts within the Government are acquiring similar capabilities. In fact, I have heard of private discussions between representatives of the NSA and industry in which the NSA urged companies to add backdoors or weaknesses to their products in order to receive preferential export treatment.

Our concerns about the privacy and civil libertarian consequences of current American encryption policy is not confined by the borders of the United States. I am also very concerned that our efforts to enlist broad international support for restraining strong encryption may inadvertently awaken Third World despots to a potential threat to their ability to stifle freedom of speech and prevent the free flow of information. Rather than conforming to U.S. proposals for mandatory key recovery or escrow, totalitarian regimes will have every incentive to implement outright bans on any encryption. Thus a tool that has the potential to foster freedom of expression and freer dissemination of knowledge is being taken away from oppressed people around the world as the result of America's ill-fated efforts to have freer access to domestic communications.

I am sanguine about our prospects to achieve legislative success with the SAFE bill this Congress. When we introduced the bill last week, Congressman Goodlatte and I were joined by more than 200 of our Colleagues, including the Leadership of the Democratic Caucus—including Congressman Gephardt, Congressman Bonior, Congressman Frost, Congresswoman DeLauro, and Congressman Lewis. The Ranking Democratic Member on the Judiciary Committee, Congressman Conyers, as well as the Ranking Democratic Member on the other Committee with primary jurisdiction on this bill, Congressman Gejdenson from International Relations, are also original cosponsors of H.R. 850.

It is important that we succeed now, sooner rather than later. If we are not successful this year, our nation could suffer egregious harm. Of course, if the Congress and the Administration fail this challenge, we are not without hope. We still have that third and co-equal third branch of Government, the Judiciary. Ongoing litigation against the Government by university professors may yet result in a finding by the courts that the Administration's restrictions on encryption are unconstitutional restraints on their First Amendment rights. These scholars maintain that software code is a form of speech and therefore is protected by the Constitution. One District Court judge has upheld this claim and found the Administration's export controls unconstitutional restraints of speech. The Ninth Circuit has heard arguments on the Government's appeal, and it appears likely that they will uphold the lower court's ruling.

Finally, I want to emphasize, as a Democrat with generally good relations with the White House, that I have been open to negotiations with the Administration on many of the issues that they have discussed. I have tried to work with Federal law enforcement and national security agencies to address their concerns. However, any broad discussions of these issues have failed to include serious discourse regarding the relaxation of export restrictions as part of the broader process, which is essential to addressing the important concerns I have expressed above. Even *Ira Magaziner*, author of the Administration's policy on e-commerce, stated late last year, "I don't agree with the policy we have." I remain open to such a dialogue, and hope that the Administration will acknowledge the shortcomings of their current policy before more serious damage is done to our computer industry and the security of all Americans.

Mr. COBLE. Mr. Conyers, do you have an opening statement that you wanted to make?

Mr. CONYERS. Chairman Coble, I would like to extend congratulations to both leaders of this measure. I think it is important. I supported it before. As electronic commerce explodes, our ability to compete in the international market will depend on the ability of our businesses and consumers to protect electronic data through encryption. Controls on the export of encryption products hinder our ability to compete, and of course there are law enforcement concerns, but I think that they will be considered adequately. I want to congratulate you for moving this forward early in the session, and I look forward to a favorable conclusion.

Mr. COBLE. I thank the gentleman from Michigan.

[The prepared statement of Mr. Conyers follows.]

PREPARED STATEMENT OF HON. JOHN CONYERS, JR., A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF MICHIGAN

Thank you, Mr. Chairman. I am proud to be a co-sponsor of H.R. 850, the "Security and Freedom through Encryption Act." In this electronic age, America's ability to compete in the international market depends upon the ability of American businesses and consumers to protect electronic data through encryption. Controls on the export of encryption products hinder that ability to compete.

Through a series of changes to the current laws on encryption, H.R. 850 ensures that America will be able to compete globally in the technology era. First, the bill states that it is legal for persons within the United States and for U.S. persons in foreign lands to use encryption. An important corollary to this is the prohibition on the Federal and State Governments from requiring "key escrows" so that third-parties, namely the Government, can access encrypted information.

While I fully believe in the authority of the Government to safeguard vital information, I am pleased that this bill precludes such key escrows. The interests of the Government are fully protected by the provisions in the bill that criminalize the use of encryption products for the furtherance of crimes.

This bill is definitely a step in the right direction. It looks out for American businesses, consumers, and for our national security. I look forward to working with the Members of this Committee on this important issue.

Mr. COBLE. Since we have liberally departed from the norm, Bill, if you or Ed have anything you would like to add, I would be happy to recognize either of you. Mr. Pease, you or Mr. Delahunt want to be heard?

Mr. PEASE. Mr. Chairman, if I have learned anything in the last 2 years, it is to be brief and to listen to the way you say things, and I guess what I would say is, in language you would understand, I don't have a dog in this hunt, but I am glad to be allowed to run with the big dogs.

Mr. COBLE. Thank you, sir.

Mr. DELAHUNT. I think I will associate myself with the remarks of the gentleman from Indiana, Mr. Pease. Let me just say—let me just acknowledge your role and the bipartisan leadership of Mr. Goodlatte and Ms. Lofgren in this matter that I think is of critical importance.

Mr. COBLE. Thank you.

Thank you all. Good to have the other gentlelady from California with us.

Our first witness today is the Honorable William Reinsch, who currently serves as the Under Secretary for Export Administration of the U.S. Department of Commerce. As head of the Bureau of Export Administration, or BXA, Mr. Reinsch is charged with administering and enforcing the export control policies of the United States Government as well as its antiboycott laws. In addition to the Bureau, he 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 and Economic Security, BXA is also responsible for monitoring and protecting the health of the United States industries critical to our national security and defense industrial base and assisting in domestic defense conversion efforts. Furthermore, in addition to his legislative role, Mr. Reinsch has served as an adjunct associate professor at the University of Maryland, University College Graduate School of Management and Technology, since 1990, teaching a course in international trade and trade policy.

Mr. Reinsch was awarded his B.A. degree in international relations from the Johns Hopkins University and an M.A. degree from Johns Hopkins School of Advanced International Studies.

Our next witness is Mr. Ronald Lee, Associate Deputy Attorney General for the United States Department of Justice. Mr. Lee is the Acting Director of the Executive Office of National Security at the Department and served as the program manager for the development of the Administration's 5-year counterterrorism and technology crime plan. Mr. Lee has served as general counsel at the National Security Agency and also served as chief of staff to the Director of Central Intelligence. He served as a law clerk to Justice John Paul Stevens and to Judge Abner Mikva, our former colleague.

Mr. Lee attended the Yale Law School, receiving his J.D. in 1985. Mr. Lee, we invited the Department of Justice to send a witness early on, and we were told initially that they would not be able to, but yesterday I think you were identified as the witness. It is good to have you with us this morning.

Mr. LEE. Thank you, Mr. Chairman. I am delighted to be here.

Mr. COBLE. The FBI has submitted a letter to us this morning, and I would ask that this letter be made a part of the record. Without objection.

[The information referred to follows:]

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, March 3, 1999.

Hon. HOWARD COBLE, *Chairman,*
Subcommittee on Courts and Intellectual Property,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: Enclosed please find copies of resolutions and letters from various law enforcement associations and groups which set forth their positions concerning encryption. Even though these letters were prepared during the last Congress, the positions set forth in them remain unchanged. You and the Members of the Subcommittee may find this information helpful as you begin consideration of H.R. 850, the "Security and Freedom Through Encryption (SAFE) Act", a bill to relax existing export controls on encryption.

Encryption is becoming a fact of everyday life in today's information age and a natural consequence of technology. Encryption is extremely beneficial when used legitimately to protect sensitive electronically stored information and the privacy of communications. But the use of strong, unbreakable encryption by hostile governments and by criminals and terrorists for illegal purposes poses a significant and unacceptable threat to our national security capabilities.

As you know, export controls on encryption products exist primarily to protect national security and foreign policy interests. On occasion, U.S. law enforcement is provided with valuable criminal-related information obtained through our Nation's intelligence gathering efforts. Law enforcement believes that such intelligence gathering capabilities derived, in part, from export controls on encryption should be preserved.

The law enforcement community continues to support the adoption of a balanced encryption policy. Such a balanced policy must satisfy the needs of commerce and communications privacy, the national security needs of the Intelligence Community as well as the public safety needs of law enforcement. We look forward to working with the Subcommittee and the Congress in an effort to develop a balanced encryption policy that effectively addresses all parties' concerns regarding this most important privacy, commerce, national security and public safety issue.

Sincerely yours,

JOHN E. COLLINGWOOD, *Assistant Director,*
Office of Public and Congressional Affairs.

Enclosures

Honorable Howard L. Berman
Ranking Minority Member
Subcommittee on Courts and
Intellectual Property
Committee on the Judiciary
House of Representatives
Washington, D.C.



**International Association of
Chiefs of Police**

616 North Washington Street
Alexandria, VA 22304-4287
Phone: 703/686-8177; 1-800/THE IACP
Fax: 703/686-4610
Cable Address: IACPOLICE

President
David L. Sanders
Chief of Police
Fresno, CA

Immediate Past President
David G. Weisbach
Chief of Police
Concord, NH

Past Vice President
Betty D. Moody
Chief of Police
Marietta, GA

Second Vice President
Ronald S. Neuberger
Chief of Police
St. Peter, MO

Third Vice President
Michael D. Robinson
Director
Michigan State Police
East Lansing, MI

Fourth Vice President
Steve D. Glasscock
Chief of Police
Plano, TX

Fifth Vice President
William B. Berger
Chief of Police
North Miami Beach, FL

Sixth Vice President
Joseph Sarnalek, Jr.
Chief of Police
Oakland, CA

Interim Vice President
Peter J. Weil Zundorf
Director of Police
Public Safety Mission on West
Street
Troy, The Netherlands

Treasurer
Donald G. Franco
Chief of Police
Bellevue, WA

**Division of State Associations of
Chiefs of Police**
General Chair
Joseph G. Esley
Chief of Police
Portland Police Department
White River Junction, VT

**Division of State and
Provincial Police**
General Chair
Samuel H. Gurneving
Director
Florida Highway Patrol
Tallahassee, FL

Past President and Parliamentarian
Don R. Downing
Worship, IL

Executive Director
David H. Fawcett
Alexandria, VA

**Deputy Executive Director/
Chief of Staff**
Stephen R. Conrath
Alexandria, VA

Encryption

*Submitted by: Legislative Committee
L006.a96*

WHEREAS, the introduction of digitally-based telecommunications technologies, as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of affordable and robust encryption products for private sector use; and

WHEREAS, on one hand encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications, On the other hand, the potential use of such encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety; and

WHEREAS, the law enforcement community is extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for law enforcement access and its timely decryption, pursuant to lawful authorization (court-authorized wiretaps or court-authorized search and seizure); and

WHEREAS, law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety needs; and

WHEREAS, law enforcement has found that robust key-escrow encryption is clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

WHEREAS, government representatives have been working with industry to encourage the voluntary development, sale, and use of key-escrow encryption in its pursuit of a balanced encryption policy; now, therefore, be it

RESOLVED, that the International Association of Chiefs of Police, duly assembled at its 103rd annual conference in Phoenix, Arizona, supports and encourages the development and adoption of a key-escrow encryption policy, which we believe represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs and that we oppose any efforts, legislatively or otherwise, that would undercut the adoption of such a balanced encryption policy.

NATIONAL SHERIFFS' ASSOCIATION



Resolution

DIGITAL TELECOMMUNICATIONS ENCRYPTION

- WHEREAS,** the introduction of digitally-based telecommunications technologies as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of affordable and robust encryption products for private sector use; and
- WHEREAS,** on one hand, encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other hand, the potential use of such encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety; and
- WHEREAS,** the law enforcement community is extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for court authorized law enforcement access and its timely decryption, pursuant to lawful authorization; and
- WHEREAS,** law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety needs; and
- WHEREAS,** law enforcement has found that robust key-escrow encryption is clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

Digital Telecommunications Encryption
Page 2

WHEREAS, government representatives have been working with industry to encourage the voluntary development, sale and use of key-escrow encryption in its pursuit of a balanced encryption policy; and

THEREFORE, BE IT RESOLVED that the National Sheriffs' Association supports and encourages the development and adoption of a key-escrow encryption policy which we believe represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs and that we oppose any efforts, legislatively or otherwise, that would undercut the adoption of such a balanced encryption policy.

Adopted at a meeting of the
Membership on this 19th day of
June, 1996 in Portland, Oregon



NATIONAL DISTRICT ATTORNEYS ASSOCIATION

99 Canal Center Plaza • Suite 510 • Alexandria, Virginia 22314

Telephone: (703) 548-9277

Fax: (703) 836-3193

RESOLUTION

ENCRYPTION

WHEREAS, the introduction of digitally-based telecommunications technologies as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of strong, affordable encryption products and services for private sector use; and

WHEREAS, on one hand the use of strong encryption products and services are extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other hand, the potential use of strong encryption products and services that do not allow for timely law enforcement decryption by a vast array of criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety; and

WHEREAS, the law enforcement community is extremely concerned about the serious threat posed by the use of these strong encryption products and services that do not allow for authorization (court-authorized wiretaps or court-authorized search and seizure); and

WHEREAS, law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for strong encryption while at the same time satisfying law enforcement's public safety needs for the timely decryption of encrypted criminal communications and information; and

WHEREAS, law enforcement has found that strong, key recovery encryption products and services are clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

WHEREAS, government representatives have been working with industry to encourage the voluntary development, sale, and use of key recovery encryption products and services in its pursuit of a balanced encryption policy;

BE IT RESOLVED, THAT the National District Attorneys Association supports and encourages the development and adoption of a balanced encryption policy that encourages the development, sale, and use of key recovery encryption products and services, both domestically and abroad. We believe that this approach represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs.

Adopted by the Board of Directors, November 16, 1996, Naples, Florida.
96-08FAL



MAJOR CITIES CHIEFS

July 24, 1997

The Honorable Orrin G. Hatch
Chairman, Judiciary Committee
531 Senate Hart Office Building
Constitution & Delaware Avenues, NE
Washington, DC 20510

Dear Mr. Chairman:

The Major Cities Chiefs is a professional association of police executives representing the largest jurisdictions in the United States. The association provides a forum for urban police chiefs, sheriffs and other law enforcement chief executives to discuss common problems associated with protecting cities with populations exceeding 500,000 people.

Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for law enforcement agencies across the country, both on the federal, state and local level, to lawfully gain access to criminal telephone conversations or electronically stored evidence. Since the impact of these proposals would seriously jeopardize public safety, our association urges you to support a balanced approach that strongly supports commercial and private interests but also maintains law enforcement's ability to investigate and prosecute serious crimes.

While we recognize that encryption is critical to communications security and privacy and that commercial interests are at stake, we all agree that without adequate legislation, law enforcement across the country will be severely limited in its ability to combat serious crime. The widespread use of non-key recovery encryption ultimately will eliminate our ability to obtain valuable evidence of criminal activity. The legitimate and lawful interception of communications, pursuant to a court order, for the most serious criminal acts will be meaningless because of our inability to decipher the evidence.

Encryption is certainly of great importance to the commercial interests across this country. However, public safety concerns are just as critical and we must not lose sight of this. The need to preserve an invaluable investigative tool is of the utmost importance in law enforcement's ability to protect the public against serious crime.

Sincerely yours,

[Handwritten signature of Mark A. Rodriguez]
Mark A. Rodriguez
Chairman

120 Chicago Police Department, 1121 S. State Street, Suite 401, Chicago, Illinois 60605

- Alaska
AK, California
WA County, California
I, California
San, California
California
Hawaii
IA, Florida
IL, Illinois, Indiana
Iowa
Kansas
KY, Kentucky
La, Louisiana
Md, Maryland
Maryland
MI, Michigan
MN, Minnesota
MO, Missouri
MS, Mississippi
MT, Montana
NE, Nebraska
NH, New Hampshire
NJ, New Jersey
NY, New York
NY, New York
NY, New York
OH, Ohio
OK, Oklahoma
OR, Oregon
PA, Pennsylvania
RI, Rhode Island
SC, South Carolina
SD, South Dakota
TN, Tennessee
TX, Texas
UT, Utah
VA, Virginia
WV, West Virginia
WI, Wisconsin
WY, Wyoming



Office of the Attorney General
Washington, D. C. 20530

July 18, 1997

Dear Member of Congress:

Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize public safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not

industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government -- including the Justice Department, Treasury Department, the National Association of Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association -- are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety.

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

- * An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot.
- * A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.

- * A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

And this is just the tip of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

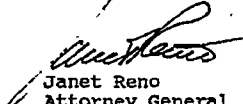
To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

- * A viable key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users.
- * A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plain text of encrypted communications and data.
- * An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

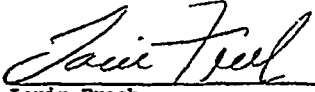
Only one bill, S.909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,



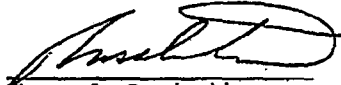
Janet Reno
Attorney General



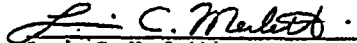
Louis Freeh
Director
Federal Bureau of Investigation



Barry McCaffrey
Director
Office of National Drug
Control Policy



Thomas A. Constantine
Director
Drug Enforcement Administration



Lewis C. Merletti
Director
United States Secret Service



Raymond W. Kelly
Undersecretary for Enforcement
U.S. Department of Treasury



George J. Weise
Commissioner
United States Customs Service



John W. Magaw
Director
Bureau of Alcohol, Tobacco
and Firearms



**International Association of
Chiefs of Police**

815 North Washington Street
Alexandria, VA 22314-2967
Phone: 703/836-8707; 1-800/THE IACP
Fax: 703/836-4648
Cable Address: IACPOLICE

President
Daniel L. Boudan
Chief of Police
Frankfort, IL

Immediate Past President
David G. Weitzel
Chief of Police
Concord, NH

First Vice President
Bobby D. Moody
Chief of Police
Marietta, GA

Second Vice President
Ronald S. Neubecker
Chief of Police
St. Petersburg, FL

Third Vice President
Michael D. Robinson
Director
Michigan State Police
East Lansing, MI

Fourth Vice President
Bruce D. Gleason
Chief of Police
Plano, TX

Fifth Vice President
William R. Berger
Chief of Police
North Miami Beach, FL

Sixth Vice President
Joseph S. Sauter, Jr.
Chief of Police
Oakland, CA

International Vice President
Peter J. van Zundert
Director of Police
Police Dept. Midden en West
Brabant
Tilburg, The Netherlands

Treasurer
Donald G. Piasco
Chief of Police
Bellingham, WA

**Division of State Associations of
Chiefs of Police**
General Chair
Joseph G. Estey
Chief of Police
Hartford Police Department
White River Junction, VT

**Division of State and
Provincial Police**
General Chair
Ronald E. Grimshaw
Director
Florida Highway Patrol
Tallahassee, FL

Past President and Parliamentarian
Don R. Deming
Winnipeg, IL

Executive Director
Daniel H. Rosenblat
Alexandria, VA

Deputy Executive Director
Chief of Staff
Eugene R. Cronauer
Alexandria, VA

July 21, 1997

Dear Member of Congress:

Enclosed is a letter sent to you by the Attorney General, the Director of National Drug Control Policy and all the federal law enforcement heads concerning encryption legislation being considered by congress. Collectively we, the undersigned, represent over 17,000 police departments including every major city police department, over 3,000 sheriffs departments, nearly every district attorney in the United States and all of the state Attorneys General. We fully endorse the position taken by our federal counterparts in the enclosed letter. As we have stated many times, Congress must adopt a balanced approach to encryption that fully addresses public safety concerns or the ability of state and local law enforcement to fight crime and drugs will be severely damaged.

Any encryption legislation that does not ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures will cause grave harm to public safety. The risk cannot be left to the uncertainty of market forces or commercial interests as the current legislative proposals would require. Without adequate safeguards, the unbridled use of powerful encryption soon will deprive law enforcement of two of its most effective tools, court authorized electronic surveillance and the search and seizure of information stored in computers. This will substantially tip the balance in the fight against crime towards society's most dangerous criminals as the information age develops.

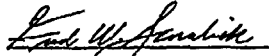
Member of Congress
page 2
July 21, 1997

We are in unanimous agreement that congress must adopt encryption legislation that requires the development, manufacture, distribution and sale of only key recovery products and we are opposed to the bills that do not do so. Only the key recovery approach will ensure that law enforcement can continue to gain timely access to the plaintext of encrypted conversations and other evidence of crimes when authorized by a court to do so. If we lose this ability--and the bills you are considering will have this result--it will be a substantial setback for law enforcement at the direct expense of public safety.

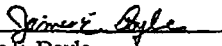
Sincerely yours,



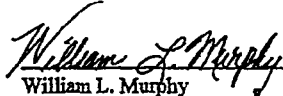
Darrell L. Sanders
President
International Association of
Chiefs of Police



Fred Scoraie
President
National Sheriffs' Association



James E. Doyle
President
National Association of
Attorneys General



William L. Murphy
President
National District Attorneys
Association



Office of the Attorney General
Washington, D. C. 20530

July 18, 1997

Dear Member of Congress:

Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize public safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not

industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government -- including the Justice Department, Treasury Department, the National Association of Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association -- are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety.

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

- * An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot.
- * A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.

- * A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

And this is just the tip of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

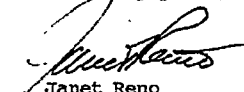
To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

- * A viable key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users.
- * A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plain text of encrypted communications and data.
- * An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

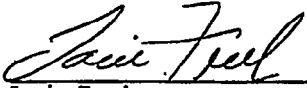
Only one bill, S.909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,



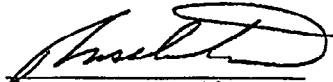
Janet Reno
Attorney General



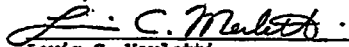
Louis Freeh
Director
Federal Bureau of Investigation



Barry McCaffrey
Director
Office of National Drug
Control Policy



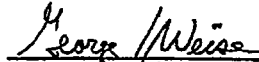
Thomas A. Constantine
Director
Drug Enforcement Administration




Lewis C. Merletti
Director
United States Secret Service



Raymond W. Kelly
Undersecretary for Enforcement
U.S. Department of Treasury



George J. Weisa
Commissioner
United States Customs Service



John W. Magaw
Director
Bureau of Alcohol, Tobacco
and Firearms

Mr. COBLE. Our final witness on this panel is the Honorable Barbara McNamara, who is the Deputy Director at the National Security Agency. Prior to assuming her current position, Ms. McNamara served as the Deputy Director of Operations, National Security Agency, Central Security Service, from January 1995 to September 1997. She was the Executive Director during 1994. The Deputy Director was briefly stationed at the Pentagon as the NSA, CSS representative to the Department of Defense. From 1984 to December 1993, she held several senior management assignments in the Operations Directory. She began her rise into the key management ranks of the Agency as Executive Assistant to the Deputy Director from 1983 to 1984.

Deputy Director McNamara graduated from Regis College in 1963 with a B.A. in French, and she attended the Armed Forces Staff College in 1976 and the National War College in 1982.

We have written statements from each of the witnesses on this panel, and I ask unanimous consent to submit them into the record in their entirety.

Let me say this before we hear from our witnesses. I am going to have to go to another meeting in about an hour, and I especially want Ms. Lofgren and Mr. Goodlatte to know that my departure is not a lack of interest in this legislation, but I will be able to stay at least for an hour.

Witnesses, if you will, we try to adhere rather rigidly to the 5-minute rule. When the red light illuminates in your eyes, you know you are skating on thin ice. We are not going to shut anybody off in the middle of a sentence, but if you could, condense your oral statement to 5 minutes, and of course we will examine in great detail the written testimony that we have.

Mr. Lee, why don't we begin with you, sir.

Mr. LEE. Mr. Chairman, I would ask your consent to defer my remarks until after those of my colleagues.

Mr. COBLE. I would beg your pardon?

Mr. LEE. I would ask your consent to defer my remarks until after those of my colleagues.

Mr. COBLE. That is fine. You go in any order you prefer.

How about ladies first, Ms. McNamara.

Ms. McNAMARA. I think it is probably more appropriate if Mr. Reinsch begins.

Mr. COBLE. Mr. Reinsch, I am hitting 0 for 2 now.

Mr. BERMAN. It is the soft line, the hard line and the really hard line.

Mr. REINSCH. No, Mr. Berman, I am in the center, as you can see from here.

Mr. COBLE. I am 1 for 3, which is not bad.

Mr. LEE. The red light is on.

STATEMENT OF WILLIAM A. REINSCH, UNDER SECRETARY OF COMMERCE FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. REINSCH. Thank you, Mr. Chairman, for the opportunity to be here and to testify. I thank Ms. Lofgren for her kind words. I note they were given before my testimony rather than after. We will see what she has to say when I am done.

I do want to talk a little bit about the progress we have made since my last testimony on this subject, which was in September 1997. 1998, I think, was the year of satellites. I didn't come up to see you on this issue, but I am glad to be back. It is clear even in the intervening period, it is clear from the crowd behind me that encryption remains a hotly debated issue.

We continue to support a balanced approach which considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the revolving realities of the marketplace.

With respect to the marketplace, the Internet and other electronic media are becoming increasingly important to the conduct of international business, as you well know. According to a recent study the value of e-commerce transactions in 1996 was \$12 million. The projected value in 2000 is \$2.16 billion. Many service industries which traditionally required face-to-face interactions such as banks, financial institutions and retail merchants are now providing cyberservice. Customers can now sit at their home computers and access their bank and investment accounts or buy a winter jacket or whatever with a few strokes of their keyboard.

Developing a new encryption policy has been complicated because we don't want to hinder its legitimate use, particularly for e-commerce, yet at the same time we want to protect our vital national security, foreign policy and law enforcement interests. We have concluded that the best way to accomplish this is to continue our balanced approach to promote the development of strong encryption products that would allow lawful government access to plaintext under carefully defined circumstances; to promote the legitimate uses of strong encryption to protect confidentiality; and continue looking for additional ways to protect important law enforcement and national security interests.

During the past 3 years we have learned that there is no one-size-fits-all solution. And we have learned that the use of strong nonrecovery encryption within certain trusted industry sectors is an important component of our policy in order to protect private consumer information and allow our high-tech industry to maintain its lead in the information security market.

Let me summarize for you some of the changes we have made in our policy in the last year or so. On September 22, 1998, we published a regulation implementing our decision to allow the export, under a license exception, which means they don't have to come in for individual advance approval, of unlimited-strength encryption to banks and financial institutions located in countries that are members of the Financial Action Task Force or have effective antimoney-laundering laws. That means that over 100 of the world's largest banks and almost 70 percent of the international financial institution market is now eligible for strong American-made encryption.

The further result of our extensive dialogue with industry, law enforcement, and privacy groups has been an update to our policy that the Vice President announced last September 16. The regulations implementing that update were published on December 31.

That is not going to end the debate, as this hearing evidences, but we believe it addresses a number of private sector concerns by opening large markets and further streamlining exports.

Let me summarize what we did last September. Specifically our policy allows for the export of 56-bit hardware and software worldwide to any end user under license exception; exports of strong encryption, including technology, to U.S. companies and their subsidiaries under license exception to protect important business proprietary information; exports of strong encryption to the insurance and medical health sectors in 46 countries under license exception for use in securing proprietary and medical health information; exports of strong encryption to secure on-line transactions between on-line merchants and their customers in 46 countries under license exception; recovery-capable or recoverable encryption products of any key length, such as the so-called doorbell products, can now be improved under a kind of bulk license called encryption licensing arrangements to recipients in 46 countries. Examples of such products are systems that are managed by a network or corporate security administrator.

We have also expanded our policy to encourage the marketing of a wider variety of recoverable products that may not be key recovery in a narrow sense, but which may be helpful to law enforcement. These are typically managed by a corporate administrator. We have also streamlined exports of key recovery products by no longer requiring review of foreign key recovery agents and no longer requiring the submission of business plans.

We also made progress internationally through the Wassenaar Arrangement. In December, through the hard work of Ambassador David Aaron, the Wassenaar members agreed on several changes in this area which go a long way to awarding increasing international security and public safety. Specific changes include removing controls on all encryption products at or below 56 bits and certain consumer items regardless of key length and on cordless telephone systems designed for home use.

Most importantly the Wassenaar members agreed to remove encryption software from the General Software Note and replace it with a new cryptography note. This was essential to modernize the General Software Note and close the loophole that permitted the uncontrolled export of encryption with unlimited key length. Under the new note, mass market hardware has been added, and a 64-bit key length or below has been set as an appropriate threshold. That will enable governments to review the dissemination of 64-bit and above encryption.

Let me close, Mr. Chairman, if I may, by saying a word specifically about H.R. 850. With respect to that bill, the Administration opposes this legislation, as we did its predecessor in the last Congress. The bill proposes export liberalization far beyond what the Administration can entertain and which will be contrary to our international export control obligations. Despite some cosmetic changes the authors have made, the bill in letter and spirit would destroy the balance we have worked so hard to achieve and would jeopardize our law enforcement and national security interests.

I will defer to other witnesses on the impact of the bill on their concerns, but let me describe particularly the export control provi-

sion. We believe that its references to IEEPA, as I understand them, would preclude controls under current circumstances and in any future situation where the EAA had expired, and we believe the definition of general availability, as in the past, would preclude export controls over most software.

In addition, whether intended or not, we believe the bill as drafted could inhibit the development of key recovery even as a viable commercial option for those corporations and end users that want it in order to guarantee access to their data.

We look forward, Mr. Chairman, to what I am sure is going to be a spirited debate about this. I thank you for your indulgence.

Mr. COBLE. I think you, Mr. Reinsch, for your leadoff hitting role. [The prepared statement of Mr. Reinsch follows:]

PREPARED STATEMENT OF WILLIAM A. REINSCH, UNDER SECRETARY OF COMMERCE
FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Thank you, Mr Chairman, for the opportunity to testify on the direction of the Administration's encryption policy. We have made a great deal of progress since my last testimony on this subject in September 1997.

Even so, encryption remains a hotly debated issue. The Administration continues to support a balanced approach which considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the market place.

The Internet and other electronic media are becoming increasingly important to the conduct of international business. One of the many uses of the Internet which will have a significant affect on our everyday lives is electronic commerce. According to a recent study, the value of e-commerce transactions in 1996 was \$12 million. The projected value of e-commerce in 2000 is \$2.16 billion. Many service industries which traditionally required face to face interaction such as banks, financial institutions, and retail merchants are now providing cyber service. Customers can now sit at their home computers and access their banking and investment accounts or buy a winter jacket with a few strokes of their keyboard.

Furthermore, most businesses maintain their records and other proprietary information, such as health records or sales strategies, electronically. They now conduct many of their day-to-day communications and business transactions via the Internet and E-mail. An inevitable byproduct of this growth of electronic commerce is the need for strong encryption to provide the necessary secure infrastructure for electronic communications, transactions and networks. The disturbing increase in computer crime and electronic espionage has made people and businesses wary of posting their private and company proprietary information on electronic networks if they believe the infrastructure may not be secure. A robust secure infrastructure can help allay these fears, and allow electronic commerce to continue its explosive growth.

Developing a new encryption policy has been complicated because we do not want to hinder its legitimate use—particularly for electronic commerce; yet at the same time we want to protect our vital national security, foreign policy and law enforcement interests. We have concluded that the best way to accomplish this was to continue a balanced approach: to promote the development of strong encryption products that would allow lawful government access to plaintext under carefully defined circumstances; to promote the legitimate uses of strong encryption to protect confidentiality; and continue looking for additional ways to protect important law enforcement and national security interests.

During the past three years, we have learned that there are many ways to assist in lawful access. There is no one-size-fits-all solution. The recovery encryption plans we received showed that different technical approaches to recovery of plaintext exist. In licensing exports of encryption products under individual licenses, we also learned that, while some products may not meet the strict technical criteria of our regulations, they are nevertheless consistent with our policy goals.

Additionally, we learned that the use of strong non-recovery encryption within certain trusted industry sectors is an important component of our policy in order to protect private consumer information and allow our US high tech industry to maintain its lead in the information security market while minimizing risk to national security and law enforcement equities.

Taking into account all that we have learned and reviewing international market trends and realities, in 1998 we made several changes to our encryption policy that I will summarize for you.

On September 22, 1998, we published a regulation implementing our decision to allow the export, under a license exception, of unlimited strength encryption to banks and financial institutions located in countries that are members of the Financial Action Task Force or have effective anti-money laundering laws. The regulation also allows exports, under a license exception, of encryption products that are specially designed for financial transactions. This new policy recognizes the fact that we need to secure and safeguard our financial networks, and the banking and financial communities cooperate with government authorities when information is required to combat financial and other crimes. The direct result of this policy change is that over 100 of the world's largest banks and almost 70% of the international financial institution market is now eligible for strong American-made encryption.

As I mentioned earlier, we have been looking for ways to make our policy consistent with both market realities and national security and law enforcement concerns. Since last March, the Administration has been engaged in a dialogue with U.S. industry, law enforcement, and privacy groups on how our policy might be improved to find technical solutions, in addition to key recovery, that can assist law enforcement in its efforts to combat crime. At the same time, we wanted to find ways to assure U.S. technology leadership, promote secure electronic commerce, and protect important privacy concerns. The purpose of this dialogue was to find cooperative solutions that could assist law enforcement, while protecting national security, plus assuring continued U.S. technology leadership and promoting the privacy and security of U.S. firms and citizens in electronic commerce. We believed then and now that the best way to make progress on this issue is through a constructive cooperative dialogue, rather than seeking legislative solutions. Through our dialogue, there has been increased understanding among the parties. And we have made progress.

The result of this dialogue was an update to our encryption policy which Vice President Gore unveiled last September 16. The regulations implementing the update were published on December 31. This will not end the debate over encryption controls, but we believe the regulation addresses some private sector concerns by opening large markets and further streamlining exports.

The policy update liberalizes controls on 56-bit products and on products of unlimited bit length, whether or not they contain recovery features, to certain industry sectors. Many of the new reforms permit the export of encryption to certain end-users under a license exception. That is, after the product receives a one-time review, it can be exported by the manufacturer, resellers and distributors without the need for a license or other additional review. In developing our policy we identified the key sectors that will form the basis of creating a reliable secure infrastructure for communicating and storing critical personal information: banks, financial institutions, insurance companies, on-line merchants, and health facilities.

Specifically, the new policy allows for:

- the export of 56-bit hardware and software worldwide to any end user under a license exception;
- exports of strong encryption, including technology, to U.S. companies and their subsidiaries under a license exception to protect important business proprietary information;
- exports of strong encryption to the insurance and medical/health sectors in 46 countries under a license exception for use in securing proprietary medical and health information;
- exports of strong encryption to secure on-line transactions between on-line merchants and their customers in 46 countries under a license exception.
- "recovery capable" or "recoverable encryption products of any key length, such as the so-called "doorbell" products, can now be approved under a kind of bulk license called an "encryption licensing arrangement" to recipients in 46 countries. Examples of such products are systems that are managed by a network or corporate security administrator.

I would note that these provisions apply to products with or without key recovery features. One of the aspects of our policy update is to permit exports of strong encryption with or without key recovery to protect electronic commerce while also minimizing the risk to national security and law enforcement. For example, in some cases we have limited our approval policy to a list of countries or a set of end users, rather than permit exports on a global basis, to help protect national security interests.

We have also expanded our policy to encourage the marketing of a wider variety of "recoverable" products that may not be key recovery in a narrow sense but which may be helpful to law enforcement pursuant to strict authorities. Again, these are typically systems managed by a network or corporate administrator. We also further streamlined exports of key recovery products by no longer requiring a review of foreign key recovery agents and no longer requiring companies to submit business plans.

This past year, we also made progress on developing a common international approach to encryption controls through the Wassenaar Arrangement, which was established in 1996 as the successor to COCOM. It is an international export control arrangement among 33 countries whose purpose is to prevent destabilizing accumulations of arms and civilian items with military uses in countries or regions of concern. It is the multilateral basis for many of our export controls.

In December, through the hard work of Ambassador Aaron, the President's special envoy on encryption, the Wassenaar Arrangement members agreed on several changes relating to encryption controls. These changes go a long way toward increasing international security and public safety by providing countries with a stronger regulatory framework for managing the spread of robust encryption.

Specific changes to multilateral encryption controls include removing controls on all encryption products at or below 56 bit and certain consumer items regardless of key length, such as entertainment TV systems, DVD products, and on cordless telephone systems designed for home or office use.

Most importantly, the Wassenaar members agreed to remove encryption software from the General Software Note and replace it with a new cryptography note. First drafted in 1991, the General Software Note allowed countries to export mass market encryption software without restriction. It was essential to modernize the GSN and close the loophole that permitted the uncontrolled export of encryption with unlimited key length. Under the new cryptography note, mass market hardware has been added and a 64-bit key length or below has been set as an appropriate threshold. This will enable governments to review the dissemination of 64-bit and above encryption.

I want to be clear that this does not mean encryption products of more than 64 bits cannot be exported. Our own policy permits that. It does mean, however, that such exports must be reviewed by governments consistent with their national export control procedures.

Export control policies without a multilateral approach have little chance of success. Agreement, by the Wassenaar members, to close the loophole for mass market encryption products is a strong indication that other countries are beginning to share our public safety and national security concerns. Contrary to what many people thought two years ago, we have found that most major encryption producing countries are interested in developing a harmonized international approach to encryption controls.

At the same time, we recognize that this is an evolutionary process, and we intend to continue our dialogue with industry. Our policy should continue to adapt to technology and market changes. We will review our policy again this year with a view toward making further changes. An important component of our review is input from industry, which we are receiving through our continuing dialogue.

With respect to H.R.850, the Administration opposes this legislation as we did its predecessor in the last Congress. The bill proposes export liberalization far beyond what the Administration can entertain and which would be contrary to our international export control obligations. Despite some cosmetic changes the authors have made, the bill in letter and spirit would destroy the balance we have worked so hard to achieve and would jeopardize our law enforcement and national security interests. I defer to other witnesses to describe the impact of the bill on their equities, but let me describe two of its other problems.

First, I want to reiterate that this Administration is not seeking controls or restraints on domestic manufacture or use of encryption. We continue to believe the best way to make progress on ways to assist law enforcement is through a constructive dialogue. As a result, we see no need for the statutory prohibitions contained in the bill.

Second, once again we must take exception to the bill's export control provisions. In particular, the references to IEEPA as I understand them would preclude controls under current circumstances and in any future situation where the EAA had expired, and the definition of general availability, as in the past, would preclude export controls over most software.

In addition, whether intended or not, we believe the bill as drafted could inhibit the development of key recovery even as a viable commercial option for those corporations and end users that want it in order to guarantee access to their data. The

Administration has repeatedly stated that it does not support mandatory key recovery, but we endorse and encourage development of voluntary key recovery systems, and, based on industry input, we see growing demand for them, especially corporate key recovery, that we do not want to cut off.

As this Committee knows better than most, public debate over encryption policy has been spirited. Many on both sides of the debate have had difficulty grasping their counterparts' views or realizing that there is a middle ground. Our dialogue with industry has gone a long way toward bridging that gap and finding common ground. We will continue this policy of cooperative exchange as it is clearly the best way to pursue our policy objectives of balancing public safety, national security, and the competitive interests of US companies.

Mr. COBLE. Ms. McNamara, you are the second batter then.

Ms. McNAMARA. I am, sir.

Mr. COBLE. Very well.

STATEMENT OF BARBARA McNAMARA, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Ms. McNAMARA. Thank you, Mr. Chairman and members of the committee, for giving me the opportunity to appear today. I would like to begin briefly by introducing the National Security Agency and its mission and explain why this issue is so important to us.

NSA secures information systems for the Department of Defense and other U.S. Government agencies and provides information derived from foreign signals to a variety of users in the Federal Government. It is this signals intelligence role that I want to address today.

NSA intercepts and analyzes the communication signals of foreign adversaries to produce critically unique and actionable intelligence for our national leaders and military commanders. Very often time is of the essence. Intelligence is perishable. It is worthless if we cannot get it to the decisionmakers in time to make a difference.

Signals intelligence proved its worth in World War II when the United States broke the Japanese naval code and learned of their plans to invade Midway Island. This intelligence significantly aided the U.S. defeat of the Japanese fleet and helped shorten the war. NSA provided the same kind of intelligence support to our troops in Desert Shield and Desert Storm, and that support continues today in Bosnia and other locations around the world where U.S. military forces are deployed.

NSA signals intelligence efforts also support policymakers and law enforcement. Demands on NSA for timely intelligence have only grown since the breakup of the Soviet Union and have expanded into other national security areas of terrorism, weapons proliferation, and narcotic trafficking.

Passage of legislation that immediately decontrols the export of strong encryption will significantly harm NSA's ability to carry out its mission and will ultimately result in the loss of essential intelligence being provided to this Government. Immediate decontrol of encryption exports will likely result in the global spread of strong encryption among our adversaries and the use of encryption at multiple levels within a communications network. This will greatly complicate our exploitation of foreign targets and the timely delivery of usable intelligence because it will take too long to decrypt a message, if indeed we can decrypt it at all.

Today many of the world's communications are encrypted. Historically encryption has been used primarily by governments and the military. It was employed for confidentiality in hardware-based systems and was difficult to use. As encryption moves to software-based implementations, and the infrastructure develops to provide a host of encryption-related security services, encryption will spread and be widely used by our adversaries that have traditionally relied upon unencrypted communications. The immediate decontrol of encryption exports would place encryption in the hands of many of these adversaries, and, as a result, much of the crucial information which we are able to provide today could quickly become unavailable to the decisionmakers.

As you will hear from my colleague from the Department of Justice, it is important that you understand that the needs of national security and law enforcement are different, and they must be addressed separately. At NSA we are focused on preserving export controls on encryption to protect national security.

As you consider Mr. Goodlatte's bill, it is very important that you understand the significant effect certain provisions of this bill will have on national security. The SAFE Act would mandate the immediate decontrol of most commercial computer software encryption and specified hardware encryption exports. It would also deprive us of the opportunity to conduct a meaningful review of a proposed encryption export to ensure its compatibility with national security interests. Historically this review process has provided us with valuable insight into what is being exported, to whom, and for what purpose. Without this review and the ability to deny an export application if necessary, it will be impossible to control exports of encryption to countless bad guys.

For instance, immediate decontrol would undermine international efforts to prevent terrorist attacks and to catch terrorists, drug traffickers and proliferators of weapons of mass destruction.

The SAFE Act would permit exports of encryption based on products comparable to those being exported for foreign financial institutions. The criteria for exporting encryption to these institutions should not be the basis for decontrolling other encryption exports. Allowing favorable treatment for specific classes of end users may be appropriate when they are well regulated and have a good record of providing access to lawful requests for information, but using the special treatment afforded banks and financial institutions as the basis for a blanket approval of export to all other end users in a country would eliminate important national security end use considerations.

Mr. Goodlatte's bill also eliminates controls for computer hardware with encryption capability if it is found that the product is available in overseas markets. The apparent availability of a product in a country without regard to its actual performance capabilities or without restrictions on end user or end uses will have the practical effect of forcing the decontrol of such exports, a condition that is unacceptable to national security.

In summary, we believe we need a balanced encryption policy that considers the needs of national security and industry. The recent U.S. and Wassenaar policy updates are positive moves in that direction, and they are examples of the kind of advances possible

under the current regulatory structure, which provides greater flexibility than a statutory structure would.

Let me make it clear, we want U.S. companies to effectively compete in world markets. In fact, it is something we strongly support as long as it is done consistent with national security needs.

In summary, the SAFE Act will harm national security by making NSA's job of providing critical, actionable intelligence to our leaders and military commanders difficult if not impossible, thus putting our Nation's security at considerable risk. The United States cannot have an effective decisionmaking process, or a strong fighting force, or a responsive law enforcement community, or a strong counterterrorism capability unless the information required to support them is available in time to make a difference. The Nation needs a balanced encryption policy, no doubt. It must allow U.S. industry to continue to be the world's technology leader, but we also must ensure that we protect the security of our Nation. Thank you for this opportunity.

Mr. COBLE. Thank you, Ms. McNamara.

[The prepared statement of Ms. McNamara follows:]

PREPARED STATEMENT OF BARBARA MCNAMARA, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. Chairman Coble, thank you for giving me the opportunity today to discuss the important issue of encryption. I will be discussing the national security needs for export controls on encryption and why we oppose legislation that would effectively lift those controls. I will then address specific concerns NSA has with provisions of Mr. Goodlatte's bill. However, I would like to begin by briefly introducing the National Security Agency (NSA) and its mission.

The National Security Agency was founded in 1952 by President Truman. As a separately organized agency within the Department of Defense, NSA provides signals intelligence to a variety of users in the Federal Government and secures information systems for the Department of Defense and other U.S. Government agencies. NSA was designated a Combat Support Agency in 1988 by the Secretary of Defense in response to the Goldwater-Nichols Department of Defense Reorganization Act.

The ability to understand the secret communications of our foreign adversaries while protecting our own communications—a capability in which the United States leads the world—gives our nation a unique advantage. The key to this accomplishment is cryptology, the fundamental mission and core competency of NSA. Cryptology is the study of making and deciphering codes, ciphers, and other forms of secret communications. NSA is charged with two complementary tasks in cryptology: first, exploiting foreign communications signals and second, protecting the information critical to US. national security. By "exploitation," I am referring to signals intelligence, or the process of deriving important intelligence information from foreign communications signals; by "protection" I am referring to providing security for information systems. Maintaining this global advantage for the United States requires preservation of a healthy cryptologic capability in the face of unparalleled technical challenges.

It is the signals intelligence (SIGINT) role that I want to address today. Our principal responsibility is to ensure a strong national security environment by providing timely information that is essential to critical military and policy decision making. NSA intercepts and analyzes the communications signals of our foreign adversaries, many of which are guarded by codes and other complex electronic countermeasures. From these signals, we produce vital intelligence reports for national decision makers and military commanders. Very often, time is of the essence. Intelligence is perishable; it is worthless if we can not provide it in time to make a difference in rendering vital decisions.

For example, SIGINT proved its worth in World War II when the United States broke the Japanese naval code and learned of their plans to invade Midway Island. This intelligence significantly aided the U.S. defeat of the Japanese fleet. Subsequent use of SIGINT helped shorten the war. NSA continues today to provide vital intelligence to the warfighter and the policy maker in time to make a difference for our nation's security. Demands on us in this arena have only grown since the break-

up of the Soviet Union and have expanded to address other national security threats such as terrorism, weapons proliferation, and narcotic trafficking, to name a few.

Because of these growing serious threats to our national security, care must be taken to protect our nation's intelligence equities. Passage of legislation that immediately decontrols the export of strong encryption will significantly harm NSA's ability to carry out our mission and will ultimately result in the loss of essential intelligence reporting. This will greatly complicate our exploitation of foreign targets and the timely delivery of intelligence to decision makers because it will take too long to decrypt a message—if indeed we can decrypt it at all.

Today, many of the world's communications are unencrypted. Historically, encryption has been used primarily by governments and the military. It was employed for confidentiality in hardware-based systems and was often cumbersome to use. As encryption moves to software-based implementations and the infrastructure develops to provide a host of encryption-related security services, encryption will spread and be widely used by other foreign adversaries that have traditionally relied upon unencrypted communications. The immediate decontrol of encryption exports would accelerate the use of encryption by many of these adversaries and as a result, much of the crucial information we are able to gather today could quickly become unavailable to us. Immediate encryption decontrol will also deprive us of the opportunity to conduct a meaningful review of encryption products prior to their export. In the past, this review process has provided us with valuable insight into what is being exported, to whom, and for what purpose. Without this review and the ability to deny an export application, it will be impossible to control exports of encryption to individuals and organizations that threaten the United States. For instance, immediate decontrol will undermine international efforts to catch terrorists, drug traffickers, and proliferators of weapons of mass destruction.

Please do not confuse the needs of national security with the needs of law enforcement. The two sets of interests and methods vary considerably and must be addressed separately. The law enforcement community is concerned about the use of non-recoverable encryption by persons engaged in illegal activity domestically. At NSA, we are primarily focused on preserving export controls on encryption to protect national security.

While our mission is to provide intelligence to help protect the country's security, we also recognize that there must be a balanced approach to the encryption issue. The interests of industry and privacy groups, as well as of the Government, must be taken into account. Encryption is a technology that will allow our citizens to fully participate in the 21st Century world of electronic commerce. It will enhance the economic competitiveness of U.S. industry. It will combat unauthorized access to private information and it will deny adversaries from gaining access to U.S. information wherever it may be in the world.

To promote this balanced approach, we are engaged in an ongoing and productive dialogue with industry. The recent Administration update to the export control regulations addresses many industry concerns and has significantly advanced the ability of U.S. vendors to participate in overseas markets. Of equal significance, the Wassenaar nations, representing most major producers and users of encryption, agreed unanimously in December 1998 to control strong hardware and software encryption products. The Wassenaar Agreement clearly shows that other nations agree that a balanced approach is needed on encryption policy and export controls so that commercial and national security interests are addressed. Both are positive developments because they open new opportunities for U.S. industry while still protecting national security. These are examples of the kinds of advances possible under the current regulatory structure, which provides greater flexibility than a statutory structure to adjust export controls as circumstances warrant in order to meet the needs of Government and industry. We want U.S. companies to effectively compete in world markets. In fact, it is something we strongly support as long as it is done consistently with national security needs. NSA supports the recent updates to the Administration's policy. The export provisions were carefully designed to open up large commercial markets while trying to minimize potential risk to national security. We believe significant progress was made.

As you move towards markup of Mr. Goodlatte's bill, it is very important that you understand the significant effect certain provisions of this bill will have on national security. If enacted, the bill would effectively decontrol most commercial computer software encryption and specified hardware encryption exports to all destinations, even regions of instability. It would also deprive the Government of the opportunity to conduct a meaningful review of a proposed export to assure it is compatible with U.S. national security interests and would also eliminate the ability to deny an export application if national security concerns are not adequately addressed.

The bill would permit exports of encryption based on products that are permitted to be exported for foreign financial institutions. The criteria for exporting encryption to these institutions should not be the basis for decontrolling other encryption exports. Allowing favorable treatment for specific classes of end-users may be appropriate in cases such as those involving banks and other financial institutions which are well regulated and have a good record of providing access to lawful requests for information. Requiring the blanket approval of exports to all other end-users in a country would eliminate important national security end-use considerations for these exports.

In summary, the SAFE Act will harm national security by making NSA's job of providing vital intelligence to our leaders and military commanders difficult, if not impossible, thus putting our nation's security at some considerable risk. Our nation cannot have an effective decision-making process, or a strong fighting force, or a responsive law enforcement community unless the intelligence information required to support them is available in time to make a difference. The nation needs a balanced encryption policy that allows U.S. industry to continue to be the world's technology leader, but that policy must also protect our national security interests.

Thank you for the opportunity to address the Subcommittee and I would be happy to answer any questions you may have.

SUMMARY

The National Security Agency (NSA) intercepts and analyzes the communications signals of our foreign adversaries to produce vital intelligence reports for national decision makers and military commanders. Demands in this arena have only grown since the break-up of the Soviet Union, and have expanded to address other national security threats such as terrorism, weapons proliferation, and narcotic trafficking.

The SAFE Act will make NSA's job of providing vital intelligence to our national leaders and military commanders difficult, if not impossible. It will effectively decontrol the export of strong encryption and greatly complicate our exploitation of foreign targets. It will take too long to decrypt a message—if indeed we can decrypt it at all. Intelligence is perishable. Our nation cannot have an effective decision-making process, or a strong fighting force, or a responsive law enforcement community unless the intelligence information required to support them is available in time to make a difference. The SAFE Act will effectively decontrol encryption exports to all destinations, even to regions of instability. It will also deprive the Government of the opportunity to conduct a meaningful review of a proposed export to assure it is compatible with U.S. national security interests, and will eliminate the ability to deny an export application, even when national security concerns exist.

To promote a balanced encryption policy that allows U.S. industry to continue to be the world's technology leader and that also protects our national security interests, we are engaged in an ongoing and productive dialogue with industry. The recent Administration update to the export control regulations addresses many industry concerns and has significantly advanced the ability of U.S. vendors to participate in overseas markets. In addition, 33 Wassenaar nations recently signed an agreement to control strong hardware and software encryption products. These are positive examples the kinds of advances possible under the current regulatory regime which provides greater flexibility than a statutory structure to adjust export controls, as circumstances warrant, to meet the needs of the Government and industry.

Mr. COBLE. Mr. Lee?

STATEMENT OF RONALD D. LEE, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. LEE. Thank you, Mr. Chairman. I appreciate the opportunity to appear before the subcommittee and to present the views of the Department of Justice on the issues of encryption and export controls. I would like to touch upon a few themes in my written statement this morning.

There are a number of misconceptions about law enforcement's position on encryption. The Department of Justice supports the spread of strong recoverable encryption. We recognize that this technology can further law enforcement's vital responsibilities to enforce the laws that protect privacy, electronic, and other forms of commerce over our Nation's communications networks.

The Department of Justice is, however, deeply concerned about the threat to public safety that is posed by the widespread availability and distribution of nonrecoverable encryption; that is, encryption where there is not a lawfully authorized means to obtain the plaintext of communications and data.

Law enforcement agencies, both Federal and State, have already begun to see cases where encryption has been used in an attempt to conceal criminal activity, and we anticipate that both the number and the complexity of these cases will increase as encryption proliferates and as encryption increasingly becomes a component of mass market software items. We remain vitally concerned that agents will not be able to fully execute the search warrants, wiretap orders, and other legal processes authorized by Congress and ordered by the courts that are essential to effective law enforcement investigations today.

The Department of Justice supports the carefully balanced approach to export controls that the Administration is actively pursuing. The Attorney General along with the Director of the Federal Bureau of Investigation and other senior Government officials have been engaging industry leaders in a continuing and cooperative dialogue, and this dialogue has continued throughout both the Department and the FBI at several different levels, technical and policy, and has provided us with an opportunity to explain the public safety concerns that the spread of nonrecoverable encryption presents. These dialogues have also very importantly provided us with a great opportunity to learn about innovative solutions that industry has presented and industry's view of where the marketplace is evolving to.

We thank the Members of Congress who have helped to facilitate this dialogue, and we will work hard to make sure that these productive discussions continue. The Department of Justice believes that the current balanced approach is most conducive to the continuation of these communications and dialogues, and we believe that the rapid elimination of export controls as proposed in the proposed Security and Freedom through Encryption Act would upset this balance and this dialogue.

In addition to intensive dialogue with industry, however, law enforcement believes that in order to discharge its obligation of protecting public safety, we must also continue to develop our technical expertise. We agree with and welcome the remarks of Congresswoman Lofgren that we need to keep close attention upon the need to provide support to State and local as well as Federal officials as we work with industry.

We have begun initiatives such as the funding of a centralized technical resource within the FBI which will support Federal, State, and local law enforcement personnel in developing a broad range of expertise, technologies, and tools to respond directly to the threat to public safety that encryption poses when in the hands of criminals and terrorists.

This resource will also allow law enforcement to stay current with technology, which moves very rapidly. We look forward to working with Congress to develop and enhance this resource so that law enforcement may continue its role of protecting public safety in the future.

I would like to add a couple of specific comments about H.R. 850. We believe that it would harm national security and public safety by liberalizing export controls far beyond their current policy and far beyond either the expectations or the agreements that we have with our allies and our counterparts. We are also concerned that the provisions in the bill may prohibit the Government from encouraging the development of key management infrastructures and other promising technologies.

For example, the Government may wish to encourage contractors and other people doing business with the Government to further a Government interest by using plaintext recovery mechanisms. The Government may also need to ensure that legally required record-keeping, such as in firearms or controlled drugs transactions, are available in plaintext form regardless of how technology evolves.

And secondly, we believe the Administration's approach, which we fully support, balances the need for secure private communications against the equally important need to protect the safety of the public against criminal threats. We will work with you on this important issue both now and in the future. Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Lee, and thanks to the entire panel. [The prepared statement of Mr. Lee follows:]

PREPARED STATEMENT OF RONALD D. LEE, ASSOCIATE DEPUTY ATTORNEY GENERAL,
U.S. DEPARTMENT OF JUSTICE

Mr. Chairman, thank you for the opportunity to testify about the Department of Justice's views on export controls on encryption, and particularly the proposed Security and Freedom through Encryption (SAFE) Act, recently introduced by Mr. Goodlatte as H.R. 850. As you are aware, export controls on encryption is a complex and difficult issue that we are attempting to address with our colleagues throughout the Administration. In my testimony, I will first outline the basic perspective and recent initiatives of the Department of Justice on encryption issues, and will then discuss some specific concerns with the SAFE Act.

The Department of Justice supports the spread of strong, recoverable encryption. Law enforcement's responsibilities and concerns include protecting privacy and commerce over our nation's communications networks. For example, we prosecute under existing laws those who violate the privacy of others by illegal eavesdropping, hacking or theft of confidential information. Over the last few years, the Department has continually pressed for the protection of confidential information and the privacy of citizens. Furthermore, we help protect commerce by enforcing the laws, including those that protect intellectual property rights, and that combat computer and communications fraud. (In particular, we help to protect the confidentiality of business data through enforcement of the recently enacted Economic Espionage Act.) Our support for robust encryption is a natural outgrowth of our commitment to protecting privacy for personal and commercial interests.

But the Department of Justice protects more than just privacy. We also protect public safety and national security against the threats posed by terrorists, organized crime, foreign intelligence agents, and others. Moreover, we have the responsibility for preventing, investigating, and prosecuting serious criminal and terrorist acts when they are directed against the United States. We are gravely concerned that the proliferation and use of non-recoverable encryption by criminal elements would seriously undermine these duties to protect the American people, even while we favor the spread of strong encryption products that permit timely and legal law enforcement access and decryption.

The most easily understood example is electronic surveillance. Court-authorized wiretaps have proven to be one of the most successful law enforcement tools in preventing and prosecuting serious crimes, including drug trafficking and terrorism. We have used legal wiretaps to bring down entire narcotics trafficking organizations, to rescue young children kidnapped and held hostage, and to assist in a variety of matters affecting our public safety and national security. In addition, as society becomes more dependent on computers, evidence of crimes is increasingly found in stored computer data, which can be searched and seized pursuant to court-authorized

thorized warrants. But if non-recoverable encryption proliferates, these critical law enforcement tools would be nullified. Thus, for example, even if the Government satisfies the rigorous legal and procedural requirements for obtaining a wiretap order, the wiretap would be worthless if the intercepted communications of the targeted criminals amount to an unintelligible jumble of noises or symbols. Or we might legally seize the computer of a terrorist and be unable to read the data identifying his or her targets, plans and co-conspirators. The potential harm to public safety, law enforcement, and to the nation's domestic security could be devastating.

I want to emphasize that this concern is not theoretical, nor is it exaggerated. Although use of encryption is still not universal, we have already begun to encounter its harmful effects. For example, in an investigation of a multi-national child pornography ring, investigators discovered sophisticated encryption used to protect thousands of images of child pornography that were exchanged among members. Similarly, in several major hacker cases, the subjects have encrypted computer files, thereby concealing evidence of serious crimes. In one such case, the Government was unable to determine the full scope of the hacker's activity because of the use of encryption. The lessons learned from these investigations are clear: criminals are beginning to learn that encryption is a powerful tool for keeping their crimes from coming to light. Moreover, as encryption proliferates and becomes an ordinary component of mass market items, and as the strength of encryption products increases, the threat to public safety will increase proportionately.

Export controls on encryption products have been in place for years and exist primarily to protect national security and foreign policy interests. The nation's intelligence gathering efforts often provide valuable information to law enforcement agencies relating to criminal or terrorist acts, and we believe that this capability cannot be lost. Nonetheless, U.S. law enforcement has much greater concerns about the use of non-recoverable encryption products by criminal elements within the United States that prevent timely law enforcement decryption of lawfully-seized encrypted data and communications relating to criminal or terrorist activity.

The Department of Justice, and the law enforcement community as a whole, supports the use of encryption technology to protect data and communications from unlawful and unauthorized access, disclosure, and alteration. Additionally, encryption helps to prevent crime by protecting a range of valuable information over increasingly widespread and interconnected computer and information networks. At the same time, we believe that the widespread use of unbreakable encryption by criminal elements presents a tremendous potential threat to both public safety and national security. Accordingly, the law enforcement community supports the development and widespread use of strong, recoverable encryption products and services.

The Department believes that encouraging the use of recoverable encryption products is an important part of protecting business and personal data as well as protecting public safety. In addition, this approach continues to find support among businesses and individuals that foresee a need to recover information that has been encrypted. For example, a company might find that one of its employees lost his encryption key, thus accidentally depriving the business of important and time-sensitive business data. Similarly, a business may find that a disgruntled employee has encrypted confidential information and then absconded with the key. In these cases, a plaintext recovery system promotes important private sector interests. Indeed, as the Government implements encryption in our own information technology systems, it also has a business need for plaintext recovery to assure that data and information that we are statutorily required to maintain are in fact available at all times. For these reasons, as well as to protect public safety, the Department has been affirmatively encouraging the voluntary development of data recovery products, recognizing that only their ubiquitous use will both provide both protection for data and protection of public safety.

Because we remain concerned with the impact of encryption on the ability of law enforcement at all levels of government to protect the public safety, the Department and the FBI are engaged in continuing discussions with industry in a number of different fora. These ongoing, productive discussions seek to find creative solutions, in addition to key recovery, to the dual needs for strong encryption to protect privacy and plaintext recovery to protect public safety and business interests. While we still have work to do, these dialogues have been useful because we have discovered areas of agreement and consensus, and have found promising areas for seeking compromise solutions to these difficult issues. While we do not think that there is one magic technology or solution to all the needs of industry, consumers, and law enforcement, we believe that by working with those in industry who create and market encryption products, we can benefit from the accumulated expertise of industry to gain a better understanding of technology trends and develop advanced tools that balance privacy and security.

We believe that a constructive dialogue on these issues is the best way to make progress, rather than seeking export control legislation. Largely as a result of the dialogue the Administration has had with industry, significant progress was made on export controls. Recent updates were announced by Vice President Gore on September 16, 1998, and implemented in an interim rule, which was issued on December 31, 1998. The Department of Justice supports these updates to export controls, which liberalized controls on products that have a bit length of 56-bits or less, and permits the export of unlimited-strength encryption to certain industry sectors, including banks, financial institutions, insurance companies, and medical facilities. These changes allow these sectors, which possess large amounts of highly personal information, to use products that will protect the privacy of their clients. We also expanded our policy to permit recoverable exports, such as systems managed by network administrators, to foreign commercial firms. We learned about these systems through our dialogue with industry, and they are largely consistent with the needs of law enforcement. In addition, the Department, in conjunction with the rest of the Administration, intends to continue our dialogue with industry, and will evaluate the export control process on an ongoing basis in order to ensure that the balance of interests remains fair to all concerned.

At the same time, the Department of Justice is also trying to address the threat to public safety from the widespread use of encryption by enhancing the ability of the Federal Bureau of Investigation and other law enforcement entities to obtain the plaintext of encrypted communications. Among the initiatives is the funding of a centralized technical resource within the FBI. This resource, when fully established, will support federal, state, and local law enforcement in developing a broad range of expertise, technologies, tools, and techniques to respond directly to the threat to public safety posed by the widespread use of encryption by criminals and terrorists. It will also allow law enforcement to stay abreast of rapid changes in technology. Finally, it will enhance the ability of law enforcement to fully execute the wiretap orders, search warrants, and other lawful process issued by courts to obtain evidence in criminal investigations when encryption is encountered.

The proposed Security and Freedom through Encryption Act raises several concerns from the perspective of the Department of Justice. First, we share the deep concern of the National Security Agency that the proposed SAFE Act would harm national security and public safety interests through the liberalization of export controls far beyond our current policy, and contrary to our international export control obligations. We are similarly concerned that a decontrol of unbreakable encryption will cause the further spread encryption products to terrorist organizations and international criminals and frustrate the ability of law enforcement to combat these problems internationally.

The second problem is that the Act may impede the development of products that could assist law enforcement to access plaintext even when also demanded by the marketplace. The Administration believes that the development of such products is important for a safe society. Unfortunately, to the extent that this provision would actually prohibit government from encouraging development of key management infrastructures and other similar technologies, the provision could preclude U.S. government agencies from complying with statutory requirements and would put public safety and national security at risk. For example, it might preclude the United States government from utilizing useful and appropriate incentives to use key recovery techniques. The government might not be able to require its own contractors to use key recovery or demand its use in the legally required storage of records regarding such matters as sales of controlled substances or firearms.

It is also important to consider that our allies concur that unrestricted export of encryption poses significant risk to national security, especially to regions of concern. As recently as December 1998, the thirty-three members of the Wassenaar Arrangement reaffirmed the importance of export controls on encryption for national security and public safety purposes and adopted agreements to enable governments to review exports of hardware and software with a 56-bit key length and above and mass-market products above 64 bits, consistent with national export control procedures. Thus, the elimination of U.S. export controls, as provided by the proposed Act, would severely hamper the international community's efforts to combat such international public safety concerns as terrorism, narcotics trafficking, and organized crime.

In light of these factors, we believe that the Administration's more cautious balanced approach is the best way to protect our national interests, including a strong U.S. industry and promoting electronic commerce, while simultaneously protecting law enforcement and national security interests. We believe that legislation that eliminates all export controls on encryption could upset that delicate balance and is contrary to our national interests.

We as government leaders should embark upon the course of action that best preserves the balance long ago set by the Framers of the Constitution, preserving both individual privacy and society's interest in effective law enforcement. We should promote encryption products which contain robust cryptography but that also provide for timely and legal law enforcement plaintext access to encrypted evidence of criminal activity. We should also find ways to support secure electronic commerce while minimizing risk to national security and public safety. This is the Administration's approach. We look forward to working with this Subcommittee as it enters the markup phase of this bill.

Mr. COBLE. Mr. Reinsch, what is the statutory authority for the regulations you mentioned in your statement?

Mr. REINSCH. The statutory authority right now is the International Emergency Economic Powers Act, because the Export Administration Act expired on August 19, 1994, and Congress has not yet renewed it. Pursuant to the International Emergency Economic Powers Act, the President declared an international economic emergency, reimposed the provisions of the Export Administration Act and our regulations by Executive Order.

Mr. COBLE. Was this statute intended to authorize an export licensing regime?

Mr. REINSCH. Yes. The Export Administration Act, which is our basic statute, dates back to 1949, Mr. Chairman. In fact, its 50th anniversary was last Friday. And it was designed to do precisely what you ask, and that is to give the executive branch authority to control exports for foreign policy, national security, and short supply purposes.

Mr. COBLE. You are saying that IEEPA wasn't intended for that purpose.

Mr. REINSCH. IEEPA was intended—Mr. Berman probably is more familiar with IEEPA than I.

Mr. BERMAN. It was intended to let the executive branch do anything that they could conceive of wanting to do that they didn't have more specific legislative authority for.

Mr. REINSCH. I wouldn't put it in exactly those terms, but he is on the right track.

Mr. COBLE. Very well. Thank you.

Ms. McNamara, is it possible that a notorious international criminal or terrorist may obtain strong encryption products from foreign sources or illegally exported from within the United States?

Ms. MCNAMARA. Yes, sir, Mr. Chairman, it is possible. It is possible. We do not disagree that there is strong encryption out there. What we are trying to prevent is the broad use of encryption, which, if the immediate decontrol of encryption or export controls were to occur, we would have broad, widely used encryption around the world.

Mr. COBLE. So you admit that there are problems now, but do you fear that the passage of this bill would exacerbate those problems?

Ms. MCNAMARA. Yes, sir, we do.

Mr. COBLE. Mr. Lee, I am told that part of the Administration's position on this matter looks for growing interest in the business community in key recovery. I am told furthermore that there may be a lack of movement or a lack of interest toward key recovery. What say ye to that?

Mr. LEE. The Administration has been working closely with industry to explore the market and other incentives both for key recovery and for a wide range of technologies. It is important to make the point that law enforcement and the Administration are not wedded to any particular technology. Key recovery is one particular technology, but there are others, and in our discussions with industry over the last year, we have learned a great deal about them.

There are other technologies that promote the balanced approach that I and my colleagues have mentioned this morning. We have seen increasing interest in these technologies. We believe some of them are promising, and as Secretary Reinsch testified, the updates to the export regulations that were announced last fall reflect in large part our ability to work with industry to seize the promise of some of these technologies which further law enforcement, public safety and other Government interests as well as being market-friendly.

Mr. COBLE. Thank you, sir. I think I can get one more question put to you before the red light illuminates.

Ms. McNamara, elaborate if you will on the Wassenaar Agreement and its effect on the Administration's encryption policy.

Ms. MCNAMARA. Sir, the encryption—the Administration's encryption policy was agreed to in September 1998. The Wassenaar Nations met and reached an agreement in December 1998. Essentially Wassenaar closed a loophole which was available to foreign nations that was disadvantaging in a way U.S. industry. I believe that is an accurate characterization. They closed that loophole, all 33 nations, the principal producers and users of encryption products in the world. So it closed a loophole that was, in some people's opinion and in the Administration's opinion, disadvantaging U.S. industry. That has happened. It is recognition that the efforts and the steps and the relaxation that the U.S. Government employed last year was in agreement with the 33 nations that signed up to Wassenaar.

Mr. COBLE. Anybody want to add to that?

Mr. GOODLATTE. Would the gentleman yield? I wonder if I might make an observation about that.

Mr. COBLE. My red light is on. Let me recognize the gentleman from California, and then I will get to you, Bob, after the gentleman from California.

Mr. BERMAN. Let me just continue on that point very quickly. I want to ask some other questions as well. Mr. Goodlatte in his opening statement says, I have just come back from France, and the French are changing their whole approach to domestic controls on encryption technology. Correct me if I am misstating you. And based on my conversations there, he predicts that their export controls on encryption technology will also be eliminated. Is France a member of Wassenaar?

Ms. MCNAMARA. Yes, sir, France is a member of Wassenaar. And I would agree with Mr. Goodlatte that what the French did was to, in fact, relax domestic controls.

Mr. BERMAN. But they did sign up to Wassenaar.

Mr. REINSCH. They have subsequently stated, Mr. Berman, that they intend to honor their Wassenaar obligation.

Mr. BERMAN. Which is 56-bit length?

Mr. REINSCH. 64.

Mr. BERMAN. 64-bit length limit.

Mr. REINSCH. Yes. But let me clarify the nature of that limit, if I may. It was one of the things I didn't have time to address in my statement. The way Wassenaar works, it doesn't mean that you can't export more than 64 bits.

Mr. BERMAN. You have to go through a licensing process?

Mr. REINSCH. Yes.

Mr. BERMAN. I understand. The thrust of your testimony other than causing people to conclude that we should indict the 205 co-sponsors for treason—

Mr. REINSCH. I was mostly responding to Mr. Rohrabacher's comments yesterday about similar subjects.

Mr. BERMAN. Right.

Mr. COBLE. If the gentleman would yield. That means the gentlelady from California, the gentleman from Virginia will be the two lead conspirators.

Mr. BERMAN. The problem is when Ms. Lofgren says, I went out yesterday and downloaded strong—I don't know if she downloaded or she saw she could click something and would be able to download strong—and I assume by strong she means 128 or higher—higher than 40, higher than 56-bit length encryption when the—you can buy a laptop computer and load it with 128 and then fly to Europe or to Afghanistan or to Iran and take that computer with that encryption technology embedded in it now.

The real question is I want to help you do what your agencies are dedicated to do, and what I can't understand is why there is any point left in doing it. I really would like you to sort of respond to that. What is the difference between a terrorist, a proliferator, a foreign government, a hostile government's ability to download encryption technology, buy it from some foreign manufacturer, take it in a computer or in just a package of software out of the United States and just buying it in a noncontrolled world that this legislation would create?

Ms. MCNAMARA. Let me just say I don't think we are ever going to prevent individuals from doing individual things and individuals taking their laptop computers or individuals being able to access things that we would prefer they not be able to do. What we are trying to do, though, is to manage the spread of encryption, not prevent it, because, in fact, we have allowed under the current Administration's policy very robust encryption to be exported when the end user was not of concern to the national security domain.

In this particular case, this bill as presented would take down all of the restrictions immediately, and we would have—

Mr. BERMAN. I thought it left some restrictions on countries on the terrorists list. I thought it left some level of restrictions.

Ms. MCNAMARA. It did, sir, but it would—they are limited because they are, I think, referred to as the pariah countries. Our concern is in our responsibility to provide support to the U.S. Government and U.S. military forces wherever they deploy or wherever they find themselves, we have to be able to do our business, and just to limit encryption export controls to that narrow set of countries would have serious impact on our ability to do that business for the U.S. Government.

Mr. BERMAN. I have a couple more questions, but I will wait till the next round.

Mr. COBLE. The gentleman from the Roanoke Valley of Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. I want to welcome all of these panelists who have become good friends of mine over the years, although we disagree on this issue. I have not had the opportunity to work with Mr. Lee much yet, but I look forward to that, and Mr. Reinsch and Ms. McNamara have come to understand each other, I think, very well on this issue.

I also appreciate the concerns that they have expressed regarding challenges the Administration is going to have to confront in dealing with encryption, but the most important point to make here is whether or not this legislation ever passes and ever becomes law, you are going to have to confront those problems because of the massive proliferation of foreign-created encryption products, of domestically-created encryption products which can be freely created and used in the United States. It is only the export control that you have any access to, and I would freely and safely predict that this country will never pass a law creating the kind of domestic control on a device to protect the privacy of American citizens that the FBI for one is calling for.

I think Mr. Berman has gotten to the heart of this matter in asking about international discussions in the Wassenaar Agreement. It is important to note that this legislation does not in any way conflict with the Wassenaar Agreement because of the reasons that Mr. Reinsch pointed out. Not only are there no limits on exportation of encryption under that agreement, they can go to any key length they want to, but there is no definition or limitation on what that export control process may be. Mr. Reinsch pointed out, in fact, the United States is allowing 128-bit encryption for banking.

Mr. BERMAN. Would the gentleman yield?

Mr. GOODLATTE. Sure.

Mr. BERMAN. But there is decontrol and the requirement to get a validated license based on a specific end user are two different—in other words, Wassenaar doesn't say you can't export it. It just says have a system which says who the purchaser is and describes what the system is. It is still a regulatory issue.

Mr. GOODLATTE. Reclaiming my time. Exactly right. And we still have a regulatory system with this legislation, and it is important to note that it isn't just those few countries and those few individuals where export controls would still apply under our bill. Our bill applies to and relaxes export controls where you have an off-the-shelf, generally available product and that software—I get criticized for not mentioning the computer—hardware industry which contains encryption as well as wireless communications, and it allows that when you have a customized product for which there is foreign competition.

But if you do not meet those two criteria, if you are a national security type encryption products, you are still fully subject to our export control laws, and we have added provisions to clarify some of the points that you pointed out, a new provision allowing the Secretary of Commerce to stop the export of specific products to specific individuals or organizations in specific countries if there is

substantial evidence that they will be used for military or terrorist purposes, and that can be any country if they are going to use it for a military purpose; a new provision for allowing the President to stop exports to terrorist nations and to impose embargoes; and a new provision giving the Secretary of Commerce a 15-day, one-time technical review of encryption products prior to export to give them the opportunity to look at the product in much the way Ms. McNamara described in her testimony.

We have also, because of our strong support of privacy of United States citizens, added provisions making it clear that encryption is a good thing. One of the things that concerns me most was Mr. Lee's—actually Ms. McNamara's statement, that they are trying to prevent the broad use of encryption. That, to me, is a very, very flawed and mistaken policy. The broad use of encryption is not only good, but vitally important to the success of the Internet and international electronic commerce and communications. The fact of the matter is if you do not have strong encryption, or if you set up this key system where billions of keys are out there, targets of terrorists and hackers, you have created the Achilles heel of our electronic communications system in the world.

So use of encryption to protect credit card numbers, medical records, copyrighted material, industrial trade secrets, financial transactions of all kinds, e-mail, and everything you can think of is vitally important, and the broad use of encryption is broadly important.

I would like to ask Ms. McNamara this question. Your predecessor Bill Crowell testified in 1997 before the House National Security Committee that the impact of key recovery on your national security mission is not significant, and that key recovery per se does not help the National Security Agency do its foreign intelligence mission. I wonder if you would comment on his remarks.

Ms. McNAMARA. Sir, I missed part of his remarks, but let me say if my answer doesn't address it, would you please repeat the statement.

For the national security—for national security purposes, key recovery is not a solution. Key recovery or data recovery in the broadest sense is, in fact, a law enforcement interest and issue and concern. For us internationally overseas we cannot present a court order and ask somebody to provide us with the information that we need to provide timely, critical decisionmaking intelligence. It just doesn't work. That is why I say—I think that is what Bill Crowell was implying when he made the statement.

There is a distinction, and as I said in my testimony, the solutions for law enforcement and the solutions for national security are decidedly different, and they have to be arrived at in a decidedly different fashion.

Mr. GOODLATTE. Thank you.

Mr. COBLE. I thank the gentleman.

The gentlelady from California.

Ms. LOFGREN. Thank you, Mr. Chairman. Just a quick comment.

Mr. Reinsch, I said nice things about you, and I was referring to your position on the export of Pentium III chips, a position I agree with. I would note also for the record that Mr. Rohrabacher, who

doesn't understand the full value of high-tech exports, is, in fact, a cosponsor of this bill.

Mr. BERMAN. That is a hurdle to overcome.

Ms. LOFGREN. A hurdle to overcome according to Mr. Berman.

In listening here, I guess one of the things I would like to say, and you don't really need to answer, is to encourage each of you, understanding that the Administration's position is in opposition to the bill, and I hope that will change, but I hope you will nevertheless come up with suggestions. I hope you will act as if this bill may become law, even though your official position is in opposition, and suggest things that we may consider to make it better or more workable—from your point of view? I am hopeful that the fact that we disagree will not preclude useful dialogue and exchange.

You know, as I think about this issue, and I do think it is important to recall that the Director of the FBI said this in last Congress, that the real issue here is the domestic control of encryption. NSA just acknowledged this. You can't go with a court order to get a key abroad. As a matter of fact, you can't get a key at all. So this is about domestic use, and I don't think the people of this country will put up for 1 minute with a key recovery system—putting aside the fact that it is technically impossible. The American people value their privacy. They are not going to allow a Big Brother Government to go in and snoop on everything they do. Nor should they.

Mr. BERMAN. Would the gentlelady yield?

Ms. LOFGREN. Yes.

Mr. BERMAN. Why couldn't you get the manufacturer of the tough encryption, high-standard software to provide a key that would allow real-time interception of foreign transmissions using that software? In other words, why doesn't it have a foreign aspect?

Ms. LOFGREN. A key is generated every time there is a communication.

Mr. BERMAN. Well, a way to—somebody is translating back all those things into, somebody said, plaintext.

Ms. LOFGREN. If I may reclaim my time, I will share with you the Administration report on this very subject that casts grave doubt on the actual technical viability of this key recovery system. I think you will find it of great interest.

One of the things I wanted to ask about has to do with where we are while this is proceeding. For years, or at least it felt like years, the Administration, both the Commerce Department and law enforcement, and the NSA, said that 56-bit encryption was good enough, that it was strong encryption. Yet last year we had a privately funded effort that broke 56-bit. Was that a surprise to you, Bill?

Mr. REINSCH. No.

Ms. LOFGREN. Okay. So then the representations earlier made were optimistic and not necessarily founded in good science. Given that, why don't we, while this bill—

Mr. REINSCH. It is one thing to say it was broken. It is another thing to apply what they did and say that it has utility for law enforcement and national security. Even if you take the most recent breaking—which I think was 22 hours, I might not be up on the latest contest, but I think that was the last one I heard about—

it doesn't do a lot for the FBI or the NSA to say a lot of computers with a lot of money, spend 22 hours, can do one message that they knew about in advance.

Ms. LOFGREN. That is an exercise for fun to show it can be done, but we have better computers that are more oriented toward breaking this. I don't want to get into it, but clearly these other computers can do a better job than kids on the Internet.

Secondarily, I think the question is why don't we move to 64-bit at least as the Wassenaar Agreement provides while we study this issue further?

Mr. REINSCH. Well, that is a question that is under discussion right now inside the Administration. What we decided to do in December was to simply implement firsthand what the Vice President announced so there would not be any further delay. You may recall, somewhat to my personal embarrassment, there was a long delay between the bank announcement and the bank reg, and I wanted very much to avoid that. So we decided first to do what the Vice President had announced and address Wassenaar issues later. We are now in the midst of doing that, but I couldn't tell you what the outcome will be.

Ms. LOFGREN. Mr. Chairman, I know the red light is on, and I won't ask for this answer, but—

Mr. COBLE. Go ahead. You have put a lot into this. We are okay timewise.

Ms. LOFGREN. I wanted to ask Mr. Lee, and he doesn't have to say this now, if he can provide to the committee in writing later, what he referenced in his testimony, that there would be other technologies available to us. I hear that a lot from various voices within the Administration as if, you know, the high-tech community has a rabbit, that if they can just pull that rabbit out of the hat, that would solve the problem. I haven't found this rabbit. I don't know where that rabbit is hiding. So I would like to know specifically which technologies you were referring to in your statement, Mr. Lee. And I will take my answer in writing, hopefully within the next couple of weeks, rather than take up my time after it is expired.

Mr. LEE. If I may, Mr. Chairman, I was responding to the chairman's question about key recovery, and the specific point I was making, perhaps not with success, was that as Secretary Reinsch had referred to, there are many technologies that aren't, strictly speaking, key recovery that do promote the interest of law enforcement as well as other Government interests.

Ms. LOFGREN. And I would like to know specifically what you have in mind with that statement.

Mr. LEE. Very well.

Mr. COBLE. Give that to us in detail if you will, Mr. Lee. I thank the gentlelady.

[The information referred to follows:]

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, DC, April 14, 1999.

Hon. ZOE LOFGREN,
House of Representatives, Washington, DC.

DEAR CONGRESSWOMAN LOFGREN: During Associate Deputy Attorney General Ron Lee's March 4, 1999 testimony before the Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary, you asked him to write to you to identify those encryption technologies in addition to key recovery that promote the interests of law enforcement.

First, I would like to thank you for your continuing interest in this topic. You will recall that you exchanged letters on this matter with former Principal Associate Deputy Attorney General Robert S. Litt just last summer and fall. In his letter to you of September 24, 1998, Mr. Litt indicated that what law enforcement needs is, quite simply, access to the plaintext of encrypted data and communications when it has lawful authority to obtain that plaintext. He also indicated that law enforcement was not seeking a one-hundred percent solution, but workable solutions that support the continued ability of law enforcement to conduct judicially authorized searches for data and interceptions of communications.

Critics of law enforcement often insist that its demands are unattainable. However, there is nothing unattainable about industry's developing products and services that protect not only the security of encrypted data and communications but also the security and safety of the persons using those products and the public, at large. It is important to remember that the goal of providing law enforcement with access to plaintext is the safety of the public.

We recognize, of course, that industry is responsible for designing and deploying information technologies, including encryption products, and that it must do so in a competitive marketplace. Both industry and Government have learned that there is a market demand for products allowing access to plaintext (e.g., businesses that need to ensure the availability of data). In addition, creating a technological environment that directly, even if inadvertently, supports criminal activity by enabling criminals to act with impunity is not good for the public, industry, or the marketplace. While we are asking that industry use its creative genius to create smart solutions, those solutions will, in the long run, promote both public safety and commerce.

In this regard, industry has engaged in active discussions with law enforcement about technical solutions that might help address law enforcement's concerns. For example, a number of companies suggested to us that for some network-based encryption products there may be points in the network where plaintext exists, or where encryption can be disabled by a system administrator in response to a court order. Other products, such as corporate encryption systems, by their very nature, tend to be operated by corporate computer or network administrators, who can otherwise provide law enforcement with access to plaintext when such access is lawfully authorized. Still other products provide each individual user with the option to activate "recovery" for stored data, so that if the user loses his key, he need not also lose his data (such "recovery-capable" products tend to use key recovery). Each of these types of products helps to meet the needs of law enforcement. And these are just three possible solutions out of a panoply that are being or may be developed by industry.

You may recall that the Administration updated its encryption export control policy in 1998, taking into account the benefits of such products for public safety worldwide. For example, "recoverable" products are approved for export to foreign commercial firms in over 40 countries. A number of companies thereafter cited firms update as an excellent example of how industry and Government can work together to find workable solutions.

Of course, the needs of public safety are just one of the many interests to be considered in the encryption debate. The Department of Justice supports the use of strong encryption for legitimate purposes, such as the protection of privacy, proprietary and financial information, and intellectual property, as well as combating fraud and securing electronic commerce. Based on our discussions with industry, we are hopeful that it will develop more solutions that meet these needs and also protect the safety of the public in general.

I look forward to continuing to work with you in this important area.

Sincerely,

DENNIS K. BURKE, *Acting Assistant Attorney General.*

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, DC, May 21, 1999.

Hon. ZOE LOFGREN,
House of Representatives, Washington, DC.

DEAR CONGRESSWOMAN LOFGREN: Thank you for your letter of April 22, 1999, to Associate Deputy Attorney General Ronald Lee, concerning a letter to you from Acting Assistant Attorney General Dennis K. Burke of the Office of Legislative Affairs, dated April 14, 1999. Your letter notes that the April 14th letter, which responded to a question which you asked Mr. Lee during a hearing on March 4, 1999, was signed by Mr. Burke and not Mr. Lee. It has been the Department's longstanding policy that letters from the Department to Members of Congress, other than matters concerning constituent correspondence, are generally signed by the Assistant Attorney General for Legislative Affairs.

The substance of your letter relates to the question you asked Mr. Lee on March 4th, regarding technologies other than key recovery that promote the interests of law enforcement. The April 14th letter described these technologies, such as encryption products under the control of system administrators and products where plaintext exists at some point in a network. Your letter indicates that you consider the April 14th response to be inadequate. But it is difficult to go much further and identify either particular products or particular proprietary implementations of the technologies that were described, if you are in fact requesting that Department of Justice do so.

The Department of Justice should not of course, endorse particular products, and it is, therefore, inappropriate for the Department to specify particular products as meeting law enforcement needs. Any list of such products in today's dynamic marketplace would also surely leave some out, which would be unfair to the excluded products and manufacturers.

Moreover, although many products promote the interests of public safety more than do products that provide individual criminals with strong, unbreakable, and non-recoverable encryption under their exclusive control, the distinctions are generally of degree. Most products that, as a general matter, promote the interests of public safety can also be used in ways that harm public safety. For example, as indicated in our April 14 letter, products in which the encryption facility is under the control of a system administrator promote the needs of public safety. In such cases, law enforcement can present a court order to the system administrator, who can then disable the encryption facility or otherwise provide law enforcement with access to plaintext. However, if the organization is itself corrupt, or the system administrator is suspected of criminal activity, law enforcement will often be unable to obtain plaintext, and crime may go unpunished.

Therefore, for most products, it is overly simplistic to label them as either meeting the needs of public safety or not. (Some products will meet the needs of law enforcement in the vast majority of cases, particularly products that provide for recovery by third parties under all circumstances.)

But it is possible to describe the needs of public safety and to discern therefrom those types of technologies that support to some degree, those needs. As the April 14th letter indicated, quoting an earlier letter to you from former Principal Associate Deputy Attorney General Robert S. Litt, what law enforcement needs is access to plaintext when it has lawful authority to obtain that plaintext. Technologies that support that end support public safety. The April 14th letter identified such technologies—such as network-based encryption, encryption where plaintext remains available at some point accessible to law enforcement, and corporate encryption systems under the control of system administrators. Each of these technologies provides, in many cases, a contact who is not the target of an investigation where law enforcement can go to obtain plaintext.

Of course, different companies have different names for these types of technologies. For example, without endorsing the particular products at issue or excluding any other products, we note that thirteen high-tech companies announced in July 1999 their support for "operator action" or "private doorbell" products, which, according to those companies, would balance the needs of privacy with the needs of law enforcement. See <http://www.t-b.com/ans>. The Department of Justice is encouraged by industry's continuing efforts to meet the needs of public safety.

I hope you find this letter responsive to your inquiry. We in the Department look forward to continuing to work with you to address your concerns.

Sincerely,

JON P. JENNINGS, *Acting Assistant Attorney General.*

Mr. COBLE. The gentleman from California, Mr. Rogan.

Mr. ROGAN. No questions, Mr. Chairman. Thank you.

Mr. COBLE. The gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Yes, thank you, Mr. Chairman.

Just an observation about remarks by both Mr. Goodlatte and Ms. Lofgren about domestic control. I concur there is no way that there will ever be domestic controls on encryption technologies in this Nation. And I think what really struck home to me when I heard those remarks is that I just left a hearing in another subcommittee on which I serve dealing with a regulation promulgated by the FDIC entitled "Know Your Customer." I see people nodding their heads in the affirmative. It had to do—they rescinded it, or I understand they intend to rescind it. It would mandate banks to profile their customers to determine whether they may be engaged in any criminal activity. One hundred thirty-five thousand comments were forwarded to the FDIC, and the comment phase isn't even over yet. And Americans everywhere are concerned about privacy.

I mean, I think this is something particular to a democracy because once you start to reduce privacy, you tend toward something that none of us want to conceive of in terms of the kind of society we are about. So dealing with that reality, there are no domestic controls. And what I hear everybody suggesting here is that—I think it was Mr. Berman—all you have to do is download an encryption technology which you can purchase in this country, the strongest possible encryption technology, download it or go to wherever they sell it. You can get on a plane and bring it to wherever you want to go in some foreign nation, or better yet, you can just sit in the comfort of your own home, put it in your laptop computer, hit a button, and it is there.

I mean, given that reality, and we all do share these concerns about criminal syndicates and terrorists and rogue nations looking for the technology, but I respectfully suggest, and maybe I am being too simplistic, maybe I am being simple-minded, but it appears to me that the position that you are putting forth here today is reminiscent of the Maginot Line. I mean, this is not, you know, a finger in the dike. There is no dike. I mean, it is out there. If they want to get it, they are going to be able to secure it.

I spent 21 years as prosecutor in a major jurisdiction. I know that if they want to get it, they are going to get it. They are not going to be concerned about export licenses. That is the last thing that they are going to be concerned about. They don't know anything about the Wassenaar Arrangement. They are just going to get it, and it is available, and I share the concerns, but meanwhile we are impeding American industry.

Mr. Reinsch, you talk about a balanced approach. Well, I am looking at panel one. I bet there aren't too many there who would agree that our position now is balanced. We are just losing. I yield back.

Mr. COBLE. I thank the gentleman. And because of the obvious interest on the part of the subcommittee, I am going to go to a second round. Mr. Goodlatte, if you would assume the Chair. I am going to have to go to my other meeting, and then we will go into a second round of questioning. Thank you again, and I apologize

to the second panel. I may be back before you all conclude, but I may not.

Mr. GOODLATTE. [Presiding.] Thank you, Mr. Chairman. I think we should proceed to a second round of questions since I have a few, and several members of the committee do as well.

Secretary Reinsch, I was pleased to hear you say that the Administration is not seeking controls or restraints on domestic manufacture or use of encryption. Does that mean that if a domestic access amendment, such as the Oxley-Manton amendment offered and defeated in the committee at the last Congress, or the domestic provisions of the Intelligence Committee substitute amendment adopted by that committee, is considered this year by any committees that receive a referral of this bill, the Administration will publicly state its opposition to such an amendment?

Mr. REINSCH. Well, that is a multipart question, Mr. Chairman.

Mr. GOODLATTE. We will take each one at a time.

Mr. REINSCH. As I recall, we did not support the Intelligence Committee's bill last year—or 1997, and said so, as I recall, at the time. I don't recall whether or not we had a position on Oxley-Manton. Frankly, I am not sure I recall all the details of the amendment.

I am glad you made your initial statement, because I was going to comment with respect to Mr. Delahunt's point that the Administration position is that we do not seek and are not seeking domestic controls on manufacture or use. Were there to be an amendment or a bill that would impose such controls, I would certainly hope and expect that we would say that we oppose it, but I don't think we would address that question until the amendment actually rolled around and was on the table for us to look at.

Mr. GOODLATTE. The reason I ask is in March 1997, you stated the Administration was not seeking domestic controls over encryption, which seemed to be the case until September 1997, when the FBI pushed for adoption of the Oxley amendment, and the FBI and NSA pushed for adoption of the intelligence committee substitute. The Administration was then eerily silent on the domestic control issue, which caused a great deal of confusion about your actual position.

I would also like to note that although you dismiss the SAFE Act prohibitions on domestic controls as unnecessary, a statutory prohibition would certainly eliminate any confusion caused by multiple Administration positions on the issue.

Mr. REINSCH. It would certainly obviate this line of questioning. There is no question—no doubt about that.

I think I can say with confidence that what I have said speaks for the Administration, and I would like to point out that I think I have been consistent from your recitation of prior quotes. I hope we will continue to be consistent.

You are asking me, though, a difficult question, which is to make a commitment about language that doesn't exist yet and may never exist. Obviously, if there were such a proposal again from either of those committees, we would have to look at it before making a final decision, but our position on this, I think, is clear.

Mr. GOODLATTE. Mr. Reinsch, when you testified before this subcommittee last Congress on this same subject, you stated the Ad-

ministration was attempting to nudge the market toward key recovery because you believe that the market was going in that direction on its own. Are you still trying to nudge the market toward key recovery?

Mr. REINSCH. With respect to stored data, Mr. Goodlatte, we believe that is what is happening. We believe the market is moving in the direction of key recovery for stored data, and we find demand out there.

Mr. GOODLATTE. But on a voluntary basis?

Mr. REINSCH. Sure.

Mr. GOODLATTE. Under certain circumstances, and I would say wisely, some people may want a second access to a key. If they lost it, they would lose all of that data.

Mr. REINSCH. For reasons that have nothing to do with either law enforcement or national security. I refer you to the sentence in my testimony about one of the things we have learned since my last testimony is the perils of one-size-fits-all policymaking, and we have begun to conclude that this is a problem that is best dealt with in pieces rather than with a unitary approach.

Key recovery we think is a good solution for stored data, and because it is a good solution, people are going to it anyway regardless of anything we say or do. We are discovering that it is not going to be a preferred solution for transient data or e-mail, but as Mr. Lee mentioned in his testimony, there are other technologies that are law-enforcement-friendly in that area as well.

Mr. GOODLATTE. Let me ask Mr. Lee the same question. Do you or the Justice Department agree with Secretary Reinsch's statement that the Administration is not seeking controls or restraints of the domestic manufacture or the use of encryption?

Mr. LEE. The Administration's policy, which has been stated consistently, is that we are not seeking controls, mandatory controls, on manufacture or use or distribution of encryption.

Mr. GOODLATTE. Is that Administration policy consistent with the FBI and the Director of the FBI's policy with regard to the use of encryption?

Mr. LEE. Sir, I don't have in front of me the specific statement of the Director you are referring to. The Director has long expressed a very deep concern, which the Department of Justice shares, about the consequences of the widespread proliferation of encryption that does not provide a means of lawful access to plaintext.

Mr. GOODLATTE. Mr. Reinsch, you stated in 1996 before the Senate that 2 years is the outside limit within which if we do not address this encryption problem, the technology will take over, and the opportunity to address it will have gone. It is now 3 years later, and according to Secretary Daley, there are now over 650 encryption products on the market. Aren't we now in a situation in which the technology has indeed taken over?

Mr. REINSCH. I don't think so yet. I recall that statement. I must say I am impressed, Mr. Goodlatte, that someone is reading my testimony. That is always encouraging to hear.

I have been consistent; I am generally wrong when I predict things are going to happen by a certain time, as anybody who has

ever asked me a question about when we are going to issue a regulation knows very well.

I think that is an important question because it relates to some comments that both Mr. Delahunt and Ms. Lofgren made as well as the point Mr. Berman made, and that is we would draw a distinction between the existence in the marketplace of products and their actual use in the marketplace.

The data that Secretary Daley was referring to that you cited was data that Trusted Information Systems published periodically when it was an independent company, the last iteration of which was December 1997, that said there were 656 products available from foreign sources. Without commenting in detail on the comparability or their level of robustness, that is still a large number, and I have no doubt it is a bigger number today than it was then, and the point is correct, we are heading in that direction.

As Ms. McNamara pointed out in her testimony, and as I would point out, there is a significant difference between the existence of the products and their actual use. We have found over the years and are still finding that use lags behind availability, if you will, in this area significantly because of trust and interoperability reasons.

Mr. GOODLATTE. Thank you. My time is expired.

Gentleman from California, Mr. Berman.

Mr. BERMAN. Thank you, Mr. Chairman.

Privacy is very important, as others here have talked about, but it is not an absolute interest. I mean, we accept that under a warrant, our law enforcement agencies can intercept and wiretap telephones. I think most of us—I certainly am very concerned that be it on a very limited basis, it be authorized, reviewed by a third party, a judge, but we do allow that compromise.

I do not want to be involved in something that significantly hurts our ability to intercept communications of the kind that was spoken about by the NSA. My problem is having a hard time understanding whether the concern is a theoretical one at this particular time, or is it a real one; and is this about export controls, or is this about getting the cooperation of the developers of the encryption software to let you in on the secret, so to speak, in some fashion, whether it is key recovery or some new technology.

Mr. Lee says the Department of Justice supports the spread of strong recoverable encryption. From that I would conclude that he would therefore be eliminating all export controls on any encryption which is recoverable. Is that a fair conclusion?

Mr. LEE. That is not an issue that the Administration has confronted at this time. Again, as I said in my written statement and as well in my verbal statement, the law enforcement community, and that includes State and local as well as the Federal law enforcement agencies, are very concerned about the dual impact on public safety and national security of an incredibly widespread proliferation of encryption abroad.

Mr. BERMAN. Then why do you say you support the spread of strong recoverable encryption?

Mr. LEE. We do.

Mr. BERMAN. Well, that to me means you don't support controls on strong recoverable encryption. Controls limit the spread.

Mr. LEE. Excuse me, sir. I think the key goes back to a statement that Secretary Reinsch made, which is there is a difference between availability and widespread use. What the Department of Justice and law enforcement ultimately will need is when strong encryption is available in a widespread way internationally, a way, whether it is key recovery or another way, to present lawful authority and be able to obtain plaintext. So you have to look both at the immediate consequences of decontrol, which is what you are asking me about, versus the end stage that—law enforcement and I think our foreign law enforcement allies would agree with this—the end stage which is we all want to have strong encryption in widespread international use. We want that to be done in a way, in a system, in an implementation with the proper doctrine and services that support law enforcement objectives.

So I would draw a distinction between what will immediately happen if H.R. 850 is passed versus the end stage, which absolutely we support, which is the widespread use of strong encryption both domestically and abroad that support the law enforcement interests.

Mr. BERMAN. The banks. You talked about the banks. You have let the banks export to—you allowed export of very strong, I take it, 128—

Mr. REINSCH. Or more.

Mr. BERMAN [continuing]. Or more without-limit encryption technology because?

Mr. REINSCH. Because we concluded two things: One, the need to secure safety of electronic financial transactions was a paramount consideration in our policymaking; and second, because financial institutions are highly regulated institutions in virtually every country in the world and have a long history of effective cooperation with law enforcement anyway, and we didn't think that some of the constraints that we have applied in other sectors were necessary.

Mr. BERMAN. Could you turn that into a more practical answer, because the banks will share with—

Mr. REINSCH. Yes.

Ms. MCNAMARA. Mr. Berman, may I comment? Is that Mr. Reinsch's red light or yours?

Mr. BERMAN. It is mine. I can't talk, but you can comment.

Ms. MCNAMARA. Banks have always enjoyed special treatment under export controls. We have always allowed banks to have robust encryption because we recognized the banking industry is important to everyone's national security. And so even in the days when 56-bit data was controlled, banks had access to that. And it is recognized because it is so important to our infrastructure.

Now, I would like to, if I may also, I would like to comment again on the issue of availability. We do not argue that encryption is available both here in the U.S. and in foreign markets. We just don't. But because encryption is our business for national security purposes, we pay attention to what is going on in the foreign marketplace in terms of actual use.

We do not see lots and lots of encryption being used in a widespread fashion. I mean, as I said, militaries and governments have always used it. They have always used it for confidentiality, but

the rest of the world is largely still today using unencrypted communications—not using encryption for transmission of their information.

Now why is that? We maintain that we will see widespread encryption used when three conditions are met. Those conditions are when it is inexpensive, and it is becoming very much so; when it is easy to use, and depending upon what you are trying to download, it is more or less easy, but it is not consistently easy everywhere; and it will also become easy—it will also become used in widespread fashion when there is an underlying security management infrastructure which allows the exchange of key across international borders or between two different organizations or industries.

Those do not exist today. So while someone can download it, and while it is inexpensive in some cases, there are not robust international security management infrastructures that will allow it to be used, and that is—and in answer to your question about is it a matter of export or isn't it, it is a matter of licensing so that we can understand how it is going to be used and who the intended end user really is. And that is what the relaxation that the Administration put in place this past September was intended to do. It identifies end use. It identifies areas that need to be protected, and it recognizes that gradual relaxation makes sense in certain areas.

Mr. GOODLATTE. The gentleman from California, Mr. Rogan.

Would the gentleman yield to me for a few seconds?

Mr. ROGAN. I yield to the chairman.

Mr. GOODLATTE. In response to that, I would like to point out while I was in Britain, a software manufacturer demonstrated a 128-bit software program that is going to be on-line dealing with the use of digital signatures in a matter of a few months that I think will become the industry standard worldwide. It is a fascinating thing. But anyway, the cost of the encryption in that program is less expensive than the cost of the screensaver in that program. We are just talking about a mathematical algorithm. It is not a very expensive technology.

Mr. BERMAN. Would the gentleman yield for just a short response to that?

Mr. ROGAN. I yield to the gentleman.

Mr. BERMAN. I think the witness Ms. McNamara was talking about, in the third part of her answer, the lack of the information management infrastructure; something about you could get it easy, but you can't do that much with it unless something is happening—I am not quite sure what you meant, but there was a third part to that.

Mr. GOODLATTE. The gentleman from California is recognized.

Mr. ROGAN. I was going to ask if I could have my time back.

Mr. GOODLATTE. If there is no objection.

Mr. ROGAN. Actually I won't need that much time, Mr. Chairman. Thank you.

I want to apologize to all of the witnesses today for not being present for all of your testimony. Regrettably I have two competing markups in other committees, so I feel like a wishbone being pulled in both directions.

As to Director McNamara's point that she made a few minutes ago that actually did raise one question in my mind. It is true that foreign encryption products can be downloaded easily. There are, I think, last survey I saw, some 600 different products available. And so I guess my question for you, Director, is our national security enhanced or hurt by a market that is dominated by United States-made encryption products rather than foreign encryption products?

Ms. MCNAMARA. Our position has been consistent in that regard, Congressman, and we have always said that national security needs a strong U.S. presence overseas.

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

Mr. GOODLATTE. Thank you.

The gentlewoman from California, Ms. Lofgren.

Ms. LOFGREN. It seems to me that really what we are risking here is the lost domination of cryptography by Americans by this prospective delay of unknown duration. We may not be able to facilitate encryption becoming more endemic than it is—in terms of use. What is worse is that the smart criminals have ready access to strong encryption. The smart criminals, presumably, will use what they need. It is only the dumb criminals who won't—until it is endemic. I really think it is not a good trade to risk our domination of this sector, both for economic and for security reasons and for such a modest goal. At least, that is just my opinion.

Now I have a question for Mr. Reinsch. It is something I wondered a long time about. Maybe the answer is obvious. But I have wondered about our current policy that throws crypto with a hole into the whole export control regime. I don't understand how we can throw crypto with the hole into the scheme since we are not actually exporting the material. What is the legal basis for the current policy in this regard?

Mr. REINSCH. Well, the act gives us broad authority to license exports for national security, foreign policy and short supply purposes. There is no question if we include that kind of product or any kind of product that has national security or foreign policy consequences, that we have authority to cover it. It may be more a question of whether it is wise to do so. In fact, we have permitted the export of some of those products.

I am not sure where you are going. I am not aware that there is any current controversy about that, but maybe I am missing something.

Ms. LOFGREN. The final question I have, and since I want to hear the next panel, I am just going to make this the last question. I understand that the NSA opposes the bill. We don't need to go over that ground again, but within the bill there is a 15-day period to review what is being exported. What is your comment on that provision? If this bill were adopted over your objection, would you offer improvements to that section of the bill that would make this, in your judgment, a better piece of legislation?

Ms. MCNAMARA. Well, for the record, let me say that we have never believed that legislation is necessary because we can do what we need to do in the regulatory process. The amount of days is not at issue. In fact, some licenses are approved today in 15 days. It is the complexity of particular product that we need to understand in terms of how it is going to be used and essentially, if it is going

to be used in a network, how that is going to be used, and I don't know how to bound that in terms of time. I can't say that a very complex product could be understood by us in sufficient detail to allow us to be able to vote in or to approve or disprove in that time frame.

Ms. LOFGREN. In the bill you don't have approval authority if it is in the marketplace. The question really is and you don't have to answer now, is should it be 15 days, or 20 days, or a number of days as a function of the length of key, or whatever? I would be interested in your response to this question, and I would be happy to take your answer in writing later, and I yield back the balance of my time.

[The information referred to follows:]

NATIONAL SECURITY AGENCY,
Fort George G. Meade, MD, July 30, 1999.

Hon. ZOE LOFGREN,
House of Representatives, Washington, DC.

DEAR MS. LOFGREN: When I testified at the hearing on the Security and Freedom Through Encryption (SAFE) Act, H.R. 850, held by the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, you asked me to provide in writing comments on the provision of the bill that allows a 15-day period to review a product prior to export.

National security interests require a meaningful technical review of an encryption product prior to export. Fulfilling that requirement generally is not a function of the time allotted for such a review. Our experience has shown that we can conduct a meaningful technical review in a relatively short time period, such as 10 days, if all the necessary technical documentation is submitted with the export application. However, delays in the technical review arise when the applicant fails to provide all the required technical information.

It is difficult, if not impractical, to bound a review in terms of a specific time period. The complexity of the product and the provision of all necessary technical documentation are the key factors in completing a review as quickly as possible.

BARBARA A. McNAMARA, *Deputy Director.*

Copy Furnished:

Honorable Howard Coble
Chairman, Subcommittee on Courts
and Intellectual Property
House Committee on the Judiciary

Mr. GOODLATTE. Would the gentlewoman yield?

Ms. LOFGREN. Yes.

Mr. GOODLATTE. I just want to make the point, and I think you would agree with me, legislation may not be necessary if the Administration's policy was changed as well. I think that is the whole point of the legislation.

The gentleman from Massachusetts.

Mr. DELAHUNT. I just have one question I will direct to Mr. Lee because I really want to be clear about this. When you indicate—and I think we have heard from everybody on the panel regarding domestic controls and that there is no intention and no desire to impose any domestic controls. You are here representing the Department of Justice, and presumably that is also the position of the Federal Bureau of Investigation. Will you agree with that statement?

Mr. LEE. Yes, it is.

Mr. DELAHUNT. Thank you.

Mr. LEE. Mr. Chairman, if I may, I realize that I may have not fully understood Mr. Berman's question about policy with regard to the export of fully key-recoverable products, so I would just like to clarify for the record that the current export regulations do permit and encourage the development and export of key-recoverable products, and as Secretary Reinsch mentions in his written testimony, we have actually streamlined that process to eliminate the need for a prior review of the key recovery agent. So I just wanted to clarify that part of my remarks.

Mr. GOODLATTE. I want to thank the members of this panel for their contribution. We look forward to working with you as this legislation works its way through the process, and we welcome your ideas along the lines of Ms. Lofgren's questions. If you do have suggestions to improve the legislation, we certainly want to consider those, and we thank you again for your participation today.

Mr. GOODLATTE. Our second panel includes a number of distinguished witnesses including Tom Parenty, who has been active in the cryptography and computer security field for over a decade, starting with his tenure at the National Security Agency in the early to mid-1980's. While at the NSA he worked on the security of global nuclear command and control networks, focusing on the formal verification of cryptographic protocols and internal computer access controls. In addition, he also advised the Director of the NSA on internal NSA computer security issues.

Mr. Parenty has worked on the security design of operating systems, networks, and database management systems for Government agencies including the Central Intelligence Agency, the Defense Intelligence Agency, and the Air Force, as well as many U.S. computer vendors.

Currently, Mr. Parenty directs all data and communication security development activities at Sybase. He holds a bachelor's degree in philosophy from the College of Holy Cross and a master's degree in computer science from the University of Massachusetts.

I would like to recognize the gentleman from California for the purpose of introducing our second witness.

Ms. LOFGREN. Thank you, Mr. Chairman. I am happy to introduce Craig McLaughlin, who hails from my district in San Jose, California, Silicon Valley. Craig is the chief technology officer for Privada, Inc., of San Jose. He has been involved for the last 9 years in defining, developing and supporting diverse quiet server applications, particularly in the area of systems administration and security. He is the inventor and main developer of the patent-pending Privada technologies, and prior to funding this firm, Mr. McLaughlin held development leadership positions at Concentric Network and also Andol, two wonderful companies in Silicon Valley. It is a pleasure to recognize such a star from San Jose. Thank you.

Mr. GOODLATTE. Sounds like we have a vote. Let me finish introducing the panelists, and then we will recess for a vote.

Our third witness is Grover Norquist, president of Americans for Tax Reform, a coalition of taxpayer groups, individuals, and businesses opposed to higher taxes at both the Federal and State levels. ATR organizes the Taxpayer Protection Pledge, which asks all

candidates for Federal and State office to commit themselves in writing to oppose tax increases.

Mr. Norquist is a native of Massachusetts and has been one of Washington's most effective issues management strategists for over a decade. Mr. Norquist served on the National Commission on Restructuring the Internal Revenue Service and writes the monthly column "Politics" for the American Spectator.

Mr. Norquist holds a master's of business administration and a bachelor of arts degree in economics, both from Harvard University.

Our next witness on this panel is Dorothy E. Denning, who is a professor and member of the advisory board of the Communication, Culture and Technology Program at Georgetown University. Professor Denning's current research encompasses the areas of information warfare and assurance, encryption policy and technology, and the impact of technology on law enforcement and society. She is teaching courses on information warfare and security, cryptography, and data communications and is cochair of the Georgetown Project on the future of the university.

Professor Denning is an ACM fellow and recipient of the Distinguished Lecturer in Computer Security Award. She received A.B. and A.M. Degrees in mathematics from the University of Michigan, and a Ph.D. degree in computer science from Purdue University.

Our next witness is Alan Davidson, who is staff counsel at the Center for Democracy and Technology, a Washington, D.C., non-profit group working to promote civil liberties on the Internet and other new digital media. Mr. Davidson is currently leading CDT's efforts to promote encryption policies that protect privacy and free expression in the information infrastructure. He has written and spoken widely on the civil liberties implications of public policies that restrict encryption.

Mr. Davidson attended law school at Yale, where he was symposium editor at the Yale Law Journal. He remains active in MIT alumni affairs and recently completed a 4-year term as a trustee of the MIT Corporation.

Our next witness is Ed Gillespie, who serves as executive director of the—at the Americans for Computer Privacy, a broad-based coalition working to ensure that the privacy of all Americans' confidential files and communications is preserved and protected in the information age.

Mr. Gillespie worked over a decade for House Majority Leader Dick Army in a number of positions, including serving as Republican Staff Director of Congress's Joint Economic Committee and Policy Communications Director at the House Republican Conference. Roll Call newspaper listed him as one of Congress' 50 most influential staffers 3 years in a row.

Ed is a New Jersey native and a graduate of the Catholic University in Washington, D.C.

The final witness on this panel is the Honorable Dave McCurdy, who was elected president of the Electronic Industries Alliance in October 1998. When I talk about the fact we have not just software products, but lots of hardware products, it is those consumer electronic manufacturers and other business electronic products that his industry represents.

As the Alliance's chief executive officer, he oversees the activities of a national trade organization representing the full spectrum of U.S. manufacturers in the more than \$500 billion electronics industry. The Alliance, with a budget of over \$50 million and a staff of 260, is headquartered in Arlington, Virginia, and represents manufacturers whose products range from small electronic components to the most complex system used by defense, space, and industry, including the full range of consumer products.

Mr. McCurdy came to EIA after a distinguished career in the United States House of Representatives for 14 years and as chairman and chief executive officer of the McCurdy Group, a successful business consulting and investment practice. He was the first recipient of the University of Oklahoma's Distinguished Service Award in 1992. In 1984, he was named one of the 10 outstanding young men in America by the United States Jaycees. Among his numerous other honors include the Association of the U.S. Army Distinguished Service and Commander in Chiefs Awards, and the U.S. Air Force Association Kramer Memorial Award. He was selected the 1993 outstanding legislator by the Senior Army Reserve Commanders Association. In 1994, he received the PTA's National Award for Child Advocacy and the USO's award for his commitment to improving education.

The former Congressman, who has paid me nothing for this introduction, is a graduate of the University of Oklahoma law school. He also studied international economics at the University of Edinburgh in Scotland as a Rotary International graduate fellow. Prior to his election to Congress, he was an assistant State attorney general in Oklahoma and practiced law in Norman.

We have written statements from all of the witnesses on this panel, and we will look forward to hearing their statements before the committee when we return from this vote. Thank you.

We are in recess. This is final passage of the disaster bill. We have 10 minutes left for anybody who cares.

[Recess.]

Mr. GOODLATTE. The subcommittee will reconvene, and we would be pleased to recognize Mr. Parenty for his oral statement.

**STATEMENT OF THOMAS PARENTY, DIRECTOR, DATA &
COMMUNICATIONS SECURITY, SYBASE, INC.**

Mr. PARENTY. Thank you, Mr. Chairman. Good morning. Actually, good afternoon. I am speaking today on behalf of the Business Software Alliance, which is an association of leading U.S. software and hardware vendors, including Lotus, Network Associates, Intel and Microsoft, as well as my own company, Sybase, and I would like to say we have complete and absolute support for the SAFE Act, and we encourage this committee to endorse that act as it is.

I would like to begin my comments by saying I do actually think export controls are an effective means of addressing national security interests in certain cases, specifically where the technology in question is of limited availability, where the United States essentially has a monopoly. That is not, however, the case with encryption. Foreign encryption, well-designed, well-implemented and strong, is widely available and widely used today.

To illustrate my point, I am going to use one foreign encryption vendor as an example, a company named Baltimore. In the slides over on the side, you will see screen shots from Baltimore Technologies' Web site. In an effort to try to reduce the number of headaches that my colleague at the computer had to go through to set this up, I am using screen shots as opposed to using a direct Internet connection. However, I would be more than happy after the hearing to tour this site with any member or staff, live.

Baltimore is an Irish company that has components in the U.K. and Australia, as well. They have customers, and so this speaks to use, not availability, in 40 countries worldwide. As we look at the next screen, you can see that they—in a somewhat fuzzy way, have a wide variety of products from basic cryptographic building blocks to tools that can be used for securing e-mail. However, I would like to bring your attention to one product in particular, their secure Web product which, as it clearly states, they, unlike U.S. companies, have the ability to export 128-bit encryption worldwide. Their product can also be used in conjunction with weakened encryption in exported U.S. products to bring the encryption level in browsers and Web servers up to the 128-bit level, essentially negating the intended purpose of the current export controls we have in place.

The last slide I would like us to look at is one where users anywhere in the world with a simple few mouse clicks can download a number of different cryptographic products for evaluation and subsequent purchase. It is as easy as that. We are not talking about products of questionable value or questionable quality. These are products from a \$50 million company, whose technology was used just this past September by President Clinton to authenticate a trade agreement with the Republic of Ireland.

It is clear that cryptography is not just desirable, but critical in a number of different areas. I want to mention only two. The first is with respect to the protection of our national infrastructures. When I was working on the President's Commission on Critical Infrastructure Protection, my working group came to the very significant conclusion that the protection of the infrastructures upon which our Nation depends are not restricted to our national borders. They are rather infrastructures that are worldwide. And so, any policy that discourages or prohibits the deployment of strong cryptography worldwide to protect those infrastructures is not in our national security interest.

Another area in which cryptography is critical is electronic commerce. Most people think of electronic commerce as people buying CDs and books over the Internet, but I want you to think about it in a different context, that is business-to-business commerce, the use of the Internet to allow businesses to form new partnerships for the development of products and services.

I want to give you one example. A Sybase customer, MGM, does collaborative film editing with a partner in the U.K. They have a lab in Hollywood and a lab in London. They share video and audio clips as well as other information that is used for the production of feature films. They built this application a few years ago before the Internet was what it is today, and they built it on a very expensive private network. They would like to move to the Internet to take advantage of the increased flexibility as well as the de-

creased cost that would result from that; however, they will only do that if they can do it in a way that will protect their intellectual property.

Now, let's look at the situation that faces them today if they were to move to the Internet. Inside the United States they are fine. They can use U.S. products, 128-bit encryption, no problem. However, because they are not one of those special kinds of companies like banks or insurance companies, they aren't allowed to use strong U.S. encryption worldwide. They would be forced to turn to a foreign vendor in order to be able to secure their intellectual property overseas. And there are companies such as Baltimore and others that have those products today for which they would be more than happy to sell them.

So what does that say with respect to the net effects of our current export control policy? One, it most definitely takes sales that could have gone to a U.S. company and puts them directly in the hands of a foreign company, yet it does this without effectively stopping the deployment of strong cryptography overseas.

Now, the Administration has admittedly made progress in trying to update their encryption policy, yet it remains a policy that encourages and promotes the use of foreign encryption over that of domestic-made. It is time as a Nation that we update our encryption policy to be in sync with the realities of the times and to do so in a statutory way, and the SAFE Act does precisely that.

In conclusion, when I think of the Administration's export policy and its intention of keeping encryption out of the hands of our enemies, it reminds me of the Humphrey Bogart line from the movie *Casablanca*, which I will paraphrase for you today: I don't mind a bad encryption policy. I object to an ineffectual one.

Thank you.

Mr. GOODLATTE. Thank you.

[The prepared statement of Mr. Parenty follows:]

PREPARED STATEMENT OF THOMAS PARENTY, DIRECTOR, DATA & COMMUNICATIONS SECURITY, SYBASE, INC.

BSA strongly supports the Security and Freedom through Encryption ("SAFE") Act (H.R. 850) because it ensures that all Americans may use and sell any encryption domestically and provides badly needed export control relief.

Congress must immediately relax export controls on software and hardware with encryption capabilities. Widespread deployment of American products with encryption capabilities will help to accelerate dramatically the growth of electronic commerce by protecting consumers' privacy and preventing electronic crime. Export control relief also is vital for protecting America's critical infrastructures and ensuring that American software and hardware companies remain not only internationally competitive but also the market leaders in both software and hardware products.

The Administration took the first step towards developing a sensible long-term encryption policy by permitting exports of select products to select users, but they still have not gone far enough. A successful encryption policy must be based on technological and market realities. It must recognize that:

- The worldwide standard is 128-bit encryption;
- Mass market software and hardware is uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

Without relaxation of export controls, U.S. manufacturers remain at a competitive disadvantage, and foreign consumers will purchase encryption products from foreign suppliers.

Foreign products are comparable in capabilities and quality. When a foreign purchaser cannot obtain an American product they simply purchase it from a foreign supplier. Unfortunately, not only are American companies losing a sale of an encryption item, but they are also losing the sale of the program or hardware such as an Internet server or an application browser that uses the encryption capability. In fact, companies risk losing sales of entire systems because of their inability to provide necessary security features. The only impact of the Administration's export policy is widespread deployment of foreign designed and manufactured software and hardware.

The SAFE Act recognizes that the United States should not try to control uncontrollable exports of mass market and public domain software and hardware. It also permits exports of 128-bit level custom software and hardware. At the same time, the SAFE Act prohibits the Government from mandating the use of key escrow, key recovery or recoverable encryption or requiring Americans to use key escrow, key recovery or recoverable encryption if they want to use an electronic signature. Ultimately, the SAFE Act will help Americans to use encryption to protect privacy, prevent crime and protect our national security.

INTRODUCTION

Good Morning. My name is Thomas Parenty, and I am the Director of Data and Communications Security for Sybase, Inc. In this capacity, I am responsible for all security-related product development for one of the ten largest software companies in the world. I have been active in the cryptography and computer security field for over 15 years, including my tenure at the National Security Agency (NSA) in the early to mid-eighties.

While at the NSA, I advised the Director of the NSA on internal NSA computer security issues and worked on the security of global nuclear command and control networks, focusing on the formal verification of cryptographic protocols and internal computer security controls. Because of my specialized security knowledge, I worked on national security-related, compartmentalized programs at other Government agencies during my service at the NSA. In addition, I have worked on the security design of operating systems, networks and database management systems for Government agencies, including the Central Intelligence Agency, the Defense Intelligence Agency, the Air Force, as well as many U.S. computer vendors. Most recently, I served as an advisor to the President's Commission on Critical Infrastructure Protection, specifically addressing the needs of the telecommunications and banking infrastructures. I am also a member of the National Research Council's panel on information technology.

Headquartered in Emeryville, California, Sybase, Incorporated, is a worldwide leader in distributed, open computing solutions with revenues in 1998 of over \$800 million. We provide customers and partners with the software and services to create business solutions for strategic, competitive advantage. These high-performance, end-to-end solutions encompass client/server, Internet and intranet transaction processing and data mart and data warehousing applications. Sybase's Adaptive Component Architecture™ enables rapid design, development and deployment of distributed multi-tier business applications. Our product lines include Sybase high-performance database servers, EnterpriseConnect™ distributed data access and connectivity products, and Powersoft open business development tools.

I greatly appreciate the opportunity to appear today before this Committee on behalf of Sybase and the Business Software Alliance (BSA). Since 1988, BSA has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. BSA promotes the continued growth of the software industry through its international public policy, education and enforcement program in 65 countries throughout North America, Europe, Asia and Latin America. Its members represent the fastest growing industry in the world. BSA worldwide members include Adobe, Attachmate, Autodesk, Bentley Systems, Corel Corporation, Lotus Development, Microsoft, Network Associates, Novell, Symantec and Visio. Additional members of BSA's Policy Council include Apple Computer, Compaq, Intel, Intuit and my company, Sybase. BSA websites: www.bsa.org; www.nopiracy.com.

But we really are here today to speak on behalf of the tens of millions of users of American software and hardware products. The American software and hardware industries have succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. American

companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way—the continued application of overbroad, unilateral, export controls by the U.S. Government.

The Security and Freedom through Encryption (SAFE) Act, H.R. 850, modernizes U.S. export laws regarding software and hardware with encryption capabilities to permit American companies to compete on a level international playing field and to provide computer users with their choice of adequate protection for their confidential information and critical infrastructures.

For these reasons, BSA strongly supports the SAFE Act. We urge the Committee to report the SAFE Act unamended and look forward to its passage by the House early this year.

We want to pay tribute to the tremendous efforts of Representatives Goodlatte and Lofgren in championing this legislation, as well as thank both you, Mr. Chairman, and Mr. Frank and the other Subcommittee members who were among the 205 original cosponsors of the SAFE Act.

This morning I want to make three points:

- Widespread deployment of encryption is not only desirable, it is critical;
- America's export policy should promote widespread deployment of products with encryption capabilities in the worldwide market; and
- BSA strongly supports the SAFE Act because it provides freedom for Americans to use and sell any encryption domestically and provides greatly needed export control relief.

WIDESPREAD DEPLOYMENT OF ENCRYPTION IS NOT ONLY DESIRABLE, IT IS CRITICAL

Confidential Information And Secure Networks In The Internet Age Are The Key To Privacy And Commerce

American individuals and companies are rapidly becoming networked together through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet. Combined, these private and public networks are the economic engine driving electronic commerce, transactions and communications. This engine is being choked by the lack of availability of strong encryption products.

Traffic on the Internet doubles every 100 days. Predictions of business-to-business Internet commerce for the year 2000 range from \$66 billion to \$171 billion, and by 2002, electronic commerce between businesses is expected to reach \$300 billion. During 1997, one leading manufacturer of computer software and hardware sold \$3 million per day online for a total of \$1.1 billion for the year.

More and more individual consumers also are going on line and spending. More than 10 million people in North America alone have purchased something over the Internet and at least 40 million have obtained product and price information on the Internet only to make the final purchase off-line. Imagine the boost in volume of e-commerce if all of these consumers had enough confidence in the security of the Internet to purchase on-line.

Yet in 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks.

Network users *must* have confidence that their communications and data—whether personal letters, financial transactions or sensitive business information—are secure and private. Electronic commerce is transforming the marketplace—eliminating geographic boundaries and opening the world to buyers and sellers. Companies, governments and individuals now realize that they can no longer protect data and communications from others by relying on limiting physical access to computers and maintaining stand-alone centralized mainframes. Instead, users expect to be able to pick up their e-mail or modify a document from any computer anywhere in the world simply by using their Internet browsers. Thus, consumers worldwide are demanding to be able to protect their electronic information and interact securely worldwide, and access to products with strong encryption capabilities has become critical to providing them with confidence that they will have this ability.

Full Deployment Of Strong Encryption Is Vital For Protecting America's Critical Infrastructures

Governments also are recognizing that without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. The U.S. General Accounting Office in its report issued in May of 1996 entitled "*Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*" found that computer attacks are an increasing threat, particularly through connections on the

Internet, such attacks are costly and damaging, and such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

As the President said on January 22, 1999, before the National Academy of Sciences, “[w]e must be ready—ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services—or military assets. More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption.”

The President has been so concerned that he established a Commission on Critical Infrastructure Protection to provide him with guidance and issued two Presidential Directives based on the Commission’s recommendations.

In the Report of the President’s Commission on Critical Infrastructure Protection entitled *Critical Foundations: Protecting America’s Infrastructures* (October 1997), the Commission emphasized that “Strong encryption is an essential element for the security of the information on which critical infrastructures depend.” In fact “[p]rotection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks. . . .
- Effective means of protecting data against unauthorized use or disclosure.
- Well-trained users who understand how to protect their systems and data.”

An earlier blue ribbon National Research Council (NRC) Committee similarly concluded in its (May 1996) CRISIS Report (“Cryptography’s Role in Securing the Information Society”) that encryption *promotes* the national security of the United States by protecting “nationally critical information systems and networks against unauthorized penetration.”

Thus, the NRC Committee found that on balance the advantages of widespread encryption use outweighed the disadvantages and that the U.S. Government has “an important stake in assuring that its important and sensitive . . . information . . . is protected from foreign government or other parties whose interests are hostile to those of the United States.”

Information security is critical to the integrity, stability and health of individuals, corporations and governments. While cryptography is but one element of security, it is the keystone of secure, distributed systems. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America’s infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

U.S. unilateral export controls have also had a significant impact on the availability of strong American encryption domestically, which is ultimately harming the American consumer. The U.S. software and hardware industry makes at least one-half of its revenues through exports. For this reason and due to the significant difficulties companies encounter selling foreign purchasers a weaker version of an encryption product, some software companies have offered products with the same encryption capabilities both domestically and abroad. Therefore, the American consumer has fewer strong American encryption products to choose from than they would without U.S. export controls. The American consumer is ultimately left with an unfortunate choice: they may either buy strong encryption which they cannot use internationally, or they may simply purchase strong foreign encryption products that are not subject to U.S. export controls. Neither choice is the best for protecting America’s critical infrastructures.

In the long-term, we believe it is in America’s best interest to have America’s critical infrastructures and national security be protected by widespread reliance on strong American encryption products both here and abroad.

Relaxed Export Controls On Encryption Products Is Vital For Ensuring America’s Global Competitiveness

American companies *do* have exciting and innovative products that can meet the demand for 128-bit encryption and compete internationally. But unless the current unilateral U.S. export restrictions are changed to allow the use of strong encryption, American individuals and businesses will not be active participants in this new networked world of commerce—let alone continue to be the leaders in its development. Furthermore, American companies will no longer be providing the world, and its critical infrastructures, with the answers to their security problems. Instead for-

eign companies will. It is unclear how U.S. national security or law enforcement will be aided or how our critical infrastructures will be secure when foreign encryption products dominate the world market.

The computer software and hardware industries are American success stories, but they are being threatened. America's software and hardware industries are important contributors to U.S. economic security—now and in the future. Information technology industries are now directly responsible for over one-third of real growth of the U.S. economy. Between 1980 and 1992, the computing and software industry grew at an annual rate of over 28%, while overall domestic growth was less than 3%. From 1990 through 1996, the software industry grew at a rate of 12.5%, nearly 2.5 times faster than the overall U.S. economy.

More than 7 million people work in IT industries. In 1996, the software industry provided a total of over 619,000 direct jobs and \$7.2 billion in tax revenues for the U.S. economy. The software industry is expected to create an average of 45,700 new jobs each year through 2005. If piracy were to be eliminated in the United States, the number of new software jobs created would double to an average of 93,000 a year.

Moreover, the computer software industry has achieved tremendous success in the international marketplace with global sales of packaged (*i.e.*, non-custom) software reaching over \$118.4 billion in 1996, and rising to \$135.4 billion in 1997. American produced software accounts for 70% of the world market, with exports of U.S. programs constituting half of the industry's output.

The incredible growth of the industry and its exporting success benefits America through the creation of jobs here in the United States. Many of these jobs are in highly skilled and highly paid areas such as research and development, manufacturing and production, sales, marketing, professional services, custom programming, technical support and administrative functions. In the U.S. software industry, workers enjoy more than twice the average level of wages across the entire economy—\$57,319 versus \$27,845 per person.

All of these revenues and jobs are dependent upon American software and hardware producers remaining the market leaders around the world, especially as the major growth markets continue to be outside the United States. Strong export controls on products with encryption capabilities are crippling the ability of these companies to compete with foreign providers.

AMERICA'S EXPORT POLICY SHOULD PROMOTE WIDESPREAD DEPLOYMENT OF AMERICAN PRODUCTS WITH ENCRYPTION CAPABILITIES IN THE WORLDWIDE MARKET

As embodied in the SAFE Act, the most successful encryption policy will ensure that Americans can use and sell any encryption that they want domestically, prohibit both Federal and State governments from imposing encryption standards or techniques, and relax export controls on products with encryption capabilities in a manner that is based on technological and market realities. Just because law enforcement and national security interests wish that they could turn back the clock and limit consumers access to strong encryption approved by the government, it will not happen, especially on a worldwide basis. This is especially true for mass market software and hardware, which by its inherent nature is uncontrollable.

The Administration Took The First Step Towards Developing A Sensible Long-Term Encryption Policy, But They Still Have Not Gone Far Enough

The BSA members welcomed the Administration's efforts to relax export controls on select products used by select users. However, the Administration's actions are merely a first step. A truly successful, sensible encryption policy would be based on technological and market realities, and would not create winners and losers in the encryption marketplace on a sector-by-sector basis. It would recognize that:

- The worldwide encryption standard is 128-bit encryption;
- Mass market software and hardware is inherently uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

Moreover, we believe it is preferable for Congress to put encryption policy on a statutory basis—sending a strong message around the world that encryption is important for a strong defense, for protecting the privacy of citizens and for preventing crime.

Unilateral U.S. Export Controls Harm American Interests

Currently, there are no restrictions on the use of cryptography within the United States. However, the U.S. Government maintains strict *unilateral* export controls on computer products that offer strong encryption capabilities.

American companies are forced to limit the strength of their encryption to the 56-bit key length level set late in 1998. The recently announced regulations will also permit companies to export stronger encryption on a sector-by-sector, user-by-user basis. However, this policy ignores the fact that:

- The minimum strength now required by new Internet applications is 128-bit encryption;
- The most widely used encryption program, PGP, with over two million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key;
- American companies cannot export encryption products to a vast majority of non-U.S. commercial entities. Foreign manufacturers provide 128-bit encryption alternatives and add-ons—filling the market void created by U.S. export controls;
- Providing sector-by-sector relief is unworkable for mass market products and does not reflect commercial realities for sales of custom products; and
- 56 bit encryption has been demonstrated to be vulnerable to commercial let alone governmental attack. (In the beginning of this year at the RSA Encryption Conference, a 56-bit DES encoded message was broken by private companies and individuals working together in 22 hours and 15 minutes—imagine what a hostile government with serious resources could do.)

Export controls also have made American companies less competitive and opened the door for foreign software and hardware developers to gain significant market share—decreasing our national and economic security.

I want to take one minute to discuss the Wassenaar Arrangement at this point. Please do not be fooled by any claims from the Administration that the Wassenaar Arrangement is the multilateral agreement on encryption that they have been touting was just around the corner for the past several years.

The Wassenaar Arrangement was an agreement among only 30 countries, and it actually decontrolled encryption products. Many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement. The Wassenaar Arrangement eliminated controls of any sort on 56-bit encryption and permits exports of up to 64-bit encryption in mass-market software and hardware. It also removed any reporting requirements—the sole official means for actually monitoring what countries are doing. Although the Arrangement left open the possibility that countries might individually control 128-bit encryption, we are skeptical that they will do so. There is no penalty for failing to control 128-bit encryption, and most countries are actually moving towards *encouraging* the use of stronger encryption. Finally, a country could technically comply with the Arrangement, while still permitting easy exports of strong encryption.

Even France, traditionally the country which placed the greatest restrictions on its own citizens by limiting them to the easily broken 40-bit level of encryption, has recognized that technology has progressed. Near the end of 1998, France relaxed controls on the domestic use of encryption and is now permitting, and in fact encouraging, the use of 128-bit encryption by its citizens.

Without Export Relief, Foreign Consumers Will Purchase Their Products From Foreign Suppliers, Keeping U.S. Manufacturers At A Competitive Disadvantage

As a result of U.S. unilateral export controls, encryption expertise is being developed off-shore by foreign manufacturers who now provide hundreds of encryption alternatives and add-ons. The Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products. In fact, foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales.

As long ago as 1995, the General Accounting Office confirmed that sophisticated encryption software is widely available to foreign users on foreign Internet sites. In 1996, a Department of Commerce study again confirmed the widespread availability of foreign manufactured encryption programs and products. An on-going industry study by Trusted Information Systems (TIS Study) highlights the ever-increasing availability of foreign developed and manufactured products as it discovered there were 656 foreign programs and products available from 29 countries as of December 1997.

Further demonstrating the worldwide availability, use and sophistication of encryption abroad is the Department of Commerce's National Institute of Standards and Technology (NIST) efforts to work with the private sector to develop an Advanced Encryption Standard (AES). Individuals and companies from eleven different countries proposed 10 out of the 15 candidate algorithms submitted to NIST: Australia's LOKI97; Belgium's RIJNDAEL; Canada's CAST-256 and DEAL; Costa Rica's FROG; France's DFC; Germany's MAGENTA; Japan's E2; Korea's CRYPTON; and the United Kingdom, Israel and Norway's SERPENT algorithms. Only 5 out of the 15 candidate algorithms were submitted by U.S.-based individuals or companies.

The impact of lost sales is enormous. If an encryption product is combined with other applications such as Internet browsers and application servers, U.S. companies will generally lose both sales. In fact, companies risk losing sales of entire systems because of inability to provide necessary security features. This permits foreign manufacturers to gain entry into companies as well as gain credibility—providing the foreign manufacturers with further opportunity to take away future sales in the same and other product lines.

I would like to mention a few specific examples with respect to foreign availability of encryption products. The Apache Group, based in the U.K., announced in April 1997 that its Apache Unix Internet Server software with very strong encryption had a 29% market share of Web server software. Today the Apache web server serves over half—50%—of the domains on the Internet.

Companies such as Brokat Informationsysteme, a German company, are developing products that are more than simply add-ons to American products. Brokat's modular e-services platform, Twister, which companies use to offer their customers secure and simple electronic services via various electronic channels, such as the Internet or mobile communications networks, is already being used by more than 1,500 companies worldwide. Brokat's sales outside of Germany, including to the United States, have now increased to be 56 percent of the company's total sales. The American market research institute Meridien Research described BROKAT as the leading company worldwide for Internet banking solutions.

The merger of two foreign companies, Zergo Holdings (U.K.) and Baltimore Technologies (Ireland), into a new company called Baltimore only further illustrates that foreign companies are flourishing solely because there is no U.S. competition. According to the Gartner Group in a Research Note dated January 28, 1999, the new company is "a competitive participant in providing e-commerce and enterprise security, with 11 international offices and a global partner network . . . with customers in 40 countries."

U.S. Encryption Export Controls Hurt American Companies Without Helping Law Enforcement Or National Security

U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for an immediate and easy exportability of products meeting general commercial requirements—which is currently 128-bit level encryption!

To summarize:

- Foreign competitors not subject to outdated U.S. export controls are ready to take sales and customers from U.S. companies today.
- Complex and cumbersome U.S. export controls make American companies less competitive. They significantly increase the costs of developing, marketing and selling products with encryption capabilities, delay the introduction of new products or features, and encourage foreign customers to purchase from foreign suppliers due to the uncertainty and delay in obtaining a comparable American product.
- Current export controls do not keep strong encryption out of the hands of foreign customers; they just keep U.S. products out of their hands.

BSA STRONGLY SUPPORTS THE SAFE ACT BECAUSE IT PROVIDES FREEDOM FOR AMERICANS TO USE AND SELL ANY ENCRYPTION DOMESTICALLY AND PROVIDES GREATLY NEEDED EXPORT CONTROL RELIEF

The SAFE Act Preserves Americans' Domestic Encryption Freedom

The SAFE Act ensures that Americans may use and sell whatever kind of encryption they want domestically. It ensures that the U.S. government may not require or provide other incentives for Americans to use encryption products "approved" by the government or meeting certain standards. Also, the Act does not permit the government to link electronic signatures to the use of certain types of encryption products.

The SAFE Act Provides Law Enforcement With Important Safeguards

Importantly, the SAFE Act does permit the Secretary of Commerce to continue preventing exports to countries of terrorist concern or other embargoed countries pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act.

The bills also contain safeguards when relaxing export controls for strong encryption products—the Secretary of Commerce is not required to permit such exports if there is substantial evidence that the software or hardware will be diverted or modified for military or terrorist use or re-exported without requisite U.S. authorization.

The SAFE Act Recognizes That Mass Market Products Are Uncontrollable And Should Be Exportable

U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market hardware manufacturers and software publishers sell products through multiple distribution channels such as OEMs (i.e., hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources.

The mass-market distribution model presupposes that hardware manufacturers and software publishers will take full advantage of these multiple channels to ship identical or substantially similar products worldwide (allowing only for differences resulting from localization) irrespective of specific customer location or characteristics.

Uncontrollable products at 56-bits cannot suddenly become controllable products at 128-bits. The SAFE Act recognizes as a fundamental proposition that the United States should not try to control the export of something that is, by its very nature, uncontrollable. Trying to control the uncontrollable squanders the limited resources of companies trying to comply with unrealistic export controls as well as the resources of the government as it tries to enforce unenforceable export controls, undermining the credibility of the entire system of export controls.

The SAFE Act Permits Exports Of Custom Hardware And Software

The SAFE Act ensures that if strong encryption products have been permitted to be exported to foreign banks, then custom software and hardware with comparable encryption capabilities should be exportable to other foreign commercial purchasers in that country. The U.S. should not control exports of competitive custom products embodying world encryption standards. Note that the type of software and hardware we are talking about here is a "custom" product (if it were generally available it would not need an individual license under the bill's other provisions).

THE TIME FOR ACTION IS NOW

To keep American vendors on a level international playing field and American computer users adequately protected, U.S. export controls must be immediately updated to reflect technological and international market realities.

Thank you.

Mr. GOODLATTE. Mr. McLaughlin.

STATEMENT OF CRAIG McLAUGHLIN, CHIEF TECHNOLOGY OFFICER, PRIVADA

Mr. PARENTY. Good afternoon, Mr. Chairman, members of the subcommittee. Thank you for the opportunity to speak with you this afternoon about this important topic. I especially appreciate

the efforts of Mr. Goodlatte and Ms. Lofgren and the cosponsors of the SAFE Act for the willingness to address this complex issue.

As you know, my name is Craig McLaughlin. I am the chief technology officer at Privada, an Internet start-up located in San Jose, California. I am pleased to be testifying this afternoon on behalf of the Software and Information Industry Association. SIIA represents 1,400 member companies engaged in every aspect of electronic commerce, and SIIA along with Privada strongly supported H.R. 850, the SAFE Act.

I am not going to pretend that I can speak better than everyone who has spoken before me already. Most of my comments would simply offer a reiteration of what they have said, so I would like to bring a bit of a personal perspective to it and tell you a little bit about Privada and how we are relying on encryption technology and actions of this committee in order to make our business successful.

Privada is a company which is dedicated to the premise that individuals and organizations should have and be able to maintain control and gain access to their personal data. For corporations, this could be sensitive financial data or project plans for individuals. It could be something as sensitive as your credit card number or your health insurance information.

There can be no question then privacy is one of the driving factors. A recent study by the Lou Harris organization indicated that privacy is the number one issue and number one concern of individuals moving on to the Internet. Eighty-five percent of respondents said they had concerns about the safety of their personal information on-line; 79 percent of those participating in e-commerce indicate concerns about the use of their personal data. A more recent study has indicated that despite the boom in e-commerce that we are currently enjoying, that boom is, in fact, half of what it could be if personal privacy is effectively granted on the Internet. The only way I would submit this is possible in today's world is with cryptography.

That being said, the current policy of restricting encryption in exports is, I respectfully submit, outdated and counterproductive. The current approach to encryption exports, like others before it, has sought to balance the needs of law enforcement and national security with the needs of Internet users, but instead has only created a situation in which U.S. industry is, as has been mentioned before, at a competitive disadvantage to its foreign counterparts where on-line communications and transactions may remain vulnerable and where users do not have tools available to them to protect their privacy.

As implied by those statements is the simple fact that encryption is no longer used simply to scramble the text of secret messages point to point. Encryption has evolved to include authentication of identity, certification of information, data integrity, and network security applications. These applications are widely used in virtually every industry today and are critical to the further development and use of networks. One example is the protection of sensitive information from misappropriation by unauthorized parties. In other words, I should be able to shop on-line without having a third party know what I am purchasing. However, another use of

cryptography, an extension of that, is to protect against the misuse of information by otherwise authorized, but perhaps negligent or malicious parties. In other words, encryption can be used to protect my privacy from the person I am conducting the transaction with.

Such capabilities are critical for both business and individuals seeking to take advantage of the Internet. Without robust encryption tools, no one can be assured that their on-line activities remain private and that their on-line transactions are trustworthy. To ensure that this market continues to grow, consumer concerns like privacy, authentication, and security must be addressed. Without encryption, I would submit, we simply cannot do it. We must be able to use and widely deploy encryption if we are to help users protect their personal privacy.

Second, as I mentioned, U.S.—current U.S. policy puts U.S. companies like mine at a competitive disadvantage compared to our foreign counterparts. Mr. Parenty brought up an excellent example of a foreign counterpart successfully marketing into the U.S. based on the strength of the U.S. export policy. I would like to bring up another one, a slightly more personal one to us.

There is a competitor in our field, a Canadian-based company, which has, in fact, routinely used in their trade and in their press releases the fact that they are based in Canada and are not subject to U.S. export controls. As a result, companies who choose to incorporate have a Faustian choice of either sacrificing the foreign market or limiting the strength of their encryption.

In conclusion, I would submit that it is critical that this committee and Congress act quickly to remove export provisions on encryption products to ensure that these—that companies such as Privada can compete fairly and effectively in the international marketplace, and I urge the members of this subcommittee to support H.R. 850. Thank you.

Mr. GOODLATTE. Thank you.

[The prepared statement of Mr. McLaughlin follows:]

PREPARED STATEMENT OF CRAIG McLAUGHLIN, CHIEF TECHNOLOGY OFFICER,
PRIVADA

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to speak with you this morning about this important topic. I appreciate the efforts of Mr. Goodlatte, Ms. Lofgren and the cosponsors of the SAFE Act for their willingness to address this complex but important issue.

My name is Craig McLaughlin and I am the Chief Technology Officer at Privada, Inc., based in San Jose, CA. I am pleased to be testifying this morning on behalf of the Software & Information Industry Association (SIIA), the result of a merger between the Software Publishers Association and the Information Industry Association. SIIA represents 1400 member companies engaged in every aspect of electronic commerce and strongly supports H.R. 850, the Security and Freedom through Encryption (SAFE) Act.

THE ROLE OF CRYPTOGRAPHY

Encryption is tremendously important for securing electronic communications and transactions. As the Internet continues to increase, more individuals and businesses "go online," and companies shift their mission-critical operations to the Internet, the need for and importance of cryptography only grows.

As a result, the market for encryption is growing. Users routinely demand robust encryption products, and global sales of encryption products are expected to reach \$20 billion by 2002.¹ Companies in every sector are seeking to utilize security prod-

¹Economic Strategy Institute, 1998.

ucts to facilitate online sales, improve their own products, protect their intellectual property and secure their private data and communications.

There can be no question that the demand for encryption products is strong. A 1997 study identified over 1600 encryption products available from more than 900 companies in thirty countries. That same year, Trusted Information Systems found more than 650 encryption products produced abroad; almost 300 of these incorporated DES-level encryption. Encryption is routinely used in software, databases, networking products, telecommunications equipment, computer peripherals, electronic commerce and financial services. Without a doubt, encryption is one of the most important tools companies and individuals have in the digital environment.

While we are beginning to realize the benefits of the global electronic marketplace, we are also realizing some of the challenges that users face. Computer crime, intellectual property theft and privacy fears are some of the issues that the Internet community is being forced to address. By using security products that incorporate robust encryption, companies and individuals can minimize these concerns.

One of the biggest challenges facing us today is the question of online privacy. While users want to take advantage of the Internet's vast resources, many are concerned about the collection and use of their personal information. According to some studies, privacy is *the* primary concern for online consumers. A Lou Harris poll recently found that 81 percent of Internet users and 79 percent of those who have purchased goods online are concerned about privacy.

My company, Privada, was founded in 1997 on the premise that individuals and organizations should have the ability to control access to and use of their personal information online—that every person should have the freedom to use the Internet responsibly, without sacrificing their privacy. We have developed a suite of products that allow individuals to protect their privacy while using the Internet for browsing, communications or purchases. Our products disassociate one's real-world identity from the online identity, ensuring that individuals can take advantage of the Internet while protecting themselves and their families online.

Companies like mine have worked hard to develop technological solutions that address these concerns, providing both individuals and businesses with the tools needed to assure their privacy. Such efforts help promote a secure online environment and improve user confidence, helping the vibrant electronic commerce market continue to grow.

CURRENT ENCRYPTION POLICY

The current policy of restricting encryption exports is, I respectfully submit, outdated and counterproductive. The Administration's approach to encryption exports, like others before it, has sought to balance the needs of law enforcement and national security with the needs of Internet users, but instead has only created a situation in which U.S. industry is at a competitive disadvantage to its foreign counterparts, where online communications and transactions may remain vulnerable, where users do not have robust tools to protect their privacy and that ultimately threatens to undermine our technological leadership in this critical area.

Let me address each of these points in some more detail.

Current policy is outdated.

The current administration policy has evolved from an era in which encryption was regulated as a munition. Encryption products were largely used to provide a level of secrecy for electronic data and communications. Not widely available, export restrictions on encryption and related products could be relatively effective in limiting the spread of these products around the world.

With the growth of electronic networks, though, the effectiveness of restrictions is seriously compromised. Digital networks cross national borders and reach around the globe. Data flows across the country and around the world in an instant, often without the user knowing where the data is originating or terminating. International networks have made it possible for individual users to take advantage of resources previously unavailable to them and for companies to develop new markets around the world.

More importantly, perhaps, is the fact that encryption is no longer used to simply scramble the text of secret messages. The use of encryption has evolved to include authentication and certification, data integrity and network security applications. These applications are widely used in virtually every industry today and are critical to the further development and use of networks in everyday life.

One example is the protection of sensitive information from misappropriation by unauthorized parties, or misuse by otherwise authorized, but negligent or malicious parties, to a transaction. Encryption is the only practical means by which parties to an online communication can trust that each is who he claims to be. It is the

only practical way to guarantee that the communication between those parties remains private.

A further example may be helpful. Many Members of Congress—including yourselves, I'm sure—receive e-mail from their constituents. Some of you choose to reply to your constituents via regular postal mail, but I am sure that many of you choose to use e-mail as a means to communicate with the citizens in your districts. It's effective and inexpensive.

Without technologies like digital signatures, though, your constituents can never really be confident that the message actually came from your office or that the message wasn't modified during the transmission process. Digital signatures, which rely on the enabling technology of encryption, provide users the ability to certify and authenticate the message and therefore trust that the message is authentic. Just as a letter on your stationery with your signature provides a level of confidence, digital signature provide similar assurances for recipients of electronic communications.

Such capabilities are critical for both business and individuals seeking to take advantage and use the Internet. Without robust tools, no one can be assured that their online activities remain private and that their online transactions are trustworthy. Companies are rapidly developing innovative technologies and applications for use on public networks and users are just as rapidly integrating these capabilities into their everyday lives. To ensure that this market continues to grow, consumer concerns like privacy, authentication and security must be addressed. Without encryption, we simply can't do it. We must be able to use and widely deploy encryption if we are to help users protect against the inherent vulnerabilities of public networks.

Current policy puts U.S. companies at a competitive disadvantage.

Second, U.S. policy puts U.S. companies like mine at a competitive disadvantage compared to our foreign counterparts. This is an issue that affects us directly at Privada. Because of the current export controls, U.S. companies face restrictions which prevent them from offering competitive products in the global marketplace—restrictions which foreign competitors do not face. Internet users, whether corporate or individual, are sufficiently sophisticated to seek and demand robust encryption tools in the products they use to facilitate their own online activities. Companies that cannot offer these features face an uphill battle in an extremely competitive marketplace.

As a result, companies who choose to incorporate encryption into their products are faced with a Faustian choice. They can either use strong encryption and forgo the lucrative export market, or they can use weaker encryption for their export products, thereby rendering them unattractive to potential customers.

Companies who choose to forgo exports face a significant challenge. In the era of the global electronic marketplace, to have products that cannot be sold on the foreign market is a tremendous disadvantage. For many software and information companies, foreign sales account for a large percentage of their total annual sales; to simply be forced to abandon this market is obstacle that our foreign competitors simply do not face.

Some companies choose an alternative route. They choose to export products that incorporate weaker encryption, placing them at a significant disadvantage to their competitors abroad. Users understand the value of encryption, and simply do not want products that are weak or easily broken. Further, because multiple product lines must be developed, production costs—and thus the cost of products and services—rise. Companies who choose this route often find that their potential international customers go elsewhere to find products that meet their need for robust privacy and security products.

This dichotomy between their foreign counterparts and US companies is so pronounced a foreign competitor of Privada has used it to market its services.

Current policy limits the ability of companies and individuals to protect data and communications.

Perhaps the most problematic aspect of current policy is that without strong encryption products, data and communications remain unprotected. With robust encryption, companies and individuals have the tools they need to ensure that their online activities and data are secure, protected and authentic.

Without strong encryption, our products and others cannot provide the level of security that customers are demanding. When forced to use weaker encryption, products and services are vulnerable, undermining the very sense of security and confidence that we seek to instill and foster. In fact, they actually weaken protections by generating a false sense of security—as has been said many times, weak cryptography is worse than none at all.

For my company and others working to develop technological tools to help users protect their privacy, the ability to use and incorporate strong encryption into our offerings is critical. Encryption is *the* core component of the technologies we develop to help users control how their personal information is collected and used. Without it, our mission is unachievable, and the privacy of millions of individuals is at risk.

Current policy ultimately undermines our technological leadership.

Finally, I think that it is critical that we consider what the impact of the current policy will be on our technological leadership in the future. The United States has benefited tremendously from the vibrant technology industries that have seen such rapid innovation and growth in recent years.

As has been widely reported in the press and as implied by our competitor's actions, the methods, algorithms and technologies being discussed today are globally known, understood and published. At its very core, encryption relies on mathematics. And while U.S. manufacturers have developed a wide array of products that incorporate these technologies, there is no reason to believe that competing products developed abroad would not meet users' functionality and performance standards.

As I mentioned earlier, foreign products are widely available. Many have downplayed the quality of these products and services, instead believing that foreign customers automatically assume that U.S.-developed software, information and electronic commerce products are inherently better than their international counterparts. This is simply not true. As I mentioned above, encryption technologies are well understood and available. There is no reason to believe that US products are simply better because they originated here, and it is important not to discount the viability of these foreign products.

The ultimate result, of course, is that companies face restricted markets, unfair competition and reduced sales, resulting in less revenues for research and development of new products. For high-tech industries, especially in software, electronic commerce and information, R&D costs are often quite significant. Without robust sales to fuel additional development, companies cannot afford to innovate or create new products that meet the rapidly changing needs of the electronic marketplace. While it unrealistic to predict that those of us who produce products and services that incorporate encryption will inevitably go out of business or move abroad, it not unreasonable to be very worried about the long-term impact that market restrictions will have on our ability to innovate and lead. Without further research and development, we risk losing the leadership that we have developed in this critical market segment.

THE NEED FOR POLICY REFORM

Clearly, a new approach is needed. It is important that Congress address this issue in a timely manner. We often speak of "Internet time" to refer to the quickly changing electronic environment, and it is critical that our policies remain appropriate to facilitate continued growth.

At the same time, we recognize that there are lingering concerns about the misuse of encryption—the very concerns that have driven the current restrictions. I suggest, though, that a more proactive, forward-looking approach may actually enhance the objectives of the current policy while providing U.S. industry with continued access to robust encryption tools.

How could such a balance be possible? First, let me suggest that maintaining U.S. technological leadership is critical. We must be able to attract and keep those talented individuals and companies that have driven the growth in the industry. If these capabilities move elsewhere or our leadership is compromised, our ability to work with law enforcement and provide assistance will be greatly reduced. As outlined above, we are not going to be able to do so if our companies cannot compete abroad or face unnecessary restrictions on their ability to do so.

In addition, we must provide the tools so that all of our industries can take advantage of new technologies. Economic espionage and computer crime are tremendous threats, and any company that uses computers in any fashion is evaluating ways to make their systems more secure and to protect their data more effectively. To ensure that these organizations, whether they be grocery stores, pharmaceutical research firms or educational facilities, have access to robust tools, we must ensure that our companies are able to develop these products.

The Administration has long recognized the value that encryption has for securing electronic systems. Its recent proposed revisions to the export restrictions, which allow for the export of 56-bit encryption and stronger products for certain sectors, underscore the importance of encryption. I think that it is unrealistic and perhaps a bit short-sighted to assume that the best approach is to regulate which sectors

should be able to deploy advanced security products, rather than letting the market and individual users decide what their security requirements are.

Second, companies throughout the industry are developing products that strike the delicate balance between the need for privacy and security with the need to access information. While it may not be feasible for individual users to purchase or deploy many of these products, companies, including those who provide online access to individuals, are beginning to demand these products.

An example may be helpful. Companies, for example, may wish to encrypt their corporate communications to protect their trade secrets or proprietary information. But they also recognize that there may be situations where they need to reconstruct an event or access protected information. The activities of an employee suspected of divulging corporate secrets may need to be investigated, for example. Several products on the market today allow for such access without compromising the security of the original data or communications.

Please do not misconstrue my comments—this is not an endorsement for key recovery. Our products, for example, do not incorporate key recovery but can be used to provide access if needed. That companies are developing such alternatives is simply a recognition that some customers demand such functionality and the market is responding appropriately. Companies must be given the opportunity to respond to market preferences without the intervention of the Government because only individual consumers can make decisions regarding what products and protections are appropriate to their unique situation.

Finally, it is important to realize that encryption is widely available from any number of sources, and that maintaining outdated policies will not meet the Administration's objectives. We all know that this genie is out of the bottle, to repeat an oft-used phrase. We cannot simply accept that our export restrictions are effective just because we hope that they are. We must recognize the realities of the market today and adapt our policies before we lose the advantages that we enjoy.

CONCLUSION

In conclusion, I submit that it is critical that Congress act quickly to remove export provisions on encryption products to ensure that our companies can compete fairly and effectively in the international marketplace and continue to provide users with the tools that they need to protect their privacy and security online. By freeing the market and allowing U.S. companies to take full advantage of the global market for these products, we can ensure that every company and individual has access to technologies that enhance this growing market.

I urge the Members of the Committee to support liberalizing encryption export provisions and to support H.R. 850.

Thank you.

Mr. GOODLATTE. Mr. Norquist, welcome.

STATEMENT OF GROVER NORQUIST, PRESIDENT, AMERICANS FOR TAX REFORM

Mr. NORQUIST. Thank you. I have submitted written testimony. I just want to make a few comments again by thanking Congressman Goodlatte and Congresswoman Lofgren for their leadership on the SAFE Act. Americans for Tax Reform is a strong supporter of this legislation. I think it is extremely important.

President Reagan said that too often governments take the point of view that if it moves, you should tax it; if it continues to move, you should regulate it; and once it has stopped moving, you should subsidize it. And too often bureaucrats have taken this attitude throughout history, and, worse reactionary forces have constantly tried to stop technology, and stop the changes that technology brings. This is always a mistake. It doesn't work. These people stand throughout history yelling, stop, and history and technology don't stop.

In Romania, they used to register all the typewriter technologies because that was the new technology. And the Soviet Union took

the same approach toward faxes and Xeroxes. China is now dealing with e-mails.

The comment earlier that Mr. Delahunt made, the Government is trying to line up a Maginot Line, I think was quite to the point; this reminds me of this Administration, of King Canute, who stood on the—or sat on the beach and was commanding the water not to come up, and when it did and do eventually come up, this Administration gets knee deep in water, and instead of getting off the beach, they said, we will move back 10 feet, and now we will make the tide stop coming. Point in fact, the tide continues to come in, even as the Government's own witnesses have pointed out.

When telephone service was originally put into Saudi Arabia, there were Muslim clerics who thought it was an instrument of the West and the devil, and we should do something about it and stop it. The wise king said, well, let's read the Koran. We have the two ends of the telephone over the wires, and if it—and if the words of the Koran can go over, it is okay. And that is how they were able to get the telephone in.

We can't have this kind of know-nothing approach toward technology continued by this Administration and this Government. The NSA was responsible for breaking Japanese and Iraqi codes, and they use that as if we were somehow endangering some Pearl Harbor with this new policy. Then at the same time they admit that all governments and militaries encrypt. So, we are not dealing with Pearl Harbor here. It is really kind of disingenuous of them to open with that kind of comment. Encryption technology is available worldwide now. There is strong encryption everywhere now. We know this. The good guys know it. The bad guys know it. I don't understand why the Government continue this position on this is.

As I heard their argument, I am reminded of the statement that no one's life is a complete waste. Some people serve as bad examples. Their arguments strike me the same way. I didn't get the point of their argument other than a bad example of an argument.

Then we went into this discussion of encouraging voluntary key recovery, and that somehow if we don't have Government regulation, we can't encourage voluntary key recovery. Well, if it is voluntary, I missed the point of what the Government's involvement is. I am not familiar with the FBI and NSA's involvement in voluntary things.

We then had a discussion of encouraging market and other incentives. I know what a market incentive is. I think we dread of the idea of what other incentives would be in the hands of the FBI. There aren't marketed incentives.

I do think, however, that in addition to having these two panels that I would very much like to see a debate. Every time I or others have come and spoken to Members of the House and the Senate, the guys from the FBI and the NSA refuse to be in the same room and have a debate. In addition, they have all left today. I think that if they believed that their position made any sense at all, they would be willing to have a debate. Let's put one on C-SPAN where we can go back and forth because—I assume they got paid for today's work, but they didn't answer your question, which was, excuse me, if this is available worldwide from Canada and Ireland and other countries, why does banning the export of American

encryption make any sense at all? If the governments of the world and the militaries of the world have this, why does banning American exports make any sense at all?

The only thing I can imagine is that some people do want to go after encryption domestically, that that is their real agenda, and that that is what the FBI would like to do. I was pleased that the Members tried to explain patiently to the Administration officials that domestic control is not an option, but otherwise their arguments don't make any sense, and I am a little bit concerned that this Administration continues to be column material for Nat Hentoff with their efforts to expand wiretaps, the secret testimony laws, and the new "know your customer" laws, in addition to threats to domestic encryption.

So on behalf of the taxpayers movement, I believe the SAFE Act legislation is extremely important. I find the arguments by this Government completely disingenuous, and I challenge them to a public debate in front of TV cameras, in front of you guys.

I know times you in Congress talk about a lack of civility. I thought you were overly generous and civil in the face of not getting your questions answered. Thank you.

Mr. GOODLATTE. Thank you, Mr. Norquist.

[The prepared statement of Mr. Norquist follows:]

PREPARED STATEMENT OF GROVER NORQUIST, PRESIDENT, AMERICANS FOR TAX REFORM

Thank you, Mr. Chairman and distinguished members of the Courts and Intellectual Property Subcommittee. It is an honor to appear before you today to express my strong support for this legislation, H.R. 850; the Security and Freedom Through Encryption Act.

Americans for Tax Reform has taken an increasing interest in the emerging economy and the implications for every taxpayer, because the digital economy does impact every taxpayer. Along those lines I have considered each issue that effects electronic commerce very seriously. In addition, I was selected to serve on the Advisory Committee on Electronic Commerce to examine the role and impact of taxation on electronic commerce. Encryption is a principle building block for the success of the digital economy both domestically and internationally. This basic fact drives both my and the taxpayer's movement interest.

For several years, and congressional sessions, policymakers, public interest groups and privacy advocates have been engaging in a great debate on the issues concerning a basic electronic necessity—encryption. As we have heard in the press and in the "Encryption and the Constitution" hearing held by Senator Ashcroft last year, the Founding Fathers had no trouble deciding whether robust encryption should be used: They actually used cypher wheels, which are encryption devices, during the discussions that would result in the very founding of this nation. The great debate that established our beloved Constitution—a document that embodies the freedoms we hold so dear—was actually developed because of the advantages of technology. Encryption has long been used as a tool to protect communications and to ensure that integrity and privacy of communications remain intact. Since that momentous time we have clearly moved away from trusting the American people and have opted instead to lay the groundwork for a weakened Bill of Rights.

It is truly ironic that the Congress, which has little difficulty raising personal income taxes and has less than 90 years experience with that notion, cannot see clear to allow the free use of robust encryption, which 250 years ago patriots were using to secure our fundamental freedoms from an ever more controlling government. The impossibly complicated federal tax system is impossible to fathom, even for IRS officials as we heard last year during the hearings on IRS reform. In addition, unlike the federal budget encryption technology is fairly straightforward by comparison and based on mathematics, instead of "creative financing."

The push towards increased federal government control seems unending. William Safire recently noted in *The New York Times* that a half-century ago, government at all levels controlled a fourth of our economy and that today government controls about one-third. Controls on encryption are one more governmental attempt to con-

trol an aspect of everyday life, our right to protect our personal information from snoops and criminals. The historical perspective on this issue is fairly apparent. Encryption has been used in, and by, this country for hundreds of years.

Today I applaud Congressman Goodlatte, Congresswoman Lofgren, and the 205 co-sponsors for re-engaging in this fundamentally important issue. House Bill 850, The Security and Freedom through Encryption "SAFE" Act, withstood many challenges last Congress and managed to move further than any other piece of legislation on the issue. This legislation should be enacted. SAFE is not a starting point as many would like to advocate, it is the solution. SAFE is not a marker, nor is it a rhetorical piece that keeps the issue alive: It is an answer.

Encryption has become an even more crucial component of communications in this digital age of high technology. The proliferation of communications and communications devices—phones, faxes, e-mails, palm pilots and laptops—make it even more critical that the vital information flowing across these mediums is secure. So privacy, security and the integrity of communications are most important to the average American.

I now want to turn to the issue of the export of encryption technology. There are very practical reasons for allowing the export of encryption technology. Perhaps the most important piece to understand here is that the definition of export is most appropriately viewed through the lens of electronic commerce. For example, did you know that it is illegal for you to use the Web browsers found on many of your laptop computers if you are outside of the United States? In fact, you are breaking the law if you even leave the country with the software installed that only uses strong encryption. This clear limitation on U.S. citizens only impacts our combined personal and professional lives by essentially limiting our mobility of efficiency. So, the issue here is not sending products manufactured here to foreign shores, but rather the mere use of technology by U.S. citizens of their laptop computers.

Also, encrypted messages, let's say medical information, cannot be securely encrypted here and then sent out of the country. Make no mistake, the information could still be sent, but not without a dramatic increase in the chance that a hacker could intercept or, maybe worse, alter the information in route. The impact for distance medicine is dramatic—all you need to do is imagine your loved one dying because the information sent was altered by a hacker.

The pure economic effect on this country is also important. We are, and have been, creating an artificial market for foreign competition by eliminating U.S. companies from the global marketplace. The current policy does not allow U.S. companies to compete internationally and with their absence several other companies have gotten their beginning and can now be competitive. Again, the specter of national security is raised. We are actively encouraging through misguided government policies the wholesale loss of U.S. intellectual capital and property. Those very companies that have driven the economic expansion of the last decade are being punished for being the best in the world. A unilateral preclusion of opportunity not only hamstring economic opportunity but is also simply unworkable. How do we benefit if other countries are producing the encryption that, according to the FBI, international terrorists may use? What are the chances that these foreign corporations will in any way cooperate with the United States?

Another historical pattern worth mentioning is the increasingly controlling nature of the rhetoric that those opposed to allowing citizens to protect their privacy have been using. Four years ago the FBI simply argued that strong encryption should not be exported. This position held for a couple years until they were pressed as to how these international concerns relate to their fundamental mission. At that point, rather than acknowledging the facts that robust encryption products, both hardware and software, are being manufactured around the world, the FBI decided that the better approach would be to suggest and support a domestic restriction on the use of encryption.

One of the most disturbing overtones of the encryption debate has been how flagrant the government has been in wanting to increasingly regulate the software and hardware market as those markets relate to encryption. The basic premise of the federal policy has been to regulate what the end user is allowed to operate. Remarkably the only people who get regulated in this environment are the law-abiding consumers who purchase their technology legally and legitimately. The criminal who uses encryption to cloak other crimes is in no way impacted. Why? Because robust encryption is easily available around the world. We are back to a governmental regime that at a fundamental level does not trust the people, that truly believes that only Big Brother can guide society, and that only an omnipotent federal government can make the correct choices.

Make no mistake that this regulation is broad and perhaps hidden at first blush. The indirect problem is that, in addition to the explicit regulation of the technology

industry, not allowing the free export of robust encryption puts the government firmly in charge of an individual's decision on how to protect their most private matters. Think of the current use of the typical personal computer, enhanced with access to the Internet. Would any of us have believed, even two years ago, the explosion we saw this holiday season in electronic commerce, the rapid growth in on-line banking, the dramatic switch to electronic trading of stock, the rapid transfer of medical documents to facilitate healthcare any where in the country, or even the greatly: increased numbers of taxpayers filing electronically? This is the information that must be protected in the best way possible, not only when being transferred domestically, but internationally as well. Why then should the federal government be in the business of exposing citizens to criminals, ranging from terrorists to hackers on a lark?

Seemingly, every time the opposition on this issue begins to lose on the facts they shift to increasingly restrictive and controlling policy positions. This unwillingness to rationally discuss and work through this issue causes a great deal of consternation and problems in trying to work toward an adequate solution. We may as well make note of the obvious—no one on this panel, in this room, or involved in this debate wants to see emboldened criminals, secure terrorists, or even cocky hackers succeed, but we cannot allow the federal government to diminish the fundamental freedoms of U.S. citizens so that the job is made easier. This concept is so basic, so necessary, that even a recent Simpson's episode could make an easily understandable point of the importance of the First, Fourth and Fifth Amendments. Those amendments mean something, they stand for our way of life, they are icons of our liberty, and because of that we do not strip them out of our lives or tear them away from the Bill of Rights so that criminals are more easily revealed.

Encryption technology is absolutely necessary for the future of electronic commerce. At the same time we must all accept the fact that the Internet is an international medium. Whether individually we like it or not, international commerce became astoundingly easier in the last several years. Policies that do not accept this basic fact are outmoded and wrongheaded from the moment of introduction. To arbitrarily limit private transactions by restricting the export of encryption only limits the success of every U.S. citizen. My feelings are so strong on this issue, in fact, that I have placed the discussion of encryption and its impact on electronic commerce as a central issue to be taken up by the Advisory Committee on Electronic Commerce. One of the express areas of direction given to the Commission is to look at the impact of Internet access on the state and local revenue base. The answer is clear that without the fair use of encryption the impact will be zero. Who would transmit sensitive financial, health, personal or taxation information if they did not have some belief that the information would not be intercepted by those intent on doing harm. These issues are fundamentally tied.

This raises yet another crucial issue - we must take measures to protect this country's critical infrastructures, including individual U.S. citizens. For years now we have heard only the most dire predictions of technological advances. You could be led to believe that the FBI's job has become impossible because of technology. Never do we hear how much easier technology has made law enforcement's mission throughout the years. Ironically, only a couple years ago the FBI was boasting, via Capitol Hill demonstrations, how more efficient it has become to catch traffickers in child pornography by going on-line and basically just asking for the material. This demonstration is all the more striking then when at the same time they claim that robust encryption use by criminals will hinder their efforts. They are also fond of touting the story of catching John Gotti because his men were not smart enough to essentially encrypt their discussions. In each case, the FBI got all the information they needed, whether because of dumb criminals or good detective work.

This is exactly why the FBI gained a reputation as the best crime-fighting force in the world—real detective work. The reputation would never have been earned if they were expending their energies looking to restrict civil liberties and attempting to make their jobs easier rather than just doing their jobs in the first place. I applaud the reputation of the FBI that it has earned as a crime fighting force out to protect citizens from criminals and others who intend harm to our way of life. However, at the same time I am discouraged by efforts that in any way expand governmental control of our lives, raise taxes, and potentially lead to abuses of power. Being a crime-fighter is an inherently difficult task, but the answer is not to stop that? flow of progress and advancements by those who are law-abiding.

Even worse than the arguments for a ban or limits on exports and a ban on domestic use, particularly from the taxpayer's perspective, have been the proposed solutions to allowing or the use of encryption. Often the argument is used that the FBI does support the use of robust encryption. Like a bad joke, the punch-line kills the setup. The FBI would agree to allow the export or domestic use of encryption

if only industry would agree to program a backdoor for the government to use to spy on individuals.

Another option has long been a failed scheme of handing a key to the FBI to unlock your files at its discretion. First, even by the most optimistic projections the costs of this key escrow are prohibitive and would cost the taxpayers billions and billions of dollars to fund this extreme expansion of police powers. Second, no one can say whether a scheme such as the government escrow of keys can even work on a scale anywhere near what is necessary. Third, the whole concept of key escrow is based on the flawed premise that customers would even consider purchasing products that allow for government intrusion. Not only is it technologically unworkable, but unmarketable customers do not want to open wide their private affairs to the government for analysis. Finally, we must always consider whether we want any organization, governmental or not, to hold the literal key to our most private affairs in one place—an ideal target for criminals.

One of the essential elements of the taxpayers' movement has been a belief in and personal responsibility and accountability. The government's current approach is antithetical to trust in people and to personal responsibility. We can no longer stand on the sidelines while government agencies, through their words or deeds, tear down the virtues of our society. We should all do what is necessary to promote those values that are central to who we are as the United States of America and, more importantly, as a people united in a quest for justice and liberty. We must restore our faith in individuals and the government must begin to reflect that the values of the American people should hold sway, not the values of a handful of Washington bureaucrats.

As many on the Committee know Americans for Tax Reform asks congressional members and challengers to take the Taxpayer's Protection Pledge each year. Another of ATR's major project is to calculate a Cost of Government Day as a follow-up to Tax Freedom Day. Cost of government takes into account all the costs of government such as regulation, not just taxation. Perhaps another calculation is relevant as well. A calculation of the costs that errant policies place on individuals, whether personal or corporate. Even if such a calculation never existed we should take great efforts to avoid regulation without factual basis, or policies based on fear of the few rather than belief in the many.

I strongly encourage those who do not feel comfortable with the arguments regarding encryption or the technology that drives encryption to become familiar with the arguments and seek an understanding of the technology. I personally work with many of the organizations represented here, and I think I speak for all of us in saying that we are confident that when the facts are presented that the answer is clear—we should be encouraging the use of robust encryption to protect each citizen in their everyday affairs, from simple personal transactions to the protection of the country.

Mr. GOODLATTE. We are now pleased to have with us Ms. Denning.

STATEMENT OF DOROTHY E. DENNING, PROFESSOR, COMPUTER SCIENCE DEPARTMENT, GEORGETOWN UNIVERSITY

Ms. DENNING. Thank you for the opportunity to testify.

I would like to make three points. First, the sad state of security on our country's information infrastructures won't be solved by the bill. This is because the security problems are not the result of using exportable encryption, but rather not using any encryption at all and not employing other essential safeguards. Sensitive data, including passwords, is routinely transmitted and stored in the clear. Of the thousands of incidents reported to the Computer Emergency Response Center, I am not aware of any that can be attributed to faulty encryption caused by export controls.

Security also requires much more than encryption. Encryption won't stop insiders from compromising proprietary information, siphoning money from bank accounts and planting destructive time bombs. It won't stop hackers from exploiting security holes in order to penetrate systems, deface Web pages and disrupt service. It won't prevent Trojan horses disguised as appealing software pro-

grams from entering users' computers and stealing passwords and other secrets while they are being typed.

In short, encryption is not a silver bullet. It must be augmented with other security measures, both technical and procedural. These include access controls, authentication, auditing, configuration management, vulnerability testing and repair, intrusion and misuse detection, malicious code detection, and security training and awareness.

Cryptographic technologies for authentication, which includes digital signatures, are not restricted for export and are at least as important as technologies for confidentiality protection.

My second point, related to the first, is that high levels of security can be achieved within the context of current export control policy. And I am not just talking about domestic users and U.S.-owned companies. An international enterprise can protect its assets by employing fully exportable encryption products that use 128 bit keys or longer and say "Made in U.S.A." Let me outline one way that can be done. I make two assumptions.

First, encryption must be considered within the context of a comprehensive enterprise-wide information security program that encompasses an organization's customers, suppliers, partners, shareholders, consultants and others who do business with the organization.

Second, an organization must be able to protect and retain control over its sensitive information whether in storage or in transit.

These two assumptions lead to an approach that is integrated with an enterprise access control policy. The approach ensures that authorized persons can get the keys needed to decrypt data, but that unauthorized persons cannot. It allows for immediate revocation of a user's decryption capabilities, and it provides an audit of every decryption so that policy violations can be detected. It does not require an organization to use third-party key management services. I recently reviewed a product that offers all of these protections and is approved for export.

My third and final point is that the current approach of gradually easing export controls may be optimal. If cryptography is over-regulated, our economic competitiveness, technology leadership, and civil liberties are at risk.

There can be little doubt that export controls drive some business overseas. If these controls are lifted entirely, law enforcement and national defense are at greater risk. Even though export controls do not prevent domestic or foreign adversaries from getting access to electronic encryption, they have influenced major product lines. Many criminals and terrorists use these products rather than going to the trouble of installing add-ons.

Today, Americans enjoy a strong and growing economy and a declining rate in crime. The Administration's encryption policy has impaired neither our economic competitiveness nor our ability to fight crime and provide for national defense. I am concerned that the bill, either in its current form or with amendments, such as those introduced in the last Congress to impose domestic regulations, could upset the delicate balance among our national interests.

In summary, H.R. 850 is not the key to safe electronic commerce or to protecting our critical infrastructures. This is because export controls are not the problem. It will help American companies compete in the global marketplace, but would also decrease industry incentives to accommodate law enforcement and national defense interests.

A few years ago the National Research Council conducted an extensive study of encryption policy at the request of Congress. They made several excellent recommendations, including the progressive relaxation but not elimination of export controls. Their proposed course of action is generally consistent with the steps taken by the Administration. A cautious approach to export globalization may be the best one.

Mr. GOODLATTE. Thank you, Professor Denning.
[The prepared statement of Ms. Denning follows:]

PREPARED STATEMENT OF DOROTHY E. DENNING, PROFESSOR, COMPUTER SCIENCE
DEPARTMENT, GEORGETOWN UNIVERSITY

Thank you for the opportunity to testify on H.R. 850, the "Security and Freedom Through Encryption (SAFE) Act." There are three points that I would like to make.

First, the sad state of security of our country's information infrastructures will not be solved by this bill. This is because the security problems are not the result of using exportable encryption, but rather of not using any encryption at all and of not employing other essential safeguards. Sensitive data, including passwords, is routinely transmitted and stored in the clear. Of the thousands of incidents reported to the Computer Emergency Response Center, I am not aware of any that can be attributed to faulty encryption caused by export controls.

Security also requires much more than encryption. Encryption will not stop insiders from compromising proprietary information, siphoning money from bank accounts, and planting destructive time bombs. It will not stop hackers from exploiting security holes in order to penetrate systems, deface Web pages, and disrupt service. It will not prevent Trojan horses, disguised as appealing software programs, from entering users' computers and stealing passwords and other secrets while they are being typed.

In short, encryption is not a silver bullet. It must be augmented with other security measures, both technical and procedural. These include access controls, authentication, auditing, configuration management, vulnerability testing and repair, intrusion and misuse detection, malicious code detection, and security training and awareness. Cryptographic technologies for authentication, including digital signatures, are not restricted for export and are at least as important as technologies for confidentiality protection.

My second point, which is related to the first, is that high levels of security can be achieved within the context of current export control policy. I'm not just talking about domestic users and U.S. owned companies. An international enterprise can protect its assets by employing fully exportable encryption products that use 128-bit keys or longer and say "Made in USA."

Let me outline one way that can be done. I make two assumptions. First, encryption must be considered within the context of a comprehensive enterprise-wide information security program that encompasses an organization's customers, suppliers, partners, shareholders, consultants, and others who do business with the organization. Second, an organization must be able to protect and retain control over its sensitive information, whether in storage or in transit. These two assumptions lead to an encryption approach that is integrated with an enterprise access control policy. The approach ensures that authorized persons can get the keys needed to decrypt data but that unauthorized persons cannot. It allows for immediate revocation of a user's decryption capabilities. And it provides an audit of every decryption so that policy violations can be detected. It does not require an organization to use third-party key management services, though this would be an option. I recently reviewed a product that offers these protections and is approved for export.

My third and final point is that the current approach of gradually easing export controls may be optimal. If cryptography is over-regulated, our economic competitiveness, technology leadership, and civil liberties are at risk. There can be little

doubt that export controls drive some business overseas. Yet if these controls are lifted entirely, law enforcement and national defense are at greater risk. Even though export controls do not prevent domestic or foreign adversaries from getting access to strong encryption, they have influenced major product lines. Many criminals and terrorists use these products rather than going to the trouble of installing add-ons.

Today, Americans enjoy a strong and growing economy and a declining rate in crime. The Administration's encryption policy has imperiled neither our economic competitiveness nor our ability to fight crime and provide for national defense. I am concerned that H.R. 850, either in its current form or with amendments such as those introduced in the last Congress to impose domestic regulations, could upset the delicate balance among our national interests.

In summary, H.R. 850 is not the key to safe electronic commerce or to protecting our critical infrastructures. This is because export controls are not the problem. The bill would help American companies compete in the global marketplace, but it would also remove industry incentives to accommodate law enforcement and national defense interests.

A few years ago, the National Research Council conducted an extensive study of encryption policy at the request of Congress. They made several excellent recommendations, including the progressive relaxation, but not elimination, of export controls. Their proposed course of action is generally consistent with the steps taken by the Administration. This cautious approach to export liberalization may be the best one.

Mr. GOODLATTE. We now are joined by Mr. Alan Davidson.

STATEMENT OF ALAN DAVIDSON, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DAVIDSON. Thank you, Mr. Chairman, and I would like to thank the committee for this opportunity to testify on behalf of the Center for Democracy and Technology in support of the SAFE bill.

CDT is a nonprofit public interest group dedicated to promoting civil liberties in new media. We have been supportive of the SAFE bill since it was first introduced, and we are pleased to be here once again. And I would like to take this opportunity to thank the Chair, Congresswoman Lofgren and the other cosponsors of the SAFE bill for their continued dedication to protecting privacy on-line, and I would also like to thank the subcommittee for its continued thoughtful exploration of what has been a very complex policy issue for the Internet.

CDT is here today because at its heart the encryption issue is about protecting privacy and our constitutional liberties on-line. We are setting the ground rules today for what kind of privacy we are going to have as Americans move their lives on-line, as they are doing in great number. Encryption is the essential tool for protecting security and privacy on-line. It is not the only tool, but we need strong encryption, not necessarily escrowed, recoverable encryption in order to be able to protect security in the Information Age. Nobody disputes the very serious law enforcement concerns here, but we believe that, on balance, encryption widely available, not necessarily recoverable, is needed to both promote privacy on-line and to protect public safety. Those arguments are laid out a little more fully in my written testimony.

What I would like to do is say a few words about where we are in 1999 on this issue.

Two years ago this subcommittee had a hearing in March 1997, almost exactly 2 years ago, that is strikingly similar to the hearing today—privacy advocates, industry representatives, Administration

officials making many of the same arguments that we have heard already today.

Two years later, in 1999, we find ourselves in a place where I would argue that the last 2 years have shown us that we need the SAFE bill more than ever, and the questions that were raised 2 years ago have gone unanswered. Two years ago Administration witnesses testified before this subcommittee that key recovery was going to be the policy compromise that would meet law enforcement desires and would be widely accepted. They said, quote, "We believe that key recovery encryption is going to become the worldwide standard."

Two years later, key recovery is not a worldwide standard. It has been greeted with great skepticism by the research community and by the marketplace and by the privacy community, and there are experts—experts have gone out where there is a study on the risks of key recovery, which I have submitted for the record, which raises serious doubts about any system that requires people to use encryption that can be broken open without their knowledge or consent. We have raised serious questions about that kind of proposal, and to date, they have gone basically un rebutted by the Administration.

Two years ago the Administration witnesses who were here in front of this subcommittee said that limits on exportable encryption were going to be strong enough to protect privacy. They said 56 bits was going to be enough to protect our security, and they said that cracking a 56-bit message would—and I am quoting from their testimony—"would take approximately 1 year and 87 days using a \$30 million supercomputer." Well, we have seen, as testimony has already shown today, that that was just not true, that in fact the Electronic Frontier Foundation, a nonprofit group, was able with a budget of \$250,000 to put together a machine that cracked a DES code in 56 hours. More recently, a similar group has done it in even less time.

I think the point is that there is a real danger in trying to say that we are going to set limits where people can crack and some people can't.

Congress was not necessarily given the right information about how easy it was to crack these codes. Two years ago the Administration testified here that the world was moving in the direction of U.S. policy, which is very important because the rest of the world doesn't go for key recovery and export controls. We don't have very much hope of them being very effective, and the fact that the Administration testified that a consensus is now emerging throughout much of the world that the way to achieve this balance is through the use of a key recovery and trusted third-party system. In fact, we have seen in the intervening 2 years that the world is not moving toward key recovery or other U.S. policies.

The European Union, the OECD, have failed to embrace key recovery despite substantial lobbying from the Administration. In recent months, countries such as Canada, Ireland, Finland, have gone 180 degrees the opposite way and have put in place encryption policies that actually allow for the free export of the encryption. And so I think what we are seeing is that you cannot

make a credible argument that the whole world is moving our way on this.

Two years ago, 50 million people were on-line, today 140 million people are on-line worldwide, nearly triple that number. As we have seen, the number one concern of all these people as they move their lives on-line is, how am I going to protect my privacy and my security on-line? The surveys show it. And we are trying to build a new medium here which has tremendous potential to reinvigorate our democracy, promote free speech on-line and promote economic growth; and we are not going to be able to do that if the people can't trust the network, and they won't trust the network if their privacy and security is not protected.

I look forward to your questions. I think the bottom line is that, on balance, the best way to protect public safety and promote constitutional liberties is by letting people get the security tools they need to protect themselves.

Thank you.

Mr. GOODLATTE. Thank you, Mr. Davidson.

[The prepared statement of Mr. Davidson follows:]

PREPARED STATEMENT OF ALAN DAVIDSON, STAFF COUNSEL, CENTER FOR
DEMOCRACY AND TECHNOLOGY

SUMMARY

The Center for Democracy and Technology (CDT) is pleased to have this opportunity once again to testify about encryption policy before the House Judiciary Committee. CDT is a non-profit public interest group dedicated to promoting civil liberties and democratic values on the Internet. CDT testified two years ago before this subcommittee in support of the Security and Freedom through Encryption (SAFE) Act, and we are happy to be here supporting the bill once again.

The last two years have made it more clear than ever that Congress should enact SAFE:

- *Developments of the last two years have confirmed the need for fundamental revision of U.S. encryption policy.* Since this Subcommittee's last encryption hearing in March 1997, 56-bit products have been cracked, key recovery has failed in the marketplace, and overseas the trend continues toward liberalization and away from further controls.
- *Over the last two years the Administration has made only incremental changes to a U.S. encryption policy that continues to jeopardize privacy online.* The Commerce Department regulations released in December do little to change the fundamental approach of export controls and incentives for key recovery.
- *Two years have shown that "key recovery" and "plaintext access" systems are not the solution.* Government-driven recovery systems require backdoor access to encrypted data, would impose significant new costs and risks on computer users, and would dramatically increase the surveillance capabilities of law enforcement at the expense of Constitutional liberties.
- *Today it is clear that national security and law enforcement are best served by policies supporting the widespread use of strong, unescrowed encryption.* Current U.S. policy dangerously impedes the deployment of accessible, easy-to-use, global security systems for the Internet that are needed to protect our privacy and our critical infrastructures.

Two years ago, there were about 50 million people on the Internet. Today that number has nearly tripled to 140 million people worldwide. Surveys indicate that the number one issue for people as they move online and begin to participate in electronic commerce is privacy and security. The Internet has vast potential to reinvigorate democracy, provide access to information, create new forms of community, and promote economic growth. But the promise of the Internet will not be met unless people can trust it. Widespread availability of strong, encryption without backdoors built in is needed to provide that trust.

It is for all of these reasons that Congress should adopt the SAFE Act of 1999. The Administration has proven unable to change its basic approach to encryption.

Congressional action is needed. The SAFE Act of 1999 improves on previous versions of the bill and would help provide Americans with the strong security and privacy products they so badly need. CDT commends Representatives Goodlatte and Lofgren, Chairman Coble, and the other cosponsors of the SAFE Act for their continued commitment to this essential debate about the electronic privacy of Americans.

DEVELOPMENTS OF THE LAST TWO YEARS HAVE CONFIRMED THE NEED FOR
FUNDAMENTAL REVISION OF U.S. ENCRYPTION POLICY

Two years ago, this committee held a hearing on encryption strikingly similar to the one being held today. Privacy advocates and industry representatives testified about the need for new encryption policies, and Administration officials argued that new regulations would allow U.S. policy to satisfy the competing interests at hand. In retrospect, the rapid pace of technical and marketplace developments over the last two years have made it clearer than ever before that the U.S. approach to encryption policy remains fundamentally flawed.

A. Exportable encryption has proven increasingly vulnerable.

Two years ago privacy advocates argued that 56-bit encryption, the maximum strength exportable for consumers without key recovery, was not secure enough for many applications. The Justice Department disputed this, claiming that "According to the National Security Agency's estimates, the average time needed to decrypt a single message by means of a brute force cryptoanalytic attack on 56-bit DES—a strength whose export we are now allowing—would be approximately one year and eighty-seven days using a thirty-million-dollar supercomputer."¹

Technical developments have proven these comments wrong. In the Fall of 1998, a group of researchers sponsored by the Electronic Frontier Foundation built a "DES Cracker" system for less than \$250,000 that broke a 56-bit key within 56 hours.² Less than six months later, in January 1999, encryption enthusiasts broke a 56-bit code in 22 hours using the DES Cracker and a network of distributed computers. If a non-profit and a group of part-time enthusiasts could develop such a system on a shoestring budget, we are only left to imagine what a foreign government, large corporation, or sophisticated criminal enterprise could do.

The U.S. Government has itself recognized the weakness in 56-bit encryption systems. In a January 1999 draft the National Institute of Standards and Technology (NIST) revised the encryption standard for government use from 56-bit DES to much stronger "Triple DES," citing the vulnerability of DES.³ Meanwhile, NIST has been leading efforts to create an Advanced Encryption Standard based on the 128-bit (and higher) algorithms that are becoming the world standard for online security. If the government does not trust 56-bit security, why should everyday computer users and companies be expected to rely on this weaker level of security?

B. Key recovery has not been widely accepted.

Two years ago before this Subcommittee, Administration witnesses touted key recovery as the compromise that met law enforcement desires and was "going to become the worldwide standard."⁴ In fact, since then government-driven key recovery has been greeted with great skepticism and widely discredited.

Research has revealed the vulnerabilities of key recovery systems, which create backdoors to plaintext without the notice or consent of an encryption user. A 1997 report by a group of encryption experts found that "[t]he deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated

¹*Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong., 2nd Sess., No. 9 (1997) (Statement of Robert S. Litt, Deputy Assistant Attorney General, Department of Justice).

²See ELECTRONIC FRONTIER FOUNDATION, *CRACKING DES* (1998).

³"With regard to use of single DES, exhaustion of the DES (i.e. breaking a DES encryption ciphertext by trying all possible keys) has become increasingly more feasible with technology advances. Following a recent hardware based DES key exhaustion attack, NIST can no longer support the use of single DES for many applications." 64 FED. REG. 10, 2625-2628 (1999) (proposed January 15, 1999).

⁴"[W]e believe that key recovery encryption is going to become the worldwide standard." *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong., 2nd Sess., No. 9 (1997) (Statement of Robert S. Litt, Deputy Assistant Attorney General, Department of Justice).

specifications will result in substantial sacrifices in security and greatly increased costs to the end-user." A year later, with no substantive response from within the Administration or the technical community, the same group of experts confirmed its findings still held true in June 1998.⁵ A copy of their report is being submitted to the Subcommittee along with this testimony.

Despite Administration predictions, the marketplace has shown little interest in even stored data recovery, and there is virtually no demand for key recovery for communications. To CDT's knowledge not one major key recovery encryption product is being widely used by consumers today.⁶

C. The world is not adopting U.S. encryption control policies.

Encryption controls are ultimately only effective if other countries control encryption products as well. In 1997, the Administration testified, "We have engaged in extensive international discussions on this topic over the last year, and a consensus is now emerging throughout much of the world that the way to achieve this balance is through the use of a 'key recovery' or 'trusted third party' system . . . We believe that key recovery will become the worldwide standard for users of the GII."⁷ To date, the opposite has been true. The OECD Cryptography Policy Guidelines and the Ministerial Declaration of the European Union, both released in 1997, failed to embrace key recovery despite lobbying by the U.S. government. In the past year, Canada, Ireland and Finland have announced encryption policies allowing free use and export of strong encryption products without key recovery. Even France, a country with sweeping controls on encryption use in the past, recently liberalized its policies.

D. Many in the national security community are now arguing for a change in U.S. policy.

Two years ago the national security community seemed to speak with one voice about the danger of strong encryption. Today there has been an increasing recognition of the cost of U.S. encryption policy. The last two years have seen Americans moving their lives online in unprecedented numbers. A Presidential Commission has highlighted the vulnerability of our nation's critical information infrastructure. Together these developments have underscored the importance today of securing the Internet, and deploying strong encryption to do so.

Today many in the national security and law enforcement community have acknowledged the limitations of current U.S. policy. As Sam Nunn testified before the Senate last year, "[I]f the deadlock continues as it is today, building the trust required between the public and private sectors in the broad area of infrastructure protection will be even more difficult."⁸ Nunn went on to note that "limiting the power of encryption over the long-haul is simply not going to be feasible. Senator Bob Kerrey, an early proponent of encryption controls, argued in an October 1998 speech that "the encryption debate has hobbled our efforts to write laws that enable our law enforcement and national security agencies to carry out their mission" and argued that it was time to "remove export restrictions on encryption products of any strength."⁹

E. The Administration has proven unable to engage in comprehensive reform.

The Department of Commerce has taken a step forward in its recently released encryption regulations, easing exports of 56-bit products and allowing export of strong encryption products to online merchants. However, U.S. policy remains focused on export controls and incentives to use key recovery. The mass market products needed by individual users remain controlled. The special relief for certain industry sectors, while surely welcome by those businesses, does

⁵ AN AD-HOC GROUP CRYPTOGRAPHERS AND COMPUTER SCIENTISTS, THE RISKS OF KEY RECOVERY, KEY ESCROW, & TRUSTED THIRD PARTY ENCRYPTION (1997). (Updated 1998 report available at <http://www.cdt.org/crypto/risks98/>.)

⁶ Cost may play a role. A recent study by the Business Software Alliance estimated the cost of key escrow systems at \$7.7 billion per year and \$38.5 billion over a five year period. BUSINESS SOFTWARE ALLIANCE, THE COST OF GOVERNMENT-DRIVEN KEY ESCROW ENCRYPTION (1998).

⁷ *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong., 2nd Sess., No. 9 (1997) (Statement of Robert S. Litt, Deputy Assistant Attorney General, Department of Justice).

⁸ *Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Senate Committee on the Judiciary*, 105th Cong., 2nd Sess. (March 17, 1998) (Statement of Sam Nunn, Co-Chair, Advisory Committee to the President's Commission on Critical Infrastructure Protection).

⁹ 144 CONG.REC. S12359 (1998).

little to change the encryption available to individual computer users or small organizations.

Taken together, these developments argue for a more comprehensive change to U.S. encryption policy, away from export controls and key recovery and towards a view where public safety is best protected by giving people the encryption tools they need to protect themselves on line. The past two years have also shown that such comprehensive reform will most likely only come with the involvement of Congress, as the interests in favor of current policy continue to dominate the Administration's approach to encryption.

U.S. ENCRYPTION POLICY CONTINUES TO DENY COMPUTER USERS ESSENTIAL TOOLS THAT PROTECT THEIR PRIVACY

Encryption protects privacy and prevents crime online. In early 1999, it is more clear than ever that the widespread use of encryption is of critical importance for public safety, national security, and law enforcement in the Information Age. The flow of sensitive information over the Internet leaves people increasingly vulnerable to the prying eyes of potential criminals, terrorists, or even foreign governments. Encryption gives people an easy and inexpensive way to protect that information. The need for encryption is becoming ever more acute as sensitive data is finding its way into electronic form:

- *Individuals need encryption* in order to trust the Internet with private data such as online banking, stock trades, medical records, electronic purchases, or personal communications.
- *Businesses need encryption* to protect their own proprietary information as it flows across vulnerable global networks.
- *The country needs encryption* to secure the critical information infrastructure governing such sensitive applications as our utilities, financial markets, or air traffic control networks.

If broad participation in electronic commerce and the information society is to become a reality, the adoption of encryption in most phases of electronic existence will be required.

Encryption is particularly important because of the inherent difficulties of securing the new digital media. The open, decentralized architecture that is the Internet's greatest strength also makes it hard to secure. Internet communications often travel "in the clear" over many different computers in an unpredictable path, leaving them open for interception. An email message from Washington to Geneva might pass through New York one day or Nairobi the next—leaving it susceptible to interception in any country where lax privacy standards leave it unprotected. Encryption provides one of the only ways for computer users to guarantee that their sensitive data remains secure regardless of what network—or what country—it might pass through.

Current U.S. policy prevents users from getting the encryption tools they need to protect security online. Today's export controls continue to limit the availability of strong encryption products both domestically and abroad. Such controls directly limit the availability of strong encryption products outside of the U.S., of particular concern to human rights groups and other organizations abroad. Export controls affect people in the U.S. when they communicate abroad, since they may be forced to use the lower levels of encryption available to parties worldwide. Most importantly, export controls have slowed the deployment of strong encryption standards. While some strong encryption products are available to consumers, export controls have largely slowed the seamless integration of good security systems into operating systems, network protocols, and many applications. Encryption should be easy for consumers; because of federal regulations, it is not.

The most recent December 1998 encryption regulations, while a welcome step forward by the Administration, do not change the fundamental premise of U.S. policy: export controls on all but the weakest encryption for mass market consumers, and strong incentives for the use of key recovery and plaintext access systems. The sector relief provided for foreign subsidiaries of U.S. companies, certain industries, and online merchants does little to provide regular consumers with strong encryption. Export controls remain a powerful incentive to adopt key recovery and plaintext access systems. The piecemeal relief offered by the regulations raises the question: When do regular people get to protect their privacy online?

Computer users remain at risk, awaiting the widespread deployment of encryption and facing increasing threats to their unprotected information.

GOVERNMENT-DRIVEN "KEY RECOVERY" AND "PLAINTEXT ACCESS" IS NOT A SOLUTION

The law enforcement community in general has variously endorsed "key escrow," "key recovery," and other forms of "plaintext access" as its favored approach to encryption policy. These variations on the failed "Clipper Chip" policy seek to guarantee third-party access to the keys for all encrypted communications and stored data without the notice or consent of the key owners. Such proposals have been greeted with much skepticism and concern from the global Internet community.

The attempt to institutionalize key recovery worldwide is a fundamental threat to privacy and security both domestically and abroad:

- *Global key access systems are vulnerable and unproven*—Centralized "back-door" access to the billions of keys used by millions of computer users will introduce new vulnerabilities into a medium that is already difficult to secure. In 1997, eleven renowned computer security experts issued a report on key recovery concluding that, "Building the secure infrastructure of the breathtaking scale and complexity demanded . . . is far beyond the experience and current competency of the field. Even if such an infrastructure could be built, the risks and costs of such a system may ultimately prove unacceptable." In 1998 these experts revisited the question and confirmed that their conclusions remained essentially unchallenged.¹⁰
- *The Fourth Amendment does not adequately protect key recovery systems both outside and inside of the U.S.*—The Administration has been unable to explain what legal standards will internationally protect the communications and data of U.S. individuals and businesses. Moreover, the Administration has indicated that the full Fourth Amendment standards of probable cause and notice would not apply to encryption keys held by third parties, even within the U.S. In a world where personal data is increasingly legally unprotected in the hands of third parties, key recovery systems further erode a person's ability to protect their privacy.
- *Recovery will never be appropriate for some applications*—For example, the American Association for the Advancement of Science has commented on the sensitive and increasingly important use of encryption by human rights advocates worldwide. "If keys can be recovered by the U.S. government, why should human rights organizations whose entire function is defined by abusive governments trust that their information will remain secure?"¹¹

Despite these concerns, current encryption regulations continue to give many encryption producers a Hobbesian choice: accept key recovery or be forced to export lower strength encryption. Moreover, proposals backed by the FBI in the past have sought to further force U.S. encryption users to adopt key recovery through a number of coercive regulations, including outright domestic mandates. While we are encouraged that the Administration appears to have backed away from mandatory domestic controls, we are wary that it has not denounced this approach. And even the current U.S. encryption policy based on key recovery and export controls threatens to leave global Internet users without the technical means to secure their communications or the international legal standards needed to protect their privacy.

NATIONAL SECURITY AND LAW ENFORCEMENT ARE BEST SERVED BY POLICIES SUPPORTING THE WIDESPREAD USE OF STRONG, UNESCROWED ENCRYPTION

The state of the emerging information society is making it increasingly clear that the law enforcement benefits of widespread encryption far outweigh the costs. The national security and law enforcement community has begun to recognize the limits of current U.S. policy. As Sam Nunn, Co-Chair of the Advisory Committee to the President's Commission on Critical Infrastructure Protection, noted in 1998 Senate testimony, "I do think we are in a different era of technology now and I do not think the nostalgia for the old-fashioned wiretap by law enforcement is going to be realistic in this age we are in now."¹²

¹⁰ AN AD-HOC GROUP CRYPTOGRAPHERS AND COMPUTER SCIENTISTS, THE RISKS OF KEY RECOVERY, KEY ESCROW, & TRUSTED THIRD PARTY ENCRYPTION (1997). (Updated 1998 report available at <http://www.cdt.org/crypto/risks98/>.)

¹¹ American Association for the Advancement of Science, Comments on Bureau of Export Administration Interim Rule on Encryption Controls (Feb. 7, 1997).

¹² *Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Senate Committee on the Judiciary*, 105th Cong., 2nd Sess. (March 17, 1998) (Statement of Sam Nunn, Co-Chair, Advisory Committee to the President's Commission on Critical Infrastructure Protection).

The benefits of current U.S. policy to law enforcement are uncertain. U.S. policy will not stop sophisticated criminals from using encryption to evade law enforcement. Strong, non-escrowed encryption is already available both inside and outside of the United States today. Foreign governments and criminals have access to these powerful tools and will be able to encrypt data despite continued export controls or key recovery. Furthermore, nothing in the Administration policies prevents users from "super-encrypting" communications even within a key recovery framework.

The law enforcement problems with encryption are important but more limited than claimed. Law enforcement faces a real, but narrowly focused, problem with encryption. Most encrypted information will still be accessible to law enforcement by legal process even in an encrypted world. For example, businesses will be still be required to produce the plaintext of encrypted business records under proper legal process. Stored information, corporate and business information, and even a great deal of electronic communication will most likely be largely available to law enforcement through legal process similar to that available today.

Important challenges remain for law enforcement interceptions of communications or seizures of data without notice to the party under surveillance. This narrower problem must be put into the context of the benefits provided by encryption and the costs associated with key recovery systems. Moreover, the information economy presents new and powerful tools and opportunities for law enforcement. Online interaction leaves a detailed trail of electronic transactions, credit card purchases, online communications, and Web-based clickstream data presenting new traffic analysis opportunities. In fact, law enforcement is operating today in a Golden Age of surveillance, with online collections of personal data offering unprecedented new tools to obtain evidence of criminal activity and raising important privacy concerns that must be dealt with as well.

U.S. policy is creating a deficit of trust around important issues we could all be working on together. U.S. policy stands in the way of a growing urgent need for strong encryption products that people trust. CDT believes that current U.S. policy dangerously impedes the deployment of accessible, easy-to-use, global security systems for the Internet that are needed to protect our privacy and our critical infrastructure.

On balance, national security demands strong encryption. CDT agrees with the conclusion of the National Research Council's major study of encryption, which argued in its 1996 encryption study, "On balance, the advantages of more widespread use of cryptography outweigh the disadvantages."¹³

CONCLUSION

U.S. policy stands in the way of a growing urgent need for strong encryption products that people trust. The past two years have shown that people and businesses are moving more and more of their lives, economic activities, and sensitive data online. The federal government has identified the vulnerability of our nation's critical information infrastructure. Strong encryption, without built-in backdoors, is an essential part of protecting that sensitive data and critical infrastructure.

That is why the SAFE Act is so important. In the current policy standoff between eroding law enforcement arguments and the emerging and acute privacy and security needs of the Information Age, it is Congressional action that is needed. Only Congress is in the position today to change U.S. encryption policy and get Americans the privacy and security tools they need. The private sector cannot do it. The Administration will not do it. The courts may do it, but not without a protracted struggle. Congress must act. CDT believes that immediate liberalization of export controls in the SAFE Act will help provide Americans on the Internet with the strong security and privacy they so badly need.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CDT is an independent, non-profit public interest policy organization in Washington, D.C. The Center's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in new digital communications media. The Center achieves its goals through policy development, public education, and coalition building. CDT also coordinates the Digital Privacy and Security Working Group (DPSWG), an ad hoc coalition of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues. Members of DPSWG assisted in the drafting of the Electronic Com-


¹³NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (1996).

munications Privacy Act in 1986 and since have been involved in ongoing policy work regarding privacy and security online.

House Rule XI, clause 2(g)(4) disclosures: Neither Alan Davidson nor the Center for Democracy and Technology have received any federal grant, contract or sub-contract in the current or preceding two fiscal years.



*THE RISKS OF
KEY RECOVERY, KEY ESCROW,
& TRUSTED THIRD PARTY
& ENCRYPTION*



Hal Abelson
Ross Anderson
Steven M. Bellovin
Josh Benaloh
Matt Blaze
Whitfield Diffie
John Gilmore
Peter G. Neumann
Ronald L. Rivest
Jeffrey I. Schiller
Bruce Schneier



ONE 1998

THE RISKS OF KEY RECOVERY, KEY ESCROW, & TRUSTED THIRD PARTY & ENCRYPTION 1998 ^[12]

Hal Abelson [1]
 Ross Anderson [2]
 Steven M. Bellovin [3]
 Josh Benaloh [4]
 Matt Blaze [5]
 Whitfield Diffie [6]
 John Gilmore [7]
 Peter G. Neumann [8]
 Ronald L. Rivest [9]
 Jeffrey I. Schiller [10]
 Bruce Schneier [11]

A variety of "key recovery," "key escrow," and "trusted third-party" encryption requirements have been suggested in recent years by government agencies seeking to conduct covert surveillance within the changing environments brought about by new technologies. This report examines the fundamental properties of these requirements and attempts to outline the technical risks, costs, and implications of deploying systems that provide government access to encryption keys.

- [1] MIT Laboratory for Computer Science/Hewlett-Packard <hal@mit.edu>
 [2] University of Cambridge <ross.anderson@cl.cam.ac.uk>
 [3] AT&T Laboratories - Research <sb@research.att.com>
 [4] Microsoft Research <benaloh@microsoft.com>
 [5] AT&T Laboratories - Research <mab@research.att.com>
 [6] Sun Microsystems <diffie@eng.sun.com>
 [7] <gn@toad.com>
 [8] SRI International <neurann@sri.com>
 [9] MIT Laboratory for Computer Science <rivest@lcs.mit.edu>
 [10] MIT Information Systems <jis@mit.edu>
 [11] Counterpane Systems <schneier@counterpane.com>
 [12] The latest version of this document can be found at <<http://www.cdt.org/crypto/risks98/>>
 in PostScript format <ftp://research.att.com/dist/mab/key_study.ps>
 and in ASCII text format <ftp://research.att.com/dist/mab/key_study.txt>

	ABSTRACT -----	1
	PREFACE -----	3
	EXECUTIVE SUMMARY -----	9
	GROUP CHARTER -----	10
1	BACKGROUND -----	11
1.1	Encryption and the Global Information Infrastructure	
1.2	"Key Recovery": Requirements and Proposals	
2	KEY RECOVERABILITY: Government vs. End-User Requirements -----	13
2.1	Communication Traffic vs. Stored Data	
2.2	Authentication vs. Confidentiality Keys	
2.3	Infrastructure: Local vs. Third-Party Control	
2.4	Infrastructure: Key Certification and Distribution vs. Key Recovery	
3	RISKS AND COSTS OF KEY RECOVERY -----	18
3.1	NEW VULNERABILITIES AND RISKS -----	18
3.1.1	New Paths to Plaintext	
3.1.2	Insider Abuse	
3.1.3	New Targets for Attack	
3.1.4	Forward Secrecy	
3.2	NEW COMPLEXITIES -----	20
3.2.1	Scale	
3.2.2	Operational Complexity	
3.2.3	Authorization for Key Recovery	
3.3	NEW COSTS -----	24
3.3.1	Operational Costs	
3.3.2	Product Design Costs	
3.3.3	End-User Costs	
3.4	TRADEOFFS -----	26
3.4.1	Key Recovery Granularity and Scope	
4	CONCLUSIONS -----	27
	THE AUTHORS -----	28

INTRODUCTION

One year after the 1997 publication of the first edition of this report, its essential finding remains unchanged and substantively unchallenged: The deployment of key recovery systems designed to facilitate surreptitious government access to encrypted data and communications introduces substantial risks and costs. These risks and costs may not be appropriate for many applications of encryption, and they must be more fully addressed as governments consider policies that would encourage ubiquitous key recovery.

Our 1997 "Risks" report was designed to stimulate a public, technical debate and analysis that, in our judgment, must precede any responsible policy decision that could result in the wide-scale deployment of key recovery systems. While there are numerous and important economic, social, and political issues raised by key recovery, the report's analysis was confined to the technical problems created by deployment of key recovery systems designed to meet government access specifications. As of mid-1998, no substantive response addressing these technical concerns has been offered.

While efforts have been made over the last year to design key recovery systems for commercial purposes, they do not alleviate the concerns raised by deployment at the scale and in the manner required to meet government demands. The design of secure key recovery systems remains technically challenging, and the risks and costs of deploying key recovery systems are poorly understood. Most significantly, government demands for access place additional requirements on key recovery systems, including covert access, ubiquitous adoption, and rapid access to plaintext. There is good reason to believe that these additional requirements amplify the costs and risks of key recovery substantially.

In the past year, the importance of cryptography for protecting computing and communications systems has gained broader recognition among the public and within industry. Most presently-deployed encryption systems support rather than hinder the prevention and detection of crime. Encryption helps to protect burglar alarms, cash machines, postal meters, and a variety of vending and ticketing systems from manipulation and fraud; it is also being deployed to facilitate electronic commerce by protecting credit card transactions on the Net and hindering the unauthorized duplication of digital audio and video. However, the deployment of encryption (and other information protection mechanisms) is still patchy. Most automatic teller machine transactions are protected by encryption, but transactions made by bank staff (which can involve much larger

amounts of money) are often not protected. Most Internet electronic mail is still sent "in the clear" and is vulnerable to interception. Most cellular telephone calls in the U.S. are still sent over the air without the benefit of strong encryption. The situation is similar in other areas.

Members of the law enforcement and intelligence communities continue to express concern about widespread use of unescrowed cryptography. At the same time, these communities have expressed increasing alarm over the vulnerability of "critical infrastructure." But there is a significant risk that widespread insertion of government-access key recovery systems into the information infrastructure will exacerbate, not alleviate, the potential for crime and information terrorism. Increasing the number of people with authorized access to the critical infrastructure and to business data will increase the likelihood of attack, whether through technical means, by exploitation of mistakes or through corruption. Furthermore, key recovery requirements, to the extent that they make encryption cumbersome or expensive, can have the effect of discouraging or delaying the deployment of cryptography in increasingly vulnerable computing and communications networks.

The technical concerns about key recovery and trusted third-party systems in 1998 remain largely unchanged from our 1997 analysis. We specifically do not address questions of how and whether key recovery might benefit law enforcement and whether there are alternatives to key recovery that might achieve equal or greater benefits. However, the predictable costs and risks of key recovery, particularly when deployed on the scale desired by law enforcement, are very substantial. The onus is on the advocates of key recovery to make the case that the benefits outweigh these substantial risks and costs.

BACKGROUND

Cryptography policy is a complex area, with scientific, technical, political, social, business, and economic dimensions. Our report is focused on the technical and economic aspects of the key recovery problem. In particular, we concentrate on the question of whether secure key recovery systems that meet government specifications are technically possible, and, if so, what additional costs and risks we would expect such systems to entail.

For the purposes of this report, "key recovery" systems are characterized by the presence of some mechanism for obtaining exceptional access to the plaintext of encrypted traffic. Key recovery might serve a wide spectrum of access requirements, from a backup mechanism that ensures a business' continued access to its own encrypted archive in the event keys are lost, to providing covert law enforcement access to wiretapped encrypted telephone conversations. Many of the costs, risks, and complexities inherent in the design, implementation, and operation of key recovery systems depend on the access requirements around which the system is designed.

We focus specifically on key recovery systems designed to meet government access specifications. These specifications diverge in important ways from the needs of commercial or individual encryption users:

1. **Access without end-user knowledge or consent** — Few commercial users need (or want) covert mechanisms to recover keys or plaintext data they protect. On the contrary, business access rules are usually well known, and audit is a very important safeguard against fraud and error. Government specifications require mechanisms that circumvent this important security practice.
2. **Ubiquitous adoption** — Government seeks the use of key recovery for all encryption, regardless of whether there is benefit to the end-user or whether it makes sense in context. In fact, there is little or no demand for key recovery for many applications and users. For example, the commercial demand for recovery of encrypted communications is extremely limited, and the design and analysis of key recovery for certain kinds of communications protocols is especially difficult.
3. **Fast paths to plaintext** — Law enforcement demands fast (near real-time), 24-hour-a-day, 365-day-a-year access to plaintext, making it impossible to employ the full range of safeguards that could ameliorate some of the risks inherent in commercial key recovery systems.

These special demands significantly increase the risks and costs identified in this report. While key recovery systems designed to meet commercial needs also have associated costs and risks, we address most of our attention to the effects caused by the special demands — rapid, covert access to all encrypted data — of government-access systems.

CRITIQUES OF THE 1997 REPORT -----

As noted above, there has been no published substantive response to the concerns we raised in our 1997 report. The few critiques of which we are aware avoid addressing the issues in any technical depth, and they mischaracterize our findings:

1. "The report assumes a single, massive, centralized infrastructure" — Although some key recovery proposals are centralized, our report examined key recovery generally, whether it takes the form of a single government-controlled infrastructure or many decentralized, private sector systems. The risks and costs identified arise chiefly from the functional requirements of key recovery (and especially on the scale sought by government), not from the manner in which these requirements are implemented.

2. "The report claims key recovery is impractical, but in fact industry, notably members of the Key Recovery Alliance (KRA), is already developing key recovery products" — While some companies are developing key recovery products, it is not at all clear that these products will achieve the ubiquitous scale envisioned by government. Many of these systems address narrow applications, where added risks and costs may be appropriate, or are at least easier to measure and weigh against end-user benefits.

3. "Key recovery's benefits outweigh its costs" — Key recovery may have benefits for some users and for government. Ultimately, weighing these benefits and costs is an exercise for the marketplace and policymakers, and is outside the scope of this report. In this report we have merely tried to explain why the costs will be substantial.

KEY RECOVERY IN 1998

As of mid-1998 we have seen a wide range of government, industry, and academic efforts toward specifying, prototyping, and standardizing key recovery systems that meet government specifications. Some of industry's efforts were stimulated by U.S. government policies that offer more favorable export treatment to companies that commit to designing key recovery features into future products, and by U.K. government moves to link the licensing of certification authorities to the use of key recovery software.

Yet despite these incentives, and the intense interest and effort by research and development teams, neither industry nor government has yet produced a key recovery architecture that universally satisfies both the demands of government and the security and cost requirements of encryption users.

The commercial key recovery products in existence today do not reconcile the conflict between commercial requirements and government specifications. In the absence of government pressure, commercial key recovery features are by their nature of interest primarily to business operations willing to pay a significant premium to ensure continued access to stored data maintained only in encrypted form. Even within enterprises that do require key recovery products, many of the applications of encryption (such as communication traffic) are known in advance not to require recoverability and therefore would not be designed to use a key recovery system.

Another problem is that the most secure and economical commercial key recovery systems do not support the real-time, third-party, covert access sought by governments in order to support surveillance. In particular, "self-escrow" by an individual does not meet government access demands. The third-party nature and global reach implied by these government demands make key recovery systems a much more difficult, expensive, and risky proposition than a facility for internal, off-line recovery in a business enterprise. For example, most organizations keep backups

in the form of plaintext on magnetic media in physically protected premises. Similarly, organizations that keep encrypted data might naturally be best served by storing backup keys in a bank safe deposit box. A requirement for near-real-time access would preclude this approach, however prudent or appropriate.

Any access-time requirement carries with it special risks. In particular, some sort of network technology will generally be required. Such a network, which must link a large number of law enforcement agencies with different key recovery centers, would be extraordinarily difficult to secure.

The current attention in the U.S. on the problem of securing critical infrastructure, such as telephone networks, power grids, national banking networks and air traffic control systems, underscores the problem of managing risk in key recovery. The systems that support critical infrastructure, which are increasingly reliant on open networks and information systems, are among the most important current and future applications of cryptography. The complexity and increased risk introduced with key recovery would make critical infrastructure protected by cryptography more vulnerable to the kinds of sophisticated attackers that pose the most serious threats to these systems.

In the 1997 edition of this report, we observed that many of the complexities, risks, and costs that make government-access key recovery difficult and expensive to build and operate in a secure manner arise from the requirements themselves. They are largely independent of the engineering details of particular systems. It is not difficult to design and implement small-scale systems that successfully recover keys or plaintext according to some access policy; indeed, many organizations already have in place practices that ensure the continued availability of their data. The difficulties arise from ensuring that a large-scale system, or system of systems, does not inadvertently or maliciously leak data.

Government specifications for key recovery systems for export approval are focused on the easier problem of ensuring that keys are recoverable when authorized. They do not address or give techniques for the far harder problem of ensuring against unauthorized disclosure of data. The design and construction of prototype key recovery systems that satisfy government specifications for export, therefore, are not sufficient to demonstrate that these systems can be operated securely, in an economical manner, on a large scale, or without introducing unacceptable new risks. Any assessment of a proposed system must take into account a broad range of design, implementation, operation, and policy considerations.

As of mid-1998, we are aware of no key recovery proposals that have undergone analysis of the kind required. On the other hand, as our report notes, there are compelling reasons to believe that, given the state of the art in cryptology and secure systems engineering, government-access key recovery is not compatible with large scale, economical, secure cryptographic systems.

THE RISKS OF KEY RECOVERY, KEY ESCROW, & TRUSTED THIRD PARTY & ENCRYPTION 1998

Hal Abelson
 Ross Anderson
 Steven M. Bellovin
 Josh Benaloh
 Matt Blaze
 Whitfield Diffie
 John Gilmore
 Peter G. Neumann
 Ronald L. Rivest
 Jeffrey I. Schiller
 Bruce Schneier

A variety of "key recovery," "key escrow," and "trusted third-party" encryption requirements have been suggested in recent years by government agencies seeking to conduct covert surveillance within the changing environments brought about by new technologies. This report examines the fundamental properties of these requirements and attempts to outline the technical risks, costs, and implications of deploying systems that provide government access to encryption keys.

The deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in

security and greatly increased costs to the end-user. Building the secure computer-communication infrastructures necessary to provide adequate technological underpinnings demanded by these requirements would be enormously complex and is far beyond the experience and current competency of the field. Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable. In addition, these infrastructures would generally require extraordinary levels of human trustworthiness.

These difficulties are a function of the basic government access requirements proposed for key-recovery

encryption systems. They exist regardless of the design of the recovery systems — whether the systems use private-key cryptography or public-key cryptography; whether the databases are split with secret-sharing techniques or maintained in a single hardened secure facility; whether the recovery services provide private keys, session keys, or merely decrypt specific data as needed; and whether there is a single centralized infrastructure, many decentralized infrastructures, or a collection of different approaches.

All key-recovery systems require the existence of a highly sensitive and highly-available secret key or collection of keys that must be maintained in a secure manner over an extended time period. These systems must make decryption information quickly accessible

to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive — and potentially too insecure and too costly for many applications and many users.

Attempts to force the widespread adoption of key-recovery encryption through export controls, import or domestic use regulations, or international standards should be considered in light of these factors. The public must carefully consider the costs and benefits of embracing government-access key recovery before imposing the new security risks and spending the huge investment required (potentially many billions of dollars, in direct and indirect costs) to deploy a global key recovery infrastructure.

This report stems from a collaborative effort to study the technical implications of controversial proposals by the United States and other national governments to deploy large-scale “key recovery” systems that provide third-party access to decryption keys [13]. Insofar as is possible, we have considered the impact of these policies without regard to individual encryption schemes or particular government proposals. Rather, we have attempted to look broadly at the essential elements of key recovery needed to fulfill the expressed requirements of governments (as distinct from the features that encryption users might desire).

This report considers the general impact of meeting the government’s requirements rather than the merits of any particular key recovery system or proposal that meets them. Our analysis is independent of whether the key-recovery infrastructure is centralized or widely distributed.

We have specifically chosen not to endorse, condemn, or draw conclusions about any particular regulatory or legislative proposal or commercial product. Rather, it is our hope that our findings will shed further light on the debate over key recovery and provide a long-needed

[13] This report grew out of a group meeting at Sun Microsystems in Menlo Park, CA in late January 1997, including many of the authors and also attended by Ken Bass, Alan Davidson, Michael Fromkin, Shabbir Safdar, David Sobel and Daniel Weitzner. The authors thank these other participants for their contributions, as well as the Center for Democracy and Technology for coordinating this effort and assisting in the production of this final report.

baseline analysis of the costs of key recovery as policymakers consider embracing one of the most ambitious and far-reaching technical deployments of the information age.

Although there are many aspects to the debate on the proper role of encryption and key recovery in a free society, we have chosen to focus entirely on the technical issues associated with this problem rather than on more general political or social questions. Indeed, many have suggested that the very notion of a pervasive

government key recovery infrastructure runs counter to the basic principles of freedom and privacy in a democracy and that that alone is reason enough to avoid deploying such systems. This reasoning is independent of whether the key-recovery infrastructure is centralized or widely distributed. The technical nature of our analysis should not be interpreted as an endorsement of the social merits of government key recovery; in fact, we encourage vigorous public debate on this question.

1.1 Encryption and the Global Information Infrastructure

The Global Information Infrastructure promises to revolutionize electronic commerce, reinvigorate government, and provide new and open access to the information society. Yet this promise cannot be achieved without information security and privacy. Without a secure and trusted infrastructure, companies and individuals will become increasingly reluctant to move their private business or personal information online.

The need for information security is widespread and touches all of us, whether users of information technology or not. Sensitive information of all kinds is increasingly finding its way into electronic form. Examples include:

- Private personal and business communications, including telephone conversations, FAX messages, and electronic mail;
- Electronic funds transfers and other financial transactions;

- Sensitive business information and trade secrets;
- Data used in the operation of critical infrastructure systems such as air traffic control, the telephone network, or the power grid; and
- Health records, personnel files, and other personal information.

Electronically managed information touches almost every aspect of daily life in modern society. This rising tide of important yet unsecured electronic data leaves our society increasingly vulnerable to curious neighbors, industrial spies, rogue nations, organized crime, and terrorist organizations.

Paradoxically, although the technology for managing and communicating electronic information is improving at a remarkable rate, this progress generally comes at the expense of intrinsic security. In general, as information technology improves and becomes faster, cheaper, and easier to use, it becomes less possible to control (or even identify) where sensitive data flows, where documents originated, or who is at the other end of the telephone. The basic communication

Infrastructure of our society is becoming less secure, even as we use it for increasingly vital purposes. Cryptographic techniques more and more frequently will become the only viable approach to assuring the privacy and safety of sensitive information as these trends continue.

Encryption is an essential tool in providing security in the information age. Encryption is based on the use of mathematical procedures to scramble data so that it is extremely difficult — if not virtually impossible — for anyone other than authorized recipients to recover the original “plaintext.” Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure networks. Only parties with the correct decryption “key” (or keys) are able to recover the plaintext information.

Highly secure encryption can be deployed relatively cheaply, and it is widely believed that encryption will be broadly adopted and embedded in most electronic communications products and applications for handling potentially valuable data. [14] Applications of cryptography include protecting files from theft or unauthorized access, securing communications from interception, and enabling secure business transactions. Other cryptographic techniques can be used to guarantee that the contents of a file or message have not been altered (integrity), to establish the identity of a party (authentication), or to make legal commitments (non-repudiation).

In making information secure from unwanted eavesdropping, interception, and theft, strong encryption has an ancillary effect: It becomes more

difficult for law enforcement to conduct certain kinds of surreptitious electronic surveillance (particularly wiretapping) against suspected criminals without the knowledge and assistance of the target. This difficulty is at the core of the debate over key recovery.

1.2 “Key Recovery”: Requirements and Proposals

The United States and other national governments have sought to prevent widespread use of cryptography unless “key recovery” mechanisms guaranteeing law enforcement access to plaintext are built into these systems. The requirements imposed by such government-driven key recovery systems are different from the features sought by encryption users, and ultimately impose substantial new risks and costs.

Key recovery encryption systems provide some form of access to plaintext outside of the normal channel of encryption and decryption. Key recovery is sometimes also called “key escrow.” The term “escrow” became popular in connection with the U.S. government’s Clipper Chip initiative, in which a master key to each encryption device was held “in escrow” for release to law enforcement. Today the term “key recovery” is used as generic term for these systems, encompassing the various “key escrow,” “trusted third-party,” “exceptional access,” “data recovery,” and “key recovery” encryption systems introduced in recent years. Although there are differences between these systems, the distinctions are not critical for our purposes. In this report, the general term “key recovery” is used in a broad sense, to refer to any system for assuring third-party (government) access to encrypted data.

[14] The National Research Council’s comprehensive 1996 report on cryptography includes a detailed examination of the rising importance of encryption. National Research Council, *Cryptography’s Role in Securing the Information Society* (1996).

Key recovery encryption systems work in a variety of ways. Early "key escrow" proposals relied on the storage of private keys by the U.S. government, and more recently by designated private entities. Other systems have "escrow agents" or "key recovery agents" that maintain the ability to recover the keys for a particular encrypted communication session or stored file; these systems require that such "session keys" be encrypted with a key known by a recovery agent and included with the data. Some systems split the ability to recover keys among several agents.

Many interested parties have sought to draw sharp distinctions among the various key recovery proposals. It is certainly true that several new key recovery systems have emerged that can be distinguished from the original "Clipper" proposal by their methods of storing and recovering keys. However, our discussion takes a higher-level view of the basic requirements of the problem rather than the details of any particular scheme; it does not require a distinction between

"key escrow," "trusted third-party," and "key recovery." All these systems share the essential elements that concern us for the purposes of this study:

- A mechanism, external to the primary means of encryption and decryption, by which a third party can obtain covert access to the plaintext of encrypted data.
- The existence of a highly sensitive secret key (or collection of keys) that must be secured for an extended period of time.

Taken together, these elements encompass a system of "ubiquitous key recovery" designed to meet law enforcement specifications. While some specific details may change, the basic requirements most likely will not: they are the essential requirements for any system that meets the stated objective of guaranteeing law enforcement agencies timely access, without user notice, to the plaintext of encrypted communications traffic.

Key recovery systems have gained currency due to the desire of government intelligence and law enforcement agencies to guarantee that they have access to encrypted information without the knowledge or consent of encryption users. A properly designed cryptosystem makes it essentially impossible to recover encrypted data without knowledge of the correct key. In some cases this creates a potential problem for the users of encryption themselves; the cost of keeping unauthorized parties out is that if

keys are lost or unavailable at the time they are needed, the owners of the encrypted data will be unable to make use of their own information. It has been suggested, therefore, that industry needs and wants key recovery, and that the kind of key recovery infrastructure promoted by the government would serve the commercial world's needs for assuring availability of its own encrypted data. Several recent government proposals (along with commercial products and services designed to meet the government's

requirements) have been promoted as serving the dual role of assuring government access as well as "owner" access to encrypted data. However, the requirements of a government and the requirements of the commercial world and individual users are very different in this regard, so different that, in fact, there is little overlap between systems that address these two problems.

The ultimate goal of government-driven key recovery encryption, as stated in the U.S. Department of Commerce's recent encryption regulations, "envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items." [15.] The requirements put forward to meet law enforcement demands for such global key recovery systems include:

- Third-party/government access without notice to or consent of the user. Even so-called "self-escrow" systems, where companies might hold their own keys, are required to provide sufficient insulation between the recovery agents and the key owners to avoid revealing when decryption information has been released.
- Ubiquitous international adoption of key recovery. Key recovery helps law enforcement only if it is so widespread that it is used for the bulk of encrypted stored information and communications, whether or not there is end-user demand for a recovery feature.
- High-availability, around-the-clock access to plaintext under a variety of operational conditions. Law enforcement seeks the ability to obtain

decryption keys quickly — within two hours under current U.S. and other proposed regulations [16.] Few commercial encryption users need the ability to recover lost keys around the clock, or on such short notice.

- Access to encrypted communications traffic as well as to encrypted stored data. To the extent that there is commercial demand for key recovery, it is limited to stored data rather than communications traffic.

In fact, the requirements of government key recovery are almost completely incompatible with those of commercial encryption users. The differences are especially acute in four areas: the kinds of data for which recovery is required, the kinds of keys for which recovery is required, the manner in which recoverable keys are managed, and the relationship between key certification and key recovery. Government key recovery does not serve private and business users especially well; similarly, the key management and key recoverability systems naturally arising in the commercial world do not adapt well to serve a government.

2.1 Communication Traffic vs. Stored Data

While key "recoverability" is a potentially important added-value feature in certain stored data systems, in other applications of cryptography there is little or no user demand for this feature. In particular, there is hardly ever a reason for an encryption user to want to recover the key used to protect a communication

[15] Dept. of Commerce, "Interim Rule on Encryption Items," Federal Register, Vol. 61, p. 68572 (Dec. 30, 1996)

[16] For example, the recent British "Trusted Third-Party" system proposes similar law enforcement demands, requiring one hour turnaround time for TTP recovery agents. See U.K. Department of Trade and Industry, "LICENSING OF TRUSTED THIRD-PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES," (March 1997) (Public Consultation Paper).

session such as a telephone call, FAX transmission, or Internet link. If such a key is lost, corrupted, or otherwise becomes unavailable, the problem can be detected immediately and a new key negotiated. There is also no reason to trust another party with such a key. Key recoverability, to the extent it has a private-sector application at all, is useful only for the keys used to protect irreproducible stored data. There is basically no business model for other uses, as discussed below.

In stored data applications, key recovery is only one of a number of options for assuring the continued availability of business-critical information. These options include sharing the knowledge of keys among several individuals (possibly using secret-sharing techniques), obtaining keys from a local key registry that maintains backup copies, careful backup management of the plaintext of stored encrypted data, or, of course, some kind of key recovery mechanism. The best option among these choices depends on the particular application and user.

Encrypted electronic mail is an interesting special case, in that it has the characteristics of both communication and storage. Whether key recovery is useful to the user of a secure E-mail system depends on design of the particular system.

The government, on the other hand, proposes a key recovery infrastructure that applies to virtually all cryptographic keys, including (especially) those used to protect communications sessions.

2.2 Authentication vs. Confidentiality Keys

Although cryptography has traditionally been associated with confidentiality, other cryptographic mechanisms, such as authentication codes and digital signatures, can ensure that messages have not been tampered with or forged. Some systems provide properties analogous to those of handwritten signatures, including “non-repudiation” — the recipient can prove to a third party that a message was signed by a particular individual.

Much of the promise of electronic commerce depends on the ability to use cryptographic techniques to make binding commitments. Yet some key recovery schemes are designed to archive authentication and signature keys along with confidentiality keys. Such schemes destroy the absolute non-repudiation property that makes binding commitments possible. Furthermore, there are simply no legitimate uses for authentication or signature key recovery. The private sector requires distinct keys for all signers, even when two or more individuals are authorized to send a given message; without that, the ability to audit transactions is destroyed. Government surveillance does not require the recovery of signature keys, either.

However, it is difficult to exclude authentication and signature keys from a key recovery infrastructure of the kind proposed by the government, because some keys are used for both signature and encryption. [17] Nor is it sufficient to exclude from the recovery system keys used only to protect financial transactions, since many electronic commerce schemes use keys that

[17] In fact, it is technically straightforward for two parties to use their authentication keys to negotiate encryption keys for secure communication. Any system that distributes trusted authentication keys would ipso facto serve as an infrastructure for private communication that is beyond the reach of government surveillance.

are general in scope. The same key might be used, for example, to encrypt personal electronic mail as well as to electronically sign contracts or authorize funds transfers.

It has been claimed that non-availability of a signature key can be a serious problem for the owner, who will then no longer be able to sign messages. But common practice allows for the revocation of lost keys, and the issuance of new keys with the same rights and privileges as the old ones. Recovering lost signature and authentication keys is simply never required.

2.3 Infrastructure: Local vs. Third-Party Control

For a key recovery scheme to be of value to the encryption user, it must allow tight control over depositing, recovering, and maintaining keys, tied to the user's own practices and requirements. Generally, only a small number of individuals will need the ability to recover any individual key, often working in the same location and personally known to one another. When a key does need to be recovered, it will frequently be a local matter, similar to the replacement of a misplaced office key or restoring a computer file with a backup copy. The hours at which the key recovery might take place, the identification of the individuals authorized for a particular key, the policy for when keys should be recovered, and other basic operational procedures will vary widely from user to user, even within a single business. Particularly important is the control over when and how "recoverable" keys are destroyed when they are no longer needed, especially for keys associated with sensitive personal and business records.

Similarly, there is usually no business need for secrecy in the recovery of keys or for the ability to obtain keys without the initial cooperation of the user. Key recovery is used in a business environment, it would generally be one component of the overall data management policy of that business. Users would normally be trusted to participate in assuring recoverability of their own keys, assisted by local management practices and supervision. When a key must be recovered, it will usually be because the users themselves realize that they do not have a copy of the correct key or because the keyholder is no longer available. Even the frequently-cited hypothetical example of the disgruntled employee who refuses to decrypt important files is probably most reliably and economically dealt with through business data management practices (such as management supervision and backup of business-critical plaintext) that do not require any centralized, standard key recovery mechanism. Even in this (rather unusual) case, there is no need to hide from the user the fact that a key has been recovered.

The U.S. government, on the other hand, proposes key recovery schemes that by their nature do not allow local control. The government's requirement for the ability to covertly recover keys on short notice and without notice to the key owner must almost by definition be implemented by a third party whose procedures are entirely divorced from those of the users. Even when the government permits an organization to manage its own keys, the key recovery agent will have to be fairly centralized and remote from the actual users. This requirement eliminates the first line of defense against misuse of key recovery: the vigilance of the most concerned party — the key owner.

2.4 Infrastructure: Key Certification and Distribution vs. Key Recovery

As electronic commerce and encryption use becomes more widespread, some form of "Certification Authorities" (CAs) will be needed in some applications to help identify encryption users. A CA is a trusted party that vouches for the identity (or some other attribute) of an encryption user. It is widely believed that development and use of certification authorities will be essential for secure and trusted electronic exchanges — and, consequently, will become a prerequisite to participation in electronic commerce and online communications. [18]

Although superficially similar, in that they are both concerned with key management, the nature of key recovery is completely different from that of key certification. The most important function of a certification authority is to certify the public keys used in digital signatures; key recovery, on the other hand, is concerned with keys used for confidentiality. More importantly, the operation of a certification authority does not require handling sensitive user data; a CA generally handles only users' public keys and never learns the associated secret keys. If a CA's secret key is compromised or revealed, the only direct damage is that the certificates from it can be forged. On the other hand, if a key recovery agent's secrets are compromised, the damage can be far greater and

more direct: every user of that recovery agent might have its own secrets compromised.

Certification can (and currently does) exist without any form of key recovery. Conversely, a key recovery infrastructure can exist completely independently of any key certification infrastructure.

Several recent government proposals have attempted to associate key recovery with key certification. This proposed linkage between CAs and key recovery makes no sense technically. On the contrary, such linkages have serious liabilities. It is not even clear whether such a system would work. To the extent it might require depositing keys used for signature and identification, such systems create additional security risks; there is no justification (even given government law enforcement requirements) for third-party access to signature keys that, if compromised, could be used to impersonate people, or to forge their digital signatures. In fact, attempts at achieving key recovery through a certification infrastructure would likely be ineffective at meeting the goals of law enforcement. Many (indeed, most) encryption keys are not certified directly, and therefore would be beyond the reach of a certification-based recovery system.

[18] There is a great deal of debate about the appropriate role of government in regulating CAs. CAs may ultimately be large, centralized, or even government-certified entities, or smaller, locally-trusted entities. At this early stage in their deployment, no consensus has emerged on what government role is appropriate. For an excellent overview of the debate over CA regulation, see Michael Froomkin, "The Essential Role of Trusted Third-Parties in Electronic Commerce," 75 Oregon L. Rev. 49 (1996).

Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. Key recovery degrades many of the protections available from encryption, such as absolute control by the user over the means to decrypt data. Furthermore, a global key recovery infrastructure can be expected to be extraordinarily complex and costly.

The impact of key recovery can be considered in at least three dimensions:

Risk — The failure of key recovery mechanisms can jeopardize the proper operation, underlying confidentiality, and ultimate security of encryption systems; threats include improper disclosures of keys, theft of valuable key information, or failure to be able to meet law enforcement demands.

Complexity — Although it may be possible to make key recovery reasonably transparent to the end users of encryption, a fully functional key recovery infrastructure is an extraordinarily complex system, with numerous new entities, keys, operational requirements, and interactions. In many cases, the key recovery aspects of a system are far more complex and difficult to implement than the basic encryption functions themselves.

Economic Cost — No one has yet described, much less demonstrated, a viable economic model to account for the true costs of key recovery. However, it is still possible to make sound qualitative judgments about the basic system elements, shared by all key recovery schemes, that will have the most dramatic impact on

the cost of designing, implementing, deploying, and operating such systems.

3.1 NEW VULNERABILITIES & RISKS

Any key recovery infrastructure, by its very nature, introduces a new and vulnerable path to the unauthorized recovery of data where one did not otherwise exist. This introduces at least two harmful effects:

- It removes the inherent guarantees of security available through non-recoverable systems, which do not have an alternate path to sensitive plaintext that is beyond the users' control.
- It creates new concentrations of decryption information that are high-value targets for criminals or other attackers.

These risks arise with cryptography used in communication and storage, but perhaps even more intensely with cryptography used in authentication. (They are compounded even further if any keys are used for more than one of these purposes.)

3.1.1 New Paths to Plaintext

Regardless of the implementation, if key recovery systems must provide timely law enforcement access to a whole key or to plaintext, they present a new and fast path to the recovery of data that never existed before.

The key recovery access path is completely out of the control of the user. In fact, this path to exceptional access is specifically designed to be concealed from the encryption user, removing one of the fundamental safeguards against the mistaken or fraudulent release of keys.

In contrast, non-recoverable systems can usually be designed securely without any alternative paths. Alternative paths to access are neither required for ordinary operation nor desirable in many applications for many users.

3.1.2 Insider Abuse

Like any other security system with a human element, key recovery systems are particularly vulnerable to compromise by authorized individuals who abuse or misuse their positions. Users of a key recovery system must trust that the individuals designing, implementing, and running the key recovery operation are indeed trustworthy. An individual, or set of individuals, motivated by ideology, greed, or the threat of blackmail, may abuse the authority given to them. Abuse may compromise the secrets of individuals, particular corporations, or even of entire nations. There have been many examples in recent times of individuals in sensitive positions violating the trust placed in them. There is no reason to believe that key recovery systems can be managed with a higher degree of success.

The risk of "insider abuse" becomes even more evident when attempts are made to design key recovery schemes that are international in scope. Such abuse can even become institutionalized within a rogue

company or government. National law-enforcement agencies, for example, might abuse their key recovery authority to the advantage of their own country's corporations.

3.1.3 New Targets for Attack

The nature of key recovery creates new high-value targets for attack of encryption systems. Key recovery agents will maintain databases that hold, in centralized collections, the keys to the information and communications their customers most value. In many key recovery systems, the theft of a single private key (or small set of keys) held by a recovery agent could unlock much or all of the data of a company or individual. Theft of a recovery agent's own private keys might provide access to an even broader array of communications, or might make it possible to easily spoof header information designed to ensure compliance with encryption export controls. The key recovery infrastructure will tend to create extremely valuable targets, more likely to be worth the cost and risk of attack.

The identity of these new rich targets will be highlighted by the key recovery systems themselves. Every encrypted communication or stored file will be required to include information about the location of its key retrieval information. This "pointer" is a road map showing law enforcement how to recover the plaintext, but it may also show unauthorized attackers where to focus their efforts. Moreover, even those systems (such as split key systems) that can decrease these risks, do so with a marked increase in cost. For example, splitting a key in half at least doubles the recovery agent costs.[19] Such systems require

multiple agents, costly additional coordination mechanisms, and faster response times necessary to assemble split keys and still provide fast access to plaintext. Regardless of how many times a key is split, law enforcement's demand for timely access will still require the development of fast systems for the recovery of key parts. Both the systems for key part assembly, and the ultimate whole key assembled for law enforcement, will present new points of vulnerability.

3.1.4 Forward Secrecy

Key recovery is especially problematic in communications systems, such as encrypted cellular telephone calls, because it destroys the property of forward secrecy. A system with forward secrecy is one in which compromising the keys for decrypting one communication does not reduce the security of other communications. For example, in an encrypted telephone call, the keys for encrypting a call can be established as the call is set up. If these keys are destroyed when the call is over, the participants can be assured that no one can later decrypt that conversation — even if the keys to some subsequent conversation are compromised. The result is that once the call is over, the information required to decrypt it ceases to exist; not even the parties to the call store the keys. Typically, keys are created and destroyed on a per-call basis, or even many times per call. This makes it possible to limit the costs and risks of secure processing and storage to the period of the call itself.

Forward secrecy is desirable and important for two reasons. First, it simplifies the design and analysis

of secure systems, making it much easier to ensure that a design or implementation is in fact secure. Secondly, and more importantly, forward secrecy greatly increases the security and decreases the cost of a system, since keys need to be maintained and protected only while communication is actually in progress.

Key recovery destroys the forward secrecy property, since the ability to recover traffic continues to exist long after the original communication has occurred. It requires that the relevant keys be stored instead of destroyed, so that later government requests for the plaintext can succeed. If the keys are stored, they can be compromised; if they are destroyed, the threat of compromise ceases at that moment.

3.2 NEW COMPLEXITIES

Experience has shown that secure cryptographic systems are deceptively hard to design and build properly. The design and implementation of even the simplest encryption algorithms, protocols, and implementations is a complex and delicate process. Very small changes frequently introduce fatal security flaws. Non-key recovery systems have rather simple requirements and yet exploitable flaws are still often discovered in fielded systems.

Our experiences designing, analyzing and implementing encryption systems convince us that adding key recovery makes it much more difficult to assure that such systems work as intended. It is possible, even likely, that lurking in any key recovery system are one or more design, implementation, or operational weaknesses that allow recovery of data by unauthorized parties.

[19] Storage of a smaller key part is not necessarily cheaper than storage of the whole key, and the preferred key-splitting methods generally produce key parts each of which is as large as the whole key.

The commercial and academic world simply does not have the tools to properly analyze or design the complex systems that arise from key recovery.

This is not an abstract concern. Most of the key recovery or key escrow proposals made to date, including those designed by the National Security Agency, have had weaknesses discovered after their initial implementation. For example, since the system's introduction in 1993, several failures have been discovered in the U.S. Escrowed Encryption Standard, the system on which the "Clipper Chip" is based. These problems are not a result of incompetence on the part of the system's designers. Indeed, the U.S. National Security Agency may be the most advanced cryptographic enterprise in the world, and it is entrusted with developing the cryptographic systems that safeguard the government's most important military and state secrets. The reason the Escrowed Encryption Standard had flaws is that good security is an extremely difficult technical problem to start with, and key recovery adds enormous complications with requirements unlike anything previously encountered.

3.2.1 Scale

Key recovery as envisioned by law enforcement will require the deployment of secure infrastructures involving thousands of companies, recovery agents, regulatory bodies, and law enforcement agencies worldwide interacting and cooperating on an unprecedented scale.

Once widely available, encryption will likely be used for the bulk of network communications and storage of sensitive files. By the year 2000 — still early in

the adoption of information technologies — fielding the ubiquitous key recovery system envisioned by law enforcement could encompass:

- **Thousands of products.** There are over 800 encryption products worldwide today, and this number is likely to grow dramatically.
- **Thousands of agents all over the world.** Proposed systems contemplate many key recovery agents within this country alone; other countries will want agents located within their borders. Large companies will want to serve as their own key recovery agents. Each of these agents will need to obtain U.S. certification and possibly certification by other countries as well.
- **Tens of thousands of law enforcement agencies.** There are over 17,000 local, state, and federal law enforcement agencies in the United States alone that might seek key information for authorized wiretaps or seized data. [20] National and local agencies around the world will also want access to keys.
- **Millions of users.** Several million Web users today use encrypted communications whenever their Web browser encounters a secure page (such as many of those used for credit card transactions). There will be an estimated 100 million Internet users by the year 2000, most of whom will be likely to regularly encrypt communications as part of the next version of the standard Internet protocols. Millions of other corporate and home computer users will also regularly encrypt stored information or intra-network communications.

[20] U.S. Department of Justice, Bureau of Justice Statistics, *Sourcebook of Criminal Justice Statistics 1995 (1996)*, p. 39.

- **Tens of millions (or more) of public-private key pairs.** Most users will have several public key pairs for various purposes. Some applications create key pairs “on-the-fly” every time they are used.
- **Hundreds of billions of recoverable session keys.** Every encrypted telephone call, every stored encrypted file, every e-mail message, and every secure web session will create a session key to be accessed. (Various key recovery scheme may avoid the need for the recovery center to process these session keys individually, but such “granularity shifts” introduce additional risk factors — see Section 3.4.1 below.)

Ultimately, these numbers will grow further as improved information age technologies push more people and more data online.

The overall infrastructure needed to deploy and manage this system will be vast. Government agencies will need to certify products. Other agencies, both within the U.S. and in other countries, will need to oversee the operation and security of the highly-sensitive recovery agents — as well as ensure that law enforcement agencies get the timely and confidential access they desire. Any breakdown in security among these complex interactions will result in compromised keys and a greater potential for abuse or incorrect disclosures.

There are reasons to believe secure key recovery systems are not readily scalable. Order-of-magnitude increases in the numbers of requesting law enforcement agencies, product developers, regulatory oversight

agencies, and encryption end users all make the tasks of various actors in the key recovery system not only bigger, but much more complex. In addition, there are significant added transaction costs involved with coordination of international key recovery regimes involving many entities.

The fields of cryptography, operating systems, networking, and system administration have no substantive experience in deploying and operating secure systems of this scope and complexity. We simply do not know how to build a collective secure key-management infrastructure of this magnitude, let alone operate one, whether the key-recovery infrastructure is centralized or widely distributed.

3.2.2 Operational Complexity

The scale on which a government-access key recovery infrastructure must operate exacerbates many of the security problems with key recovery. The stated requirements of law enforcement demand the construction of highly complex key recovery systems. Demands on the speed and process for recovering keys will greatly increase the complexity of tasks facing those trusted with key recovery information. Demands for ubiquitous worldwide adoption of key recovery will greatly increase the complexity and number of entities involved. Each of these will in turn have a significant impact on both the security and cost of the key recovery system.

Consider the tasks that a typical key recovery center will perform to meet one law enforcement request for a session key for one communication or stored file:

- Reliably identify and authenticate requesting law enforcement agents (there are over 17,000 U.S. domestic law enforcement organizations).
- Reliably authenticate court order or other documentation.
- Reliably authenticate target user and data. Check authorized validity time period.
- Recover session key, plaintext data, or other decryption information.
- Put recovered data in required format.
- Securely transfer recovered data, but only to authorized parties.
- Reliably maintain an audit trail.

Each of these tasks must be performed securely in a very short period of time in order to meet government requirements. For example, the most recent U.S. Commerce Department regulations governing recovery agents require two hour turnaround of government requests, around the clock. The tasks must be performed by agents all over the world serving millions of clients and responding to requests from both those clients and numerous law enforcement agencies.

There are few, if any, secure systems that operate effectively and economically on such a scale and under such tightly-constrained conditions — even if these requirements are relaxed considerably (e.g.,

one day response time instead of two hours). The urgent rush imposed by very short retrieval times, and the complexity of the tasks involved, are an anathema to the careful scrutiny that should be included in such a system. If there is uncertainty at any step of the access process, there may be insufficient time to verify the authenticity or accuracy of a retrieval request.

It is inevitable that a global key recovery infrastructure will be more vulnerable to fraudulent key requests, will make mistakes in giving out the wrong key, and will otherwise compromise security from time to time. While proper staffing, technical controls, and sound design can mitigate these risks to some extent (and at considerable cost), the operational vulnerabilities associated with key recovery cannot be eliminated entirely.

3.2.3 Authorization for Key Recovery

One of the requirements for a key recovery operation is that it must authenticate the individual requesting an archived key. Doing so reliably is very difficult.

“Human” forms of identification — passports, birth certificates, and the like — are often easily counterfeited. Indeed, news reports describe “identity theft” as a serious and growing problem. Electronic identification must be cryptographic, in which case a key recovery system could be used to attack itself. That is, someone who steals — or recovers — a signature key for a law enforcement officer or a corporate officer could use this key to forge legitimate requests for many other keys. For that matter, if a sensitive confidentiality key were stolen or obtained from the repository, it might be possible to use it to eavesdrop on other key recovery conversations.

In contrast, a business's local, day-to-day key recovery process could rely on personal identification. A system administrator or supervisor would know who had rights to which keys. Even more questionable requests, such as those over the phone, could be handled appropriately; the supervisor could weigh such factors as the sensitivity of the information requested, the urgency of the request as known a priori, and even the use of informal authentication techniques, such as references to shared experiences. But none of these methods scale well to serve requests from outside the local environment, leaving them unsuitable for use by larger operations or when requests come from persons or organizations not personally known to the keyholders.

3.3 NEW COSTS

Key recovery, especially on the scale required for government access, will be very expensive. New costs are introduced across a wide range of entities and throughout the lifetime of every system that uses recoverable keys.

The requirements set out by law enforcement impose new system costs for designing, deploying, and operating the ubiquitous key recovery system.

These costs include:

- **Operational costs for key recovery agents** — the cost of maintaining and controlling sensitive, valuable key information securely over long periods of time; of responding to both law enforcement requests and legitimate commercial requests for data; and of communicating with users and vendors.

- **Product design and engineering costs** — new expenses entailed in the design of secure products that conform to the stringent key recovery requirements.
- **Government oversight costs** — substantial new budgetary requirements for government, law enforcement, or private certification bodies, to test and approve key recovery products, certify and audit approved recovery agents, and support law enforcement requests for and use of recovered key information.
- **User costs** — including both the expense of choosing, using, and managing key recovery systems and the losses from lessened security and mistaken or fraudulent disclosures of sensitive data.

3.3.1 Operational Costs

The most immediately evident problem with key recovery may be the expense of securely operating the infrastructure required to support it. In general, cryptography is an intrinsically inexpensive technology; there is little need for externally-operated "infrastructure" (outside of key certification in some applications) to establish communication or store data securely. Key recovery, on the other hand, requires a complex and poorly understood — and hence expensive and insecure — infrastructure.

The operational complexity described in the previous section introduces substantial ongoing costs at each key recovery center. These costs are likely to be very high, especially compared with the ordinary operational expenses that might be expected in commercial key recovery systems. Government key recovery requires,

for example, intensive staffing (7x24 hours), highly trained and highly trusted personnel, and high-assurance hardware and software systems in order to meet the government's requirements in a secure manner. These costs are borne by all encryption applications, even those where key recovery is not beneficial to the user or even to law enforcement.

It remains unclear whether the high-risk, high-liability business of operating a key recovery center, with limited consumer demand to date, will even be economically viable.

3.3.2 Product Design Costs

Key recovery also increases the difficulty and expense of designing user-level encryption software and hardware. These costs vary depending on the particular application and the precise nature of the recovery system, but could be substantial in some cases. Integrating key recovery, especially in a secure manner, can also substantially delay the release of software. Given the highly competitive nature and short product life-cycles of today's hardware and software markets, such delays could discourage vendors from incorporating it at all, or worse, encourage sloppy, poorly-validated designs. Compatibility with older products presents special challenges and further increases these costs.

3.3.3 End-User Costs

Without government-driven key recovery, encryption systems can easily be fielded in a way that is largely transparent to their users. Highly secure communication and storage need require nothing further than the purchase of a reputable commercial product with

strong encryption features tested in the marketplace. The use of that encryption need require nothing more than the setting of an option, the click of an icon, or the insertion of a hardware card. We are fully confident that, in an unregulated marketplace, many applications will ship with such high-quality user-transparent encryption built in. This is already happening at negligible cost to the user.

In contrast, the use of a secure key recovery system requires at least some additional user effort, diligence, or expense. In addition to the purchase of an encryption product, one or more key recovery agent(s) must be chosen. The user must enter into an important (although possibly implicit) contractual relationship with that agent, a relationship that will govern the potential disclosure of the most sensitive key information — now and for years to come. In many cases, there will need to be some communication of key information between user and the recovery agent. (Although some products will come with a built-in key, prudent users may want to change their keys on a regular basis. Also, software, especially mass-market “shrink-wrapped” software, cannot usually be economically distributed with unique keys installed in each individual copy).

The burdens on key recovery users continue long after data have been encrypted. Key recovery agents will maintain the ability to decrypt information for years. During that time, an agent might relax its security policies, go bankrupt, or even be bought out by a competitor — but will retain, and in fact must retain, the ability to decrypt. Diligent and concerned encryption users will need to be aware of the fate of their key recovery agents for years after their initial encryption use.

These burdens will apply to all users of encryption. Each use of encryption may entail the entry into a contractual relationship with a third-party key recovery agent. Under any rational business model, each such instance will entail some additional cost.

3.4 TRADEOFFS

Some aspects of key recovery can be easily shifted along a spectrum from higher cost to higher risk. While it may be possible to field a particular key escrow system in a relatively secure way, this often results in tremendous costs to the user. While relatively simple and inexpensive key escrow systems exist, they often jeopardize security. For example, a poorly-run key recovery agent, employing less-skilled low-paid personnel, with a low level of physical security, and without liability insurance could be expected to be less expensive to operate than a well-run center.

Interestingly, security and cost can also be traded off with respect to the design itself. That is, the simplest designs, those that are easiest to understand and easiest to verify, also tend to require the most stringent assumptions about their environment and operation or have the worst failure characteristics. For example, imagine a design in which session keys are sent to the recovery center by encrypting them with the center's globally-known public key. Such a system might be relatively simple to design and implement, and one might even be able to prove that it is secure when operated correctly and under certain assumptions. However, this is among the worst possible designs from a robustness point of view: it has a single point of failure (the key of the recovery agent) with which all keys are encrypted. If this key is compromised (or a corrupt version distributed), all the recoverable keys in the system could be compromised. (We note that several commercial systems are based on almost exactly this design.)

3.4.1 Key Recovery Granularity and Scope

One of the most important factors influencing the cost and security of key recovery is the granularity and scope of the keys managed by the key recovery system. In particular, it is important to understand two issues:

- Granularity: the kinds of keys (user, device, session, etc.) that are recoverable
- Scope: the consequences of compromising a recovery agent's key.

Granularity is important because it defines how narrowly-specified the data to be recovered from an agent can be and how often interactions (by the user and by law enforcement) with the recovery agent must take place. Various systems have been proposed in which the recovery agent produces "master" keys that can decrypt all traffic to or from individual users or hardware devices. In other systems, only the keys for particular sessions are recovered. Coarse granularity (e.g., the master key of the targeted user) allows only limited control over what can be recovered (e.g., all data from a particular individual) but requires few interactions between law enforcement and the recovery center. Finer granularity (e.g., individual session keys), on the other hand, allows greater control (e.g., the key for a particular file or session, or only sessions that occurred within a particular time frame), but requires more frequent interaction with the recovery center (and increased design complexity).

Also important is the scope of the recovery agent's own secret. Most key recovery systems require the user software or hardware to send keys to the recovery agent by encrypting them with the recovery agent's public key. If a recovery agent has only a single such key, that key becomes an extraordinarily valuable, global, single point of failure. Worse, because the

recovery agent must use the secret component of this key in order to decrypt the keys sent to it (or at least any time a key is recovered), its exposure to compromise or misuse is also increased. To address this vulnerability, a recovery agent may have many

such keys, perhaps one or more for each user. However, negotiating and distributing these keys to the users introduces still other complexities and vulnerabilities.

Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current

competency of the field, and may well introduce ultimately unacceptable risks and costs.

Attempts to force the widespread adoption of key recovery through export controls, import or domestic use regulations, or international standards should be considered in light of these factors. We urge public debate to carefully weigh the costs and benefits of government-access key recovery before these systems are deployed.

Harold (Hal) Abelson is a Professor in the EECS Department at MIT and a Fellow of the IEEE. He is co-author of the textbook *Structure and Interpretation of Computer Programs* and the 1995 winner of the IEEE Computer Society's Education Award. Abelson consults at Hewlett-Packard Corporation, in the Internet Technology Group.

Ross Anderson teaches and directs research in computer security, cryptology and software engineering at Cambridge University in England. He is an expert on engineering secure systems, how they fail, and how they can be made more robust. He has done extensive work on commercial cryptographic systems, and recently discovered flaws in a British government key escrow protocol.

Steven M. Bellovin is a researcher on cryptography, networks and security at AT&T Laboratories. He is co-author of the book *Firewalls and Internet Security: Repelling the Wily Hacker*. In 1995 he was a co-recipient of the Usenix Lifetime Achievement Award for his part in creating Netnews. He is a member of the Internet Architecture Board.

Josh Benaloh is a Cryptographer at Microsoft Research and has been an active researcher in cryptography for over a decade with substantial contributions in the areas of secret-ballot elections and secret sharing methods and applications. Before joining Microsoft, he was a Postdoctoral Fellow at the University of Toronto and an Assistant Professor at Clarkson University.

Matt Blaze is a research scientist at AT&T Laboratories in Florham Park, NJ. In 1994 his research led to the discovery of weaknesses in the U.S. government's "Clipper" key escrow system. An active member of the cryptology research community, he is responsible for a number of cryptographic concepts and systems, including trust management, remotely-keyed encryption, proxy cryptography and IP-layer and file-system layer security protocols.

Whitfield Diffie is a Distinguished Engineer at Sun Microsystems specializing in security, and co-author of *Privacy on the Line* (MIT Press) in 1998 with Susan Landau. In 1976 Diffie and Martin Hellman created public key cryptography, which solved the problem of sending coded information between individuals with no prior relationship and is the basis for widespread encryption in the digital information age.

John Gilmore is an entrepreneur and civil libertarian. He was an early employee of Sun Microsystems, and co-founded Cygnus Solutions, the Electronic Frontier Foundation, the Cypherpunks, and the Internet's "alt" newsgroups. He has twenty years of experience in the computer industry, including programming, hardware and software design, and management.

Peter G. Neumann is a Principal Scientist in the Computer Science Lab at SRI. He is Moderator of the Risks Forum (comp.risks), author of *Computer-Related Risks* (Addison-Wesley), and co-author of the National Research Council study report, *Cryptography's Role in Securing the Information Society* (National Academy Press). He is a Fellow of the AAAS, ACM and IEEE.

Ronald L. Rivest is the Webster Professor of Electrical Engineering and Computer Science in MIT's EECS Department. He is also an Associate Director of MIT's Laboratory for Computer Science. He is perhaps best known as a co-inventor of the RSA public-key cryptosystem and a founder of RSA Data Security, Inc.

Jeffrey I. Schiller is the Network Manager at MIT and has managed the MIT campus computer network since its inception in 1984. Schiller is the author of the Kerberos Authentication System, serves as the Internet Engineering Steering Group's Area Director for Security, and is responsible for overseeing security-related Working Groups of the Internet Engineering Task Force (IETF).

Bruce Schneier is president of Counterpane Systems, a Minneapolis-based consulting firm specializing in cryptography and computer security. He is the author of *Applied Cryptography* and inventor of the Blowfish and Twofish encryption algorithms.

||
**CENTER FOR
DEMOCRACY**
TECHNOLOGY

1634 Eye Street, NW Suite 1100
Washington, DC 20006
telephone 202.637.9800
facsimile 202.637.0968
info@cdt.org www.cdt.org

Mr. GOODLATTE. Mr. Gillespie, welcome.

**STATEMENT OF ED GILLESPIE, EXECUTIVE DIRECTOR,
AMERICANS FOR COMPUTER PRIVACY**

Mr. GILLESPIE. Thank you, Mr. Chairman. I appreciate the opportunity to appear before you today.

I want to add my voice to the others on the panel who express their appreciation for your leadership and the leadership of Congresswoman Lofgren and the leadership of this subcommittee on the issue of encryption.

I serve as Executive Director of Americans for Computer Privacy, a broad-based coalition of over 40 trade associations, over 100 companies and over 3,000 individuals. It is worth noting that this coalition is not comprised only of industry sources, but financial services, manufacturing, retail and transportation industries, as well as law enforcement, civil liberty, taxpayer and privacy groups. We strongly endorse enactment of the SAFE Act, and we very much appreciate your leadership.

Strong encryption is key to the continued vitality and growth of the new economy and will play an increasingly important role in how we govern, communicate, conduct commerce and protect our national infrastructure. Accordingly, the United States needs a clear and realistic national policy to ensure that industry is able to develop the products that will help us to meet our national objectives.

Significant progress was made last year with the Administration's September policy pronouncement implementing the regulations of December 31. However, the Administration has yet to allow U.S. encryption manufacturers to compete on a level playing field in the global marketplace. The Administration policy remains highly problematic and does not represent the clear and realistic national policy that this issue requires.

One example is that the Administration's encryption export regulations impose greater restrictions on American companies than those called for under the Wassenaar arrangement discussed this morning. The Administration should at least eliminate all controls on encryption software and hardware for products up to 64 bits and make U.S. controls consistent with the revised Wassenaar arrangement.

As a rule, however, the Administration's efforts to develop a global approach to this issue through Wassenaar are doomed to failure. Wassenaar has only 33 members, and does not include encryption producing companies like China, India, South Africa or Israel. Further, the Wassenaar Arrangement is only as effective as the implementing regulations adopted by the member countries. Some of the member nations will promulgate regulations less restrictive than those of the U.S., resulting in a competitive advantage over domestic encryption manufacturers. In short, the Wassenaar arrangement is a toothless tiger.

ACP also believes that our current export policy shortchanges our long-term national interest by jeopardizing our current global leadership in this vital technology. Strong, high-quality encryption products are now widely available, as we have seen on this panel,

from foreign makers rendering our export policy an exercise in futility.

We worry that America will lose this critical market to foreign makers. When and if it does, it will be too late to change U.S. policy and too late to preserve U.S. leadership in this vital arena. In the long run, U.S. national security objectives are best served by an information technology world in which U.S. companies are market leaders in all aspects, especially encryption.

ACP's industry members have ample evidence of the rapidly growing market share of foreign encryption and examples of U.S. businesses losing out to foreign manufacturers because of these restrictions on our exports. We do not pretend to have all of the answers to questions about national security, but our knowledge of the technology in global markets leads us to believe that our long-term national security objectives can only be achieved if the United States realistically acknowledges the inevitability of a world of ubiquitous, strong encryption.

We are joined in this view by the Center for Strategic International Studies. CSIS recently conducted a study of our Nation's technical vulnerabilities. The study was chaired by former FBI and CIA Director William Webster. The subsequent report entitled *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*, calls for, "the intelligence gathering communities—law enforcement and foreign intelligence—to examine the implications of the emerging environment and alter their traditional sources and means to address those strategic warfare needs of the 21st century. Continued reliance on limited availability of strong encryption without the development of alternative sources and means will seriously harm law enforcement and national security."

ACP has advocated that the U.S. Government should work cooperatively with our Nation's hardware and software manufacturers to develop the technical tools and know-how to achieve a policy that effectively responds to society's needs for law enforcement, national security, critical infrastructure protection, privacy preservation and economic well-being.

U.S. technology companies will happily do their part to help the Government prepare for an uncertain 21st century, but Congress should pass the SAFE Act and establish a clear and realistic national policy on encryption. That is the best way to preserve U.S. leadership in encryption technology upon which the successful protection of our critical infrastructure and achievement of our national security objectives certainly and inevitably depend.

Thank you again for your time here this morning.

Mr. GOODLATTE. Thank you, Mr. Gillespie.

[The prepared statement of Mr. Gillespie follows:]

PREPARED STATEMENT OF ED GILLESPIE, EXECUTIVE DIRECTOR, AMERICANS FOR
COMPUTER PRIVACY

Mr. Chairman and members of the Subcommittee,
Thank you for the opportunity to testify before you on H.R. 850, the SAFE Act, sponsored by Representatives Goodlatte and Lofgren and over 200 members of the House. I serve as Executive Director of Americans for Computer Privacy (ACP), a broad coalition of 40 trade associations, over 100 companies and over 3,000 individuals. The coalition includes the financial services, manufacturing, high-tech, and transportation industries as well as law enforcement, civil-liberty, taxpayer and privacy groups. ACP supports policies that allow American citizens continued use of

strong encryption without government intrusion, and advocates lifting export restrictions on U.S. made encryption products.

ACP strongly endorses enactment of the SAFE Act, and we appreciate the leadership provided by Representatives Goodlatte and Lofgren very much. We urge your subcommittee to report it promptly for full committee consideration.

As Vice President Gore said in September 1998 when he announced the current administration policy, developing a national encryption policy is one of the most difficult issues facing the country. It requires balancing many competing objectives—all of which are of great importance to the nation.

As ACP noted in our policy paper of May 8, 1998, strong encryption is essential to:

- Protecting the nation's infrastructure and assuring the integrity of information;
- Ensuring the privacy of electronic communications of American citizens and organizations;
- Protecting our national security interests;
- Safeguarding the public; and
- Maintaining U.S. leadership in the development of information technology industry.

As we move into the new millenium, information technology will play an increasingly important role in the way we govern, communicate, conduct commerce, and operate and protect our national infrastructure. Strong encryption is key to the continued vitality and growth of all of these activities. Accordingly, the United States needs a *clear and realistic* national policy to assure that industry is able to develop the products that will help us to meet our national objectives.

Significant progress was made last year with the Administration's policy announced by the Vice President in September and contained in the interim final regulations of December 31, 1998. ACP commends the government for the hard work and thoughtful consideration that went into the development of that policy and those regulations. Last year, ACP had several productive meetings with the Administration's inter-agency task force, including representatives from law enforcement and the Justice Department. Those meetings were conducted in good-faith on both sides and led to a greater understanding on both sides of the needs and concerns of the other. The Clinton Administration incorporated many of our interim recommendations into its updated export policy, including: export relief for encryption products that use symmetric algorithms up to and including 56-bits; products that use asymmetric algorithms up to and including 1024-bits; and relief for various sectors of the business community.

The Clinton Administration, however, has yet to allow U.S. encryption manufacturers to compete on a level playing field in the global marketplace. The Administration policy remains highly problematic and does not represent the clear and realistic national policy that this issue requires.

First, the Administration has entered into an agreement with 32 other countries—the Wassenaar Arrangement—containing certain export controls on encryption. Unfortunately, the Administration's encryption export regulations impose greater restrictions on American companies than those called for under the arrangement. As a first step, we believe the Administration should at least eliminate all controls on encryption software and hardware for products up to 64-bits, and should eliminate all reporting requirements on higher-level encryption exports. Such actions would make U.S. controls consistent with the revised Wassenaar Arrangement.

We also believe that the Administration's efforts to develop a global approach to this issue through the Wassenaar Arrangement are doomed to failure. We recognize that this is a global problem and if it were truly possible to achieve universal agreement that was fairly enforced, industry would no doubt be supportive. But Wassenaar only has 33 members and does not include encryption-producing countries such as China, India, South Africa, or Israel. Further, the Administration should recognize that the Wassenaar Arrangement is only as effective as the implementing regulations adopted by the member countries. Some of the member nations will promulgate regulations that are less restrictive than those of the United States, thereby providing those nations with a competitive advantage over domestic encryption manufacturers. In short, the Wassenaar Arrangement is a toothless tiger.

Second, the Interim Rule falls short on a number of short-term points. For example, the Interim Rule does not fulfill the mandate promised by Vice President Gore on September 16 to allow all 56-bit encryption products to be eligible for export to all end-users (except terrorist states). In reality, the Interim Rule does not allow the

export of 56-bit encryption chips, integrated circuits, toolkits, and executable or linkable modules for export under license exception except to U.S. subsidiaries.

Further, the Interim Rule is so complex that a number of the benefits in the new policy are undermined by provisions of the Interim Rule. For example, the reporting requirements are so onerous to companies that reporting costs may exceed the price of some products, much less the profit. In the same vein, the Government has shown little understanding of mass-market distribution techniques. It makes no sense that the Government does not expect manufacturers to be able to control mass-market encryption products using 56-bit encryption, but does expect manufacturers to be able to control mass-market encryption products using algorithms higher than 56-bits. Furthermore, it is simply impractical to expect manufacturers to collect reporting data on mass-market encryption products. My personal experience is that I never return registration cards on coffee makers, answering machines, or software products—I expect most people in this room have similar experiences.

And so the Administration's new policy, as grateful as we are for this limited progress, remains flawed even on its own terms.

Beyond this, in the encryption debate in the larger sense, we continue to have good-faith disagreements with the Administration about its current policy, which only Congress and this legislation can address.

Primarily, ACP believes that our current export policy short-changes our long-term national interest in that it puts at jeopardy our current global leadership in this vital technology. Strong, high-quality encryption products are now widely available from foreign makers. That renders our export policy an exercise in futility. We worry that America will lose this critical market to foreign makers. When and if it does, it will be too late to change U.S. policy and too late to preserve U.S. leadership in this vital arena.

If we do lose that U.S. leadership position, what will that mean? It will mean that the national security agencies will be confronting ubiquitous encryption made not by U.S. companies, but by foreign companies. Where then will the national security agencies go for technical help on encryption, if the most sophisticated encryption experts and product-makers reside abroad? It could put us in the untenable position of protecting our critical national infrastructure with foreign-made encryption.

We must retain leadership in this vital technology if we are to meet our long-term national security objectives. That is why we must assess our encryption export policies from a long-term, not a short-term, perspective.

In the long run, there can be no doubt that U.S. national security objectives are best served by an IT world in which U.S. companies are market leaders in all aspects, especially encryption. ACP's industrial members have ample evidence of the rapidly growing market share of foreign encryption and examples of U.S. businesses losing out to foreign manufacturers because of the U.S. export regulations. For example, a December 1997 study conducted by Trusted Information System found that 656 non-American encryption products are available from 29 foreign countries. These encryption manufacturers are located as far from the U.S. as China and as close as Mexico. The products in the study were purchased via routine channels, either directly from the foreign manufacturer or from a distributor.

RSA Data Security has lost business opportunities with major foreign conglomerates such as Lloyds TSB PLC, SAP AG, and Siemens Ag because of U.S. export control regulations. U.S. software companies estimate they have lost millions of potential users of their software due to the encryption regulations. It is naïve to believe these foreign customers and entities are forgoing strong encryption to protect their proprietary information because it is not available from U.S. manufacturers, rather than purchasing strong, non-American encryption.

Further, foreign encryption manufacturers are marketing their products by using U.S. encryption regulations against American companies. For example, Baltimore Technologies, an Irish encryption manufacturer that President Clinton visited during his trip to Europe last year, specifically points out the shortcomings of U.S. encryption products in their marketing of their product, WebSecure. Their opening paragraph of their website states that the export versions of U.S. browsers "are limited to 40 bits of encryption, which is not secure enough for most applications." In contrast, WebSecure provides 128-bit encryption for "real security."¹

Strong encryption is also available for sale and for free on the Internet to anybody in the world with a computer. Here is just one example of the ease with which a person outside the United States can obtain strong encryption with a few clicks on their computer. One, they can visit the international Pretty Good Privacy site: www.pgpi.com. From that URL, anybody in the world can download strong, 128-bit

¹ Located at the following URL:
www.baltimore.com/products/secure_web/mn_secure_web.html

encryption within 47 seconds. And because any citizen in the U.S. can download encryption legally from the Internet, and anyone in the world has access to those same web sites, the Internet makes controlling encryption exports a very difficult proposition.

ACP also believes it is vital to our national interests that our critical infrastructure is secure and we praise President Clinton for recognizing this vulnerability in his speech earlier this year. We wish, however, that the President recognized the importance of the role of strong encryption produced by U.S. high technology companies.

We do not believe we have all the answers to questions about national security, but ACP strongly believes based on our knowledge of the technology and global markets that our long term national security objectives can only be achieved if the United States realistically acknowledges the inevitability of a world of ubiquitous, strong encryption. Trying to control the proliferation of encryption is like trying to control the proliferation of mathematics. For that is what we are talking about here. Encryption algorithms are nothing but sophisticated mathematics. And while the United States may realistically hope to remain the leader in such a field, it cannot realistically expect to monopolize it.

We are joined in this view by the Center for Strategic and International Studies ("CSIS"). CSIS recently conducted a study of our nation's technical vulnerabilities; the study was chaired by William Webster, the former director of the FBI and Central Intelligence and former U.S. Circuit Judge. The subsequent report, entitled *Cybercrime . . . Cyberterrorism . . . Cyberwarfare . . . Averting an Electronic Waterloo*, calls for the "intelligence gathering communities—law enforcement and foreign intelligence—to examine the implications of the emerging environment and alter their traditional sources and means to address the SIW needs of the twenty-first century. *Continued reliance on limited availability of strong encryption without the development of alternative sources and means will seriously harm law enforcement and national security.*"

For instance, ACP proposed last year the creation of a "NET Center" (and, since then, "Tech Center" has been created) to help law enforcement officials understand how to deal with encryption and other technological advances when encountered in a criminal setting. We have been cooperating on these projects, and we are pleased with the development of this forward-thinking strategy.

On the national security side, Senator Bob Kerrey recently suggested that (1) the President should convene a public-private panel to examine the implications of this new technological age for our national security, and (2) the creation of a new national laboratory for information technology to perform research and to act as a forum for further discussions on technological breakthroughs. These views may deserve further exploration, and ACP wants to play a leading role in crafting industry cooperation.

ACP wishes to emphasize that it recognizes a legitimate governmental need to obtain access to the plain text of communications when authorized by proper legal authority. ACP and its members are responsible citizens of the nation and the globe and have no wish to facilitate the commission of crime, the spread of terrorism or the acquisition and delivery of weapons of mass destruction. Similarly, we are committed to strengthening the nation's infrastructure, enhancing the privacy of American citizens and ensuring the security of electronic commerce. We believe that these sometimes competing objectives can be met, but only if government does not seek to force solutions on the industry that are not compatible with the development of technology and market demands.

ACP has advocated that the U.S. Government should work cooperatively with our nation's hardware and software manufacturers to develop the technical tools and know-how to achieve a policy that effectively responds to society's needs for law enforcement, national security, critical infrastructure protection, privacy preservation, and economic well-being.

In closing, Secretary of Defense William Cohen gave a speech at Microsoft two weeks ago in which he stated: "To maintain peace and stability in this uncertain world, we have mapped out a strategy defined by three words: Shape, Respond, Prepare." ACP and its member companies are willing to do our part in helping the Government prepare for an uncertain 21st century, and we look forward to working with the Government on these projects. But Congress needs to pass the SAFE Act and establish a clear and realistic national policy on encryption. That is the best way to preserve U.S. leadership in encryption technology, upon which the successful protection of our critical infrastructure and achievement of our national security objectives certainly and inevitably depend.

Mr. GOODLATTE. And a special welcome to our former colleague, Congressman McCurdy.

Mr. MCCURDY. Thank you, Mr. Chairman. I have a written statement that I would like to submit for the record, but for the sake of time, I will just make a couple of quick comments, if I could. It is a pleasure being on this side of the table, by the way, and especially appearing before such a distinguished group of former colleagues and friends.

Mr. Goodlatte, I want to commend you and Congresswoman Lofgren for your leadership on this bill. EIA is very pleased and excited to be part of the coalition that supports the SAFE Act. We represent over 2,100 manufacturers in the electronics sector, but rather than give a commercial—that is not our purpose—I want to explain my personal view that I think it has taken a lot of courage on your part to step forward and provide leadership when those on the other side often claim national security or law enforcement interests, but do so oftentimes under the cloak of confidentiality or classification.

As you know, I served in this body for 14 years, and at one point was chairman of the House Intelligence Committee, so I am very familiar with the arguments that are raised. It is clear that during the Cold War, when Howard Berman and I first came to this body, there were very legitimate national security interests involved, and there was a real need for some of the technology that our agencies needed to employ. But what you have done, I think very articulately, is demonstrate that this is no longer the Cold War era.

We had a policy during the Cold War of containment. In the Information Age, it appears that the Administration is trying to develop a policy of restraint or slowing or just trying to stop the spread of technology, as opposed to really having a policy that is effective to accomplish their desired ends. In the Information Age, in the digital economy, I believe it is time for a realistic policy and I think you are trying to advance that.

It was stated today, and I think very clearly, that the Administration can act without congressional action. There may be need for a legislative solution, but in fact the Administration, I believe, should consider moving toward a much more current and updated encryption policy.

We will soon be proposing to the Administration four basic points which we think they should consider in addition to the SAFE Act. In brief, first, the Government needs to significantly ease the restrictions on low-level and mass market encryption software. The chairman has talked about hardware being included, and we appreciate the inclusion of both the telecommunications wireless provisions that he has included, as well as the consumer electronics concerns.

Secondly, law enforcement and national security agencies should better define their access requirements—that is an important point—thereby allowing the industry to develop a variety of marketable solutions. Ms. Lofgren asked Mr. Lee for some specifics on that, and we would like to work with them as they develop that list.

Third, a new policy needs to differentiate between the increasing new uses for the technology such as voice communications, data

transmission and consumer electronics, with appropriate controls on those applications which clearly present problems for Government and decontrolling the rest.

Finally, U.S. policymakers need to recognize the futility of unilateral export restrictions which serve only to damage our domestic industries while doing little to protect our national security. The bottom line is that we in the high tech industry believe that this is a controversy which has dragged on for too long and that a reasonable solution is possible if all sides are willing to work together.

Our industry is willing to accept restrictions on the exports if the controls are reasonable, if they are effective in addressing the problem that they are meant to solve, and if they do not impose unnecessary, overly burdensome requirements. We believe that by implementing these basic proposals, the Administration's legitimate concerns can be addressed; the U.S. high tech industry will be allowed to compete globally, and users will have the security that they need.

I would be happy to take your questions.

Mr. GOODLATTE. Thank you, Congressman McCurdy.

[The information referred to follows.]

PREPARED STATEMENT OF DAVE MCCURDY, PRESIDENT, ELECTRONIC INDUSTRIES ALLIANCE

Thank you, Mr. Chairman for the opportunity to testify today on U.S. encryption policy for the Information Age. With over 2000 member companies, EIA is the premier alliance of trade associations for the high-technology industry. Our mission is to promote an economic and political environment, in this country and around the world, in which our industry can thrive.

I am also a former member of Congress from Oklahoma. During my 14 year tenure in this body, I served as Chairman of the House Intelligence Committee, as well as subcommittee chairman on the Armed Services Committee and the Science Committee. I continue to serve as a member of the Weapons of Mass Destruction Commission, a group of experts investigating how this country can combat proliferation. So I am well aware of how dual-use civilian technologies like encryption can be used for illicit purposes, and the important role of export controls to our national security. But I also recognize the severely limited effectiveness of export controls, as well as the vital importance of a strong and innovative high-technology sector to keep our armed forces a step ahead of any adversary.

Mr. Chairman, it is now clear that 1998 was the year the Internet became mainstream, with more than 100 million people worldwide using the network, up from only three million just four years earlier. Furthermore, shoppers are likely to spend upwards of \$10 billion online this year, and the figure could quadruple by 2002. But as the Net proves itself to be a powerful means for commerce, with potentially hundreds of billions of dollars moving across the network, it also becomes a tempting target for criminals seeking to steal consumers' credit card data or eavesdrop on their online communications. Similarly, as large and small companies turn to the Net to exchange information with their various divisions, or communicate with their suppliers and customers around the world, those electronic transmissions become targets for hackers or business rivals. Other examples of electronic information needing protection are the intellectual property on DVD's or posted on websites; voice conversations moving across wireless networks; or product designs, employee records, and other sensitive data stored on companies' internal computers.

In each of these cases, individuals and companies need encryption to protect themselves. Additionally, with the exponential advances in computing power available to ordinary people and criminals alike, ever stronger encryption is needed to defend against illegal attempts to unscramble sensitive electronic information. Yet, the Administration continues to impose regulations which threaten the security and privacy of millions of Internet users.

The net effect of this policy is to damage the global competitiveness of the U.S. high-tech industry, as well as to jeopardize the security of individuals and companies which operate internationally. Meanwhile, if the so-called "bad actors" want to use encryption, they have the choice of buying it off the shelf of any software store

in America, or downloading it from the Internet, or buying it from a producer overseas no questions asked. Because of these overly strict and burdensome, yet futile export controls, one of this country's most dynamic and competitive industries is ceding marketshare to foreign competitors. Even the Commerce Department, which administers the encryption rules, has acknowledged that there are over 600 encryption products being produced in 29 countries outside the United States, and they are competitive with anything the U.S. produces. It would be tragic if these export rules forced U.S. high-tech companies, and the high-paying jobs associated with them, to move offshore. Such a development would also have the ironic effect of compelling our law enforcement and national security officers to confront encryption made by more non-U.S. companies, with which they have no cooperative relationships.

Mr. Chairman, I have the privilege of representing the most dynamic and competitive industry in the U.S. economy today—actually, I should say, in the world economy today. The companies we represent operate globally, they think and plan in global terms, and they face intense international competition. The fact is, the days when U.S. companies dominated the high-technology industry are over. Similarly, the days when the domestic U.S. market could sustain the industry are also over. It has become almost cliché, but the global economy is a fact of doing business for us, and is a critically important concept to keep in mind as we formulate public policy in this area.

As any successful CEO will tell you, competing—indeed, surviving—in the global economy means exporting. The phenomenal success of the U.S. technology industry comes from its entrepreneurialism, its aggressiveness, its willingness to compete—all those free market forces that drive innovation. In this kind of business environment, tapping new markets before the competition does is the key to success. In 1997, more than one-third of what the U.S. electronics industry produced was exported overseas, over \$150 billion in goods. That means more than a third of the 1.8 million employees who work for U.S. electronics companies depend on exports for their jobs, and the percentage goes up every year.

We must also recognize that our high-tech companies are the engine for technological innovation and economic growth in the world today. The U.S. economy is the most competitive in the world due in no small part to the amazing advancements our companies have achieved. Technologies which, not long ago, had only military or limited civilian applications are now pervasive in our society, and the greater economic efficiency stemming from this diffusion of technology has been the driving force for the remarkable prosperity so many Americans are experiencing.

The impact of export controls on how this industry competes in the global economy can hardly be overstated. They hold us back from competing. Unilateral export controls essentially force us to cede the playing field to our overseas competitors, or at least burden us to the point that we cannot compete effectively. The case of export controls on encryption is perhaps the best example. No amount of Government subsidies could do more to develop the European encryption industry than U.S. export controls have.

We assert that a more balanced policy is needed—one which recognizes the interests of Government, the high-tech industry, and corporate and individual users. While we in the business community recognize the importance of keeping potentially dangerous technologies out of the wrong hands, the Government must similarly recognize the importance of a dynamic and innovative high-tech industry to our economy, and not incidentally, to our national security. We believe that the national security vs. economic arguments present a false choice, and that a well-balanced and realistic compromise is within reach.

The Security and Freedom Through Encryption Act (SAFE) is a vital aspect of the strategy to develop a meaningful Information Age encryption policy, and we sincerely appreciate the tremendous efforts of Congressmen Goodlatte and Lofgren as leaders of effort. Among other things, this bill would reaffirm the right of all Americans to use whatever encryption they choose to protect themselves, their digital property, and their electronic communications. Furthermore, it would prevent the Government from requiring businesses to use only certain types of encryption in their global operations. EIA is excited to be part of the coalition working to enact this important legislation, and we look forward to working with this committee towards that end.

EIA has also put forward a proposal which we urge the Administration to consider, and which is attached to my written testimony. In brief, our compromise proposal has four basic elements. First, the Government needs to significantly ease the restrictions on low-level and mass market encryption software. It was not very long ago that encryption was a solely military application, and therefore easily con-

trolled, but to continue imposing onerous controls on software which anyone can purchase at the local shopping mall just does not make sense.

Second, the law enforcement and national security agencies could better define their access requirements, thereby allowing industry to develop a variety of marketable solutions, as well as enabling the Clinton Administration to finally abandon its key recovery policy.

Third, our new policy needs to differentiate between the increasingly numerous uses for the technology, such as for voice communications, data transmission, and in consumer electronics, with appropriate controls on those applications that clearly present problems for Government, and decontrolling the rest.

Finally, U.S. policymakers need to recognize the futility of unilateral export restrictions, which serve only to damage our domestic industries while doing little to protect our national security. Only when we encourage our allies to develop meaningful multilateral controls can we hope to prevent the bad actors from acquiring these technologies.

The bottom line is, we in the high-tech industry believe this is a controversy which has dragged on for too long, and that a reasonable solution is possible if all sides are willing to compromise. Our industry is willing to accept restrictions on exports if the controls are reasonable, if they are effective at addressing the problem they are meant to solve, and if they do not impose unnecessary, overly burdensome requirements. We believe that by implementing these basic proposals, the Administration's legitimate concerns can be addressed, the U.S. high-tech industry will be allowed to compete globally, and users will have the security they need.

I would be happy to take your questions.

Mr. GOODLATTE. Before we take questions, if there are no objections, I would like to put two items in the record:

One is a *National Journal's Technology Daily*, March 1, 1999, p.m. edition, an article on encryption, entitled "Relaxing in Europe," and let me just read briefly from it. "The EU has always taken a liberal approach on encryption, said DeGraaf—referring to Gerard DeGraaf, First Secretary of the European Union's Washington delegation. "We feel that in many instances restrictions are not always the best way of protecting national security. "The European Union has resisted U.S. efforts to gain international support for key recovery," DeGraaf said. He noted that an announcement earlier this year by France that it plans to ease controls on encryption within that country brings the French more in line with the rest of Europe."

Secondly, an article prepared by the Business Software Alliance, a study entitled, "The Cost of Government-Driven Key Escrow Encryption," which concludes that the cost per key request for key recovery will average \$12 million, an estimate of over \$7 billion as an annual cost and an estimate of about 640 requests from law enforcement agencies for what I think is a staggering \$12 million for each wiretap, which involves getting a key to decrypt somebody's communication.

At this time, we will turn to questions.

Professor Denning, we appreciate your testimony.

[The information referred to follows:]

National
Journals
TECHNOLOGYdaily

03-01-1999

Relaxing In Europe

European Union officials are examining whether to relax controls on the export of encryption products within the borders of its member states, an EU official said.

While discussions are in the early stages, officials are considering some liberalization of encryption export rules as part of a review of policies on dual-use products, those that have both military and commercial value, according to Gerard de Graaf, first secretary to the European Union's Washington delegation. A proposal could be made before the summer, he said.

"The EU has always taken a liberal approach on encryption," de Graaf told National Journal's Technology Daily. "We feel in many instances, restrictions are not always the best way of protecting national security."

The Clinton Administration is concerned that increasing the availability of encryption technology, which scrambles data or communications for privacy, will lead to its broader use, hampering law enforcement and intelligence gathering.

A significant liberalization in EU encryption rules could undermine U.S. efforts to create an international regime in the more restrictive U.S. mold. It would bolster industry's argument that the United States cannot control the spread of robust encryption, and that controls on the export of U.S. products will only lead to a loss in market share for American companies.

"To the extent that they lessen restrictions on exports and adopt standards that were seeking to adopt here in the U.S. that would be helpful," said Rep. Rick Boucher D-VA, co-chairman of the Congressional Internet Caucus. He introduced H.R. 850 last week with Rep. Bob Goodlatte R-VA, legislation to ease U.S. controls on encryption exports.

The European Union has resisted U.S. efforts to gain international support for key-recovery, de Graaf said. He noted that an announcement earlier this year by France that it plans to ease controls on encryption within that country brings the French more in line with the rest of Europe.

One notable exception is Great Britain, which has floated a proposal for establishment of a voluntary third-party key escrow system. The proposal calls for licensing key-escrow agents who would hold a "key" needed to unscramble encrypted data or communications.

National Journal's Technology Daily

TABLE OF CONTENTS

	Executive Summary	1
	1. Introductory Background	2
	1.1 Purpose	3
	1.2 Assumptions and Limitations	3
	1.3 Summary Findings	4
	2. The Increasing Use of Encryption	5
	3. Costs of Third-Party Key Escrow	5
	3.1 Based on Conservative Estimates, On Average, 89.2 Million People Will Escrow Encryption Keys Each Year	7
	3.1.1 Keys Held by Employees and Business Establishments	8
	3.1.2 Keys Held by Home Users	8
	3.2 Users' Cost Will Average \$1.7 Billion Per Year	9
	3.3 Payments to Escrow Agents Will Average \$6.0 Billion Per Year	10
	3.3.1 Escrow Services for Businesses Will Cost \$4.2 Billion Per Year	10
	3.3.2 Escrow Services for Households Will Cost \$1.8 Billion Per Year	11
	3.3.3 Annual Cost of Key Recovery Requests Will Average \$12 Million Per Request	11
	Appendix	12

Despite the almost decade-long national debate about U.S. encryption policy and the FBI's repeated calls for back-door access to encrypted information, there has been no careful analysis of the cost of a government-inspired key escrow encryption system. In this report, Nathan Associates Inc., commissioned by the Business Software Alliance, provides one. As a result of this analysis, we now know that a government-driven key escrow encryption system is a very expensive proposition for American taxpayers and computer users. This expense must be weighed against the utility of such a system in the deliberations about U.S. encryption policy.

The main findings of the study are highlighted below:

- The total direct cost of the kind of key escrow encryption system envisioned by the U.S. government is \$7.7 billion per year and \$38.5 billion over five years.
- The cost for users to comply with such a key escrow system is at least \$1.7 billion per year.
- The payments that users would have to make to escrow agents to comply with this system is \$6.0 billion per year.
- The average annual cost of each court-approved "wiretap" under this system is \$12.0 million.

As anyone who follows this issue knows, U.S. encryption policy is very controversial. This study does not address the differences of opinion about whether a government-inspired key escrow encryption system is technologically feasible or whether criminals who want to avoid law enforcement will use it. The BSA continues to have reservations about the feasibility and ultimate merit of such a system. The high cost documented in this study only adds to their concerns.

1.

INTRODUCTORY BACKGROUND

In this digital age of encrypted electronic communications and stored data, governments are seeking ways to preserve a "wiretapping capability" (remote anonymous access) for law enforcement purposes. Encryption is based on mathematical procedures to scramble data so that it is extremely difficult – if not impossible – for anyone other than the authorized recipients to recover the original "plaintext." Encryption is used to protect data and prevent crimes. Governments also are concerned that criminals will use encryption to conceal their communications and illicit data. Therefore, a government-inspired "key escrow" proposal floated among policymakers in the United States attempts to address the issue — encrypted data and communications. The proposal requires computer users to keep the keys to their encrypted electronically-stored data *and* their encrypted communications with a government-approved third party (escrow agent).¹ When appropriately requested by an authorized law enforcement official, the escrow agent would be required to reveal the key without notifying the encryption user, thereby preserving the ability of governments to secretly monitor electronically-communicated and stored information. Although it is argued that revealed keys would only be used in appropriate judicially-approved circumstances,² for the system to be functional, all computer users that employ security systems based on encryption technologies will be subject to the requirement.

In a May 1997 report, the Center for Democracy and Technology (CDT) examined the funda-

mental properties of a variety of proposed encryption key escrow requirements, including a government-mandated key escrow system.³ The report addresses tradeoffs that naturally exist in any key recovery system.⁴ For example, the most secure third-party key escrow system will impose the highest costs on encryption users and the greatest incentive not to comply. But, a simple and relatively inexpensive system is likely to be insecure, and, in the end, more costly to society.

While the CDT study identifies cost categories of any key escrow system, it did not quantify cost. The four categories of costs identified in the report were:

1. **Operational costs of key escrow agents:** Costs of maintaining and controlling keys, and responding to law enforcement requests for keys.
2. **User costs:** Expense of choosing, using, and managing a key escrow system, as well as the cost of losses from lessened security and mistaken or fraudulent disclosures of sensitive data.
3. **Product design and engineering costs:** New expenses incurred to design secure products that conform to the key escrow requirements.
4. **Government oversight costs:** New budgetary requirements for government, law enforcement, and private certification bodies to test and approve key escrow products, certify and audit approved escrow agents, and support law enforcement requests for and use of recovered key information.

1.1

3

PURPOSE

This study, prepared by the Family, Industry, and Community Economics group of Nathan Associates Inc., analyzes and estimates the direct cost of a government-approved, third-party key escrow system. Within the system, costs will be imposed on businesses whose employees encrypt communications and sensitive data, and on households that access the Internet and have a need to use encryption. Medical records, electronic commerce, home banking, and electronic mail are particularly important and rapidly growing applications requiring encryption.

The Nathan Associates study considers only the first two cost categories identified in the CDT report: the operational costs of key recovery escrow agents (which users will be required to pay to the escrow agent) and user costs. Escrow agents' costs, passed on to the user, will include escrow account set-up and maintenance costs, as well as the cost of recovering keys. User costs are the monetary value of time spent complying with the mandate, and the cost of unauthorized use of sensitive data, the latter of which is not analyzed here.

The estimate was developed in the following three-step process:

- Estimate the number of encryption users required to comply with the mandate and the number of keys to be held in escrow.
- Estimate the user costs of time spent complying with the mandate.
- Estimate the operational costs of key recovery escrow agents.

The cost estimates are based only on

escrow services demanded and provided in the United States. To be effective, government law enforcement agencies will need to require access to encrypted communications and electronically-stored data *worldwide*, a factor not accounted for here.

Finally, only direct costs were estimated. When encryption users are required to purchase third-party key escrow services, the pattern of spending on all goods and services in the U.S. economy will be disrupted. Sales in some industries will decline and, as a result, cost-cutting measures will be taken, including laying off employees. These and other indirect impacts have not been estimated.

1.2

APPROACH TO ESTIMATION

The approach to key recovery analyzed in this study differs from the current market-driven approach. Businesses are demanding key recovery services only for their encrypted electronically-stored data, not for their electronic communications. Furthermore, most users choose where to place their keys, often choosing to self-escrow keys. The proposal analyzed here, however, will require businesses and home users of encryption to keep keys in escrow for communications, as well as stored data. Moreover, it will require such escrow to be with a government-approved third party. While the proposal will allow self-escrow to a limited extent and "other" (non-specified) recovery mechanisms, the basic thrust remains government-approved third-party escrow.

The analysis we present is based on two key assumptions. First, we must assume that the system

mandated is technologically feasible and secure. The CDT report questions its feasibility and finds that any key recovery infrastructure introduces vulnerabilities.⁵ By entrusting keys with a third party, the third party itself becomes a point of vulnerability. In addition, the key repositories become high-value targets for those seeking access to encrypted communications and data. Second, we assume that users, including criminals who want to avoid law enforcement, will comply with the mandate. This assumption also has been widely questioned.⁶

Few companies currently offer encryption key recovery services. Those that do serve the business community by escrowing keys to stored databases, not encrypted communications. Although the issue of key recovery is global, the analysis and estimates presented here are relevant to the U.S. market only.

The cost-estimating methodology is based on three additional assumptions. First, we make the simplifying assumption that an encryption user will set-up and maintain an escrow account with a key escrow service provider, and, more importantly, pay a fee for the escrow service that does not vary with the number of keys held by the user. Given the number of keys an individual could generate, this is a significant assumption. Certainly the cost of the system will vary with the number of keys held in escrow, but determining the number of keys and how the number of keys will affect the cost of the system requires information that currently is not available. Second, for the purpose of estimating the cost of providing key escrow services to U.S. households, we assume that the basic fee structure will be similar to the current fee structure for safe deposit box services at commercial banks. However, another measure we could have chosen is the monthly fee paid for a home security alarm monitoring service. When you compare safe deposit box fees to home security alarm monitoring fees, the

difference is significant. The fee for a safe deposit box is approximately \$40 *per year*. The fee for a home security monitoring service is approximately \$40 *per month*. Our third assumption is that user costs are measured by the opportunity cost of time spent complying with the mandate.

The costs estimated here represent only a fraction of all costs that will be imposed on the U.S. economy by the government mandate. First, we consider only the first two cost categories identified in the CDT report: the operational costs of key recovery escrow agents and user costs. More importantly, our user costs estimate does not include costs of compromised sensitive data. No product design, engineering, and government oversight costs are included here. Second, the costs we estimated are only the *direct* impacts of the mandate. Indirect impacts on sales and employment throughout the U.S. economy are not quantified here.

1.3

The cost of the mandate will total at least \$7.7 billion per year during its first five years. In the initial year, 88 percent of this amount will be incurred by U.S. business establishments whose employees use encryption. By the fifth year, however, increasing demand for Internet access and electronic commerce by home users of personal computers will shift the majority of the costs onto U.S. households. Therefore, only 36 percent of the cost of the mandate will be incurred by U.S. business establishments in the fifth year of the mandate. The annual cost of the mandate is equivalent to \$12 million per court-approved "wiretap" order and \$6,000 per "wiretap-order-allowed listening opportunity."

Although the estimate detailed here is a very conservative accounting of all costs, it is significant.

An average annual cost of \$7.7 billion represents more than seven percent of sales of all products and services by the software industry in the U.S. economy?⁷

The remainder of this report describes these and other estimates in more detail. All cost estimates are detailed in Section 3. Data and calculations are presented in the Appendix.

2.

THE INCREASING USE OF ENCRYPTION

The use of sophisticated encryption products is on the rise. At the end of 1997, 1,619 hardware and software encryption products were produced and distributed by 949 companies in at least 68 countries.⁸ More than half (56 percent) of these products were produced in the United States. Based on a survey of 1,600 U.S. businesses, the U.S. Chamber of Commerce estimated that, in 1995, 17 percent of U.S. businesses used encryption to protect confidentiality.⁹ Another survey of 1,300 information-security managers conducted in 1996 by Ernst & Young and *Information Week* found that 26 percent used encryption to protect data files, and 17 percent used encryption to protect telecommunications.¹⁰ The Chamber of Commerce estimates the use of encryption by U.S. businesses is growing 29 percent per year.¹¹ By 2000, 60 percent of U.S. businesses will use encryption.

3.

COSTS OF THIRD PARTY KEY ESCROW

The key recovery proposal analyzed in this study is one requiring the escrow of encryption keys with a government-approved third party. Keys to encrypted electronic digital communications *and* electronically stored data will be escrowed. In the evolving market for encryption and key recovery, businesses are demanding key recovery services only for encrypted stored data, but not for their electronic communications. Therefore, data available for estimating the cost of the requirement are limited.

Data limitations require reliance on the following specific assumptions:

- The key recovery system is technologically feasible and secure.
- Encryption users will comply with the mandate.
- Users of encryption will pay key escrow service providers to set up and maintain a key escrow account, the fee for which does not vary with the number of keys held in escrow in the account.

We consider two sources of demand for key escrow services. U.S. business establishments employing workers using encryption will be required to set-up and maintain escrow service agreements. U.S. households using encryption also will be required to escrow their encryption keys.

The total cost estimated here includes only the following two cost categories representing part of four cost categories identified in the CDT report.

- Operational costs of key recovery agents.
- User costs.

Businesses and households will pay the operational costs of key recovery agents. The agents will charge encryption users fees to cover the costs of setting up and maintaining an escrow account. They also will pass on to businesses and households the

cost of requests by the government for key recovery. (Although business establishments, employees, and home users could conceivably request recovery of their keys, we do not include the agents' costs of complying with such requests.) User costs are measured by the time spent complying with the mandate. Compliance activities include finding escrow service providers, reviewing contract offerings, choosing from among competing service providers, and entering into a written service contract.

The period of our analysis is the first five years of the mandate. The five-year time frame allows for growth in the demand for encryption based on recent trends. More importantly, it eliminates the distortion of the high cost that will occur during the first year of the mandate when all businesses and households currently using encryption will be required to enter into escrow service agreements.

The general methodology consists of three major steps. First, we estimate the number of people in the United States using encryption. U.S. workers using encryption are allocated to business establishments to derive an estimate of the number of U.S. business establishments that must set-up and maintain key escrow accounts with escrow service providers. Each home user of encryption will be required to set-up and maintain a key escrow account. Next, we estimate the costs of complying with the mandate. Compliance activities are the responsibility of each establishment employing workers who use encryption and each home user of encryption. In the third step, we estimate escrow account set-up and annual maintenance fees, and the cost incurred to comply with a key recovery request from government law enforcement agencies. The average annual estimated costs by major category and market segment are summarized as follows.

<i>Cost Category and Market Segment</i>	<i>Average Annual Cost (\$millions)</i>
USERS' COSTS	
Compliance by establishments	112.03
Compliance by households	1,577.16
TOTAL	1,689.19
USER FEES TO COVER ESCROW	
AGENTS COSTS	
Paid per establishment	
Set-up	1,712.39
Account maintenance	2,473.64
Subtotal	4,186.07
Paid per employee	
Account maintenance	21.44
Key recovery incidents	.02
Subtotal	21.46
Total	4,207.53
Paid per home user	
Set-up and maintenance	1,779.09
Key recovery incidents	.02
Subtotal	1,779.11
TOTAL	5,986.64
GRAND TOTAL	7,675.83

3.1

7

ESTIMATION OF THE NUMBER OF ENCRYPTION USERS AND THE NUMBER OF KEYS HELD IN ESCROW

In this analysis, an encryption user is anyone who at any time during the year sent or received an encrypted communication or worked with encrypted electronically-stored data. People use encryption, often without knowing that they are doing so. For example, encryption is used when someone establishes Internet connections through an Internet service provider and accesses a page on the World Wide Web. Anyone who engages in electronic commerce transactions uses encryption, as do people who engage in electronic banking transactions or other electronic financial transactions. Employees who connect to a client-server network rely on an encrypted connection to provide a secure passageway to the network. When employees connect to their office computer while at home or otherwise away from the office, their connection is encrypted.

The cost of requiring encryption users to hold keys in escrow will depend first on the number of users and then on the number of encryption keys used by each. Because of the complexity of this issue, we made the very conservative assumption that each encryption user holds only one key. This assumption, made purely for the sake of simplicity, results in an extremely low estimate of the number of keys held in escrow. Encryption users can generate new keys practically every time they log onto a new Internet web site (and, in fact, do so with a popular technology, secure socket layer or SSL), save a document or send a message. Repeatedly generating new keys is recommended for the highest levels of security—to protect against crime. Further-

more it is likely that they will use different keys for different applications. For example, users might choose one key for personal use and another for business use. Within these two categories, users might choose one key for their electronic communications and another for their electronically-stored information. Moreover, within this layer, users might choose to encrypt different applications differently. For example, Internet transactions using one Internet service provider might be encrypted one way; transactions using another provider might be encrypted another way. The database created using one developer's application software might be encrypted differently from the database created using another developer's application.

On average, 89.2 million people will use encryption at least once and hold at least one key in escrow during each year of our analysis. Of these total users, 44.8 million will be using encryption at work (35 percent of the 129.6 million employed civilians in the U.S. economy in 1997) and 44.5 million will be using encryption at home.

Hidden in the annual average is a shifting pattern of use. In the first year, 43.3 million people use encryption at work, and only 19.5 million people use encryption at home. By the fifth year, Internet home use will have grown substantially. As a result, 67.6 million people will be using encryption at home in the fifth year. Only 46.3 million people will be using encryption at work.

3.1.1

KEYS HELD BY EMPLOYEES AND BUSINESS ESTABLISHMENTS

According to a report by the U.S. Census Bureau, 51.1 million adults used computers at work in 1993.¹² Approximately 41 million, or 22 percent of the U.S. adult population, were reported to use computers in occupations that we deemed more likely to involve the use of encrypted communications or data. Such occupations are executive, administrative, and management; professional specialties; sales; and administrative and clerical.

Even with the conservative assumption that the proportion of the U.S. adult population using computers at work in these occupations in 1997 is no different from the proportion in 1993, we still concluded that a total of 43.3 million people used encryption at least once at work during 1997.

Starting with this estimate for the first year of our analysis, we project use to grow 1.7 percent per year during the succeeding four years.¹³ In the fifth year, 46.3 million employees will be using encryption at work at least once. Over the five years of our analysis, the average number of employees using encryption per year at least once during the year is 44.8 million, approximately 35 percent of the 129.6 million civilians employed in 1997.

Based on the distribution of employees by establishment size in the U.S. economy in 1995, we

estimated 3.1 million U.S. establishments employed workers who used encryption at least once in 1997. These establishments were mostly small; 89 percent employed fewer than 25 people. Of all encryption users at work, 29 percent were employed at these small establishments. If a third-party key escrow proposal is adopted through mandates or incentives that provide few alternatives, by the fifth year after adoption, 3,270,000 establishments will require escrow services for the encryption keys used by their employees.

3.1.2

Internet users accessing the World Wide Web via Netscape's Navigator Browser, Microsoft's Internet Explorer, or by most other means, will be using encryption (SSL) probably without realizing it. Thus, based on household Internet access, the 19.5 million people who accessed the Internet also used encryption at home at least once in 1997. Reported demand for Internet access ranges from 16 million to 23 million.¹⁴ Although Internet home use has been reportedly growing 75 percent per year, our projection of household demand for encryption is based on successive yearly increases of 60 percent, 45 percent, 30 percent, and 15 percent, respectively. By the fifth year of our period of analysis, 67.6 million people will be using encryption at home at least once during the year.

3.2

U.S. USER COSTS WILL AVERAGE \$1.7 BILLION PER YEAR

To estimate the user costs of complying with the mandate, we need to estimate the amount of time users spend each year in compliance activities and the monetary value of their time. Compliance activities include identifying escrow service providers, obtaining fee structures from service providers, reviewing agreement offerings, completing an agreement, transmitting the materials to be escrowed, and updating and monitoring the agreement as necessary.

The total time spent on compliance activities by each user of encryption will be, at the barest minimum, three hours each year. Identifying escrow service providers can involve as little as perusing a telephone directory or going to the Internet. We estimate each user will spend at least 15 minutes on the initial activities of identifying service providers, contacting at least two providers, and requesting information on their service offerings and fees. It is not unreasonable to assume that an individual will take 20 minutes to review carefully an escrow service agreement and its fee structure. A careful review of the terms of agreement offered by at least two competing service providers will require at least 40 minutes. Choosing a provider, completing an agreement, and transmitting the items to be escrowed is likely to take at least an additional 60 minutes. And, in the course of a year, it is likely that users will devote at least another hour to maintaining their relationships with their escrow service providers. Hence, in total, during a year, each user will likely spend a minimum of 2 hours and 55 minutes in compliance activities.

We make the further conservative assumption that compliance activities will be the responsibility of a single individual at all business establishments with employees using encryption. Each home user of encryption also will spend time on compliance activities.

The remaining piece of information required to estimate total compliance costs at U.S. business establishments and at U.S. households is the value of the time of the individual engaged in compliance activities. In this analysis, we do not distinguish between the time value of the employee at the business establishment who is responsible for compliance activities and the time value of the home users of encryption. A monetary value of time spent on these activities is conservatively measured by the average annual wages of all U.S. employees.

The monetary value of time spent on compliance activities is at least \$11.82 per hour, the average hourly earnings of employees in private nonagricultural industries in 1996.¹⁵ Studies have shown that employees who use computers at work earn wages that are 10 percent to 15 percent higher than the wages earned by those who do not use computers at work.¹⁶ Therefore, the value of time spent on compliance activities is likely to be greater than \$11.82 per hour.

The total cost of compliance per year will be \$1.7 billion. On average, more than 3 million U.S. business establishments will spend 9.5 million hours or \$112 million per year on compliance activities. U.S. households will spend 133.4 million hours or \$1.6 billion per year on compliance.

3.3

PAYMENTS TO ESCROW AGENTS WILL AVERAGE \$6.0 BILLION PER YEAR

The government mandate will require U.S. business establishments and households to establish and maintain key escrow agreements with escrow service providers. The providers of escrow services will charge customers for the costs of setting up escrow accounts. Escrow agents also will incur costs associated with government requests for key recovery.

Our estimate of the payments to escrow agents to comply with the government mandate is based on the simplifying assumption that escrow service providers charge a set fee for an escrow account. For businesses whose workers use encryption, the account is opened and held by the business establishment. The fee varies with the number of employees at the establishment who use encryption, but not with the number of keys used by each employee. The fee charged home users likewise does not vary with the number of keys used and escrowed by the home user of encryption.

The fee structure analyzed here should not be interpreted to mean that the cost of the infrastructure required by the government mandate will not be sensitive to the number of keys held in escrow. Indeed, as explained earlier in section 3.1, it is likely that encryption users will require different keys for different uses and applications and, hence, have to hold numerous keys in escrow. Instead, the fees analyzed here should be thought of as the minimum cost of providing key escrow service to the typical encryption user, because we assume only one key per user per year.

Although one would expect to find some economies of scale in the provision of key escrow

service, the data available to us are not adequate for modeling and measuring these economies. The limitations of the data are perhaps most obvious in the home segment of the market, where we estimate the fee per account to be \$40, based on a typical annual fee for safe-deposit box rental at commercial banks. Even box rentals vary with the size of the box. But for a given box size, the renter can hold one or more valuables without paying a higher fee.

3.3.1

ESTABLISHMENTS WILL PAY \$4.2 BILLION PER YEAR TO SET UP AND MAINTAIN ESCROW ACCOUNTS

In the business segment of the market, the fee structure of escrow service providers will consist of a set-up fee and an annual maintenance fee. Business establishments whose workers use encryption will be required to pay the set-up fee, which varies with the number of employees at the establishment. Larger establishments pay a higher set-up fee. The annual maintenance fee consists of an establishment component and a component based on the number of employees with keys held in escrow. The per employee maintenance fee varies with the number of employees at the establishment. Smaller establishments pay a higher per employee maintenance fee.

During the first five years of the escrow requirement, business establishments will pay \$4.2 billion per year to set-up and maintain escrow agreements with service providers. The set-up fee will range from \$2,500 for the smallest establishments to \$25,000 for the largest.¹⁷ Annual maintenance fees will be approximately \$783 per year, regardless of the size of the establishment.¹⁸ Annual per employee fees will range from \$1.00 at the smallest establishments to \$0.05 at the largest establishments.¹⁹

3.3.2

ESCROW SERVICES FOR HOUSEHOLDS WILL COST \$1.8 BILLION PER YEAR

For the purpose of estimating the cost of providing key escrow services to U.S. households, we assume that the basic fee structure will be similar to the current fee structure for safe deposit box service at commercial banks. Alternatively, the fee might approximate the current fee for home security alarm monitoring services. The difference is significant. The fee for a safe deposit box is approximately \$40 per year. The fee for a home security monitoring service is approximately \$40 per month.

The total fee for all home users will average \$1.8 billion per year during the first five years of the requirement. Again, this figure is based on the conservative estimate that home users pay a combined set-up and maintenance fee of \$40 per year.

3.3.3

ANNUAL COST OF KEY RECOVERY REQUESTS WILL BE \$12 MILLION PER REQUEST

The major purpose of requiring that encryption keys be held in escrow is to maintain the government's ability to conduct covert surveillance in the electronic digital age. Therefore, an additional element of payments to escrow agents must account for the costs of complying with government requests for key recovery under the mandate.

Individuals, as well as governments, could make requests for key recovery. In this report, we estimate costs for incidents of request by the government only. Costs will depend on the number of requests and the cost per request.

Assuming that the criminal tendency of the population of encryption users is not significantly different from the tendency of the general adult population, key recovery requests will range from 444 during the first year of our analysis to 851 during the fifth year, an average 640 per year. Our

estimate is based on the incidence of court-approved wiretap orders in 1996—7.076 per million adults between the ages of 18 and 64. In 1996, the courts approved 1,149 orders that allowed federal, state, and local law enforcement officials to listen to approximately 2.3 million telephone calls.²⁰ The adult population between the ages of 18 and 64 totaled 162.4 million in 1996. Our estimate of key recovery requests is the product of the incidence rate and the number of encryption users.

The cost per key recovery request will be \$69, an estimate that is an average of costs reported by two sources.²¹ Combining the number of key recovery requests and the cost per request yields an estimate of escrow agents' cost of key recovery requests that averages \$44,200 per year. Although this amount seems small, it is only one cost component.

The *entire* cost of the government mandate can be attributed to the government's purported need to secretly monitor electronic digital communications and electronically-stored data. Therefore, the cost of key recovery is more appropriately measured on the basis of the total cost of the mandate. When expressed in this manner, the cost averages \$12 million per request (\$7.7 billion divided by 640 requests). On the basis of the number of telephone conversations that will be monitored as a result of these requests, the cost will be \$6,000 per call (\$7.7 billion divided by 1.3 monitored calls).

Protecting the privacy of citizens in the digital era presents unique technological challenges. If citizens who protect their privacy using encryption were required to keep in escrow the key to decoding their encrypted communications and data, U.S. business establishments and households would incur an average annual cost of \$7.7 billion. Based on average annual number of key recovery requests, the infrastructure cost will total \$12 million per request per year, an apparently expensive undertaking.

APPENDIX

12

The Constitution of the United States

¹ "Key escrow" in this paper refers to proposals under which keys would be stored with government approved third parties. This study does not analyze the costs of voluntary, market driven key recovery, which has different components and assumptions. Many such systems involve self-escrow systems. Additionally, some in law enforcement argue that a key escrow system or other system that guarantees access to plaintext data would be acceptable. However, this study does not address the other systems because it is unclear which systems would be acceptable. The study only addresses third party government-approved systems.

² There is some question as to whether this can be accomplished under existing legal authority or whether it would require an expansion of such authority, issues not addressed here.

³ *The Risks of Key Recovery, Key Escrows, and Trusted Third Party Encryption, A Report by an Ad Hoc Group of Cryptographers and Computer Scientists*, Center for Democracy and Technology, Washington, May 1997.

⁴ *Ibid.*, p. 18.

⁵ *Ibid.*, p. 11.

⁶ Hearing of the Subcommittee on the Constitution, Federalism, and Property Rights, Senate Committee on the Judiciary, March 17, 1998.

⁷ Software companies' receipts from sales of all U.S. software industry products and services totaled \$102.8 billion in 1996. See Nathan Associates Inc., *Building an Information Economy, Software Industry Positions U.S. for New, Digital Era*, Business Software Alliance, Washington, June 1997.

⁸ See http://www.isa.com/research/crypto/crypt_surv.html; Internet.

⁹ See "Encryption Policy and Market Trends," Dorothy E. Denning, May 17, 1997, <http://www.orac.georgetown.edu/~denning/crypto/Trends.html>; Internet, p. 3.

¹⁰ *Ibid.*, p. 4.

¹¹ *Ibid.*, pp. 3-4.

¹² *Computer Use in the United States: October 1993*, U.S. Census Bureau.

¹³ Projected rate is based on the Bureau of Labor Statistics, *Employment Outlook: 1994 to 2005*, U.S. Department of Labor.

¹⁴ See www.cisnd.com/news/inctash.html; Internet and strg.findsvp.com/financial/homeuse.html; Internet.

¹⁵ *Economic Report of the President*, February 1997, Table B-45, p. 352.

¹⁶ Alan B. Krueger, "How Computers Have Changed the Wage Structure: Evidence From Microdata, 1984-1989," *Quarterly Journal of Economics*, CVIII (1), 1993.

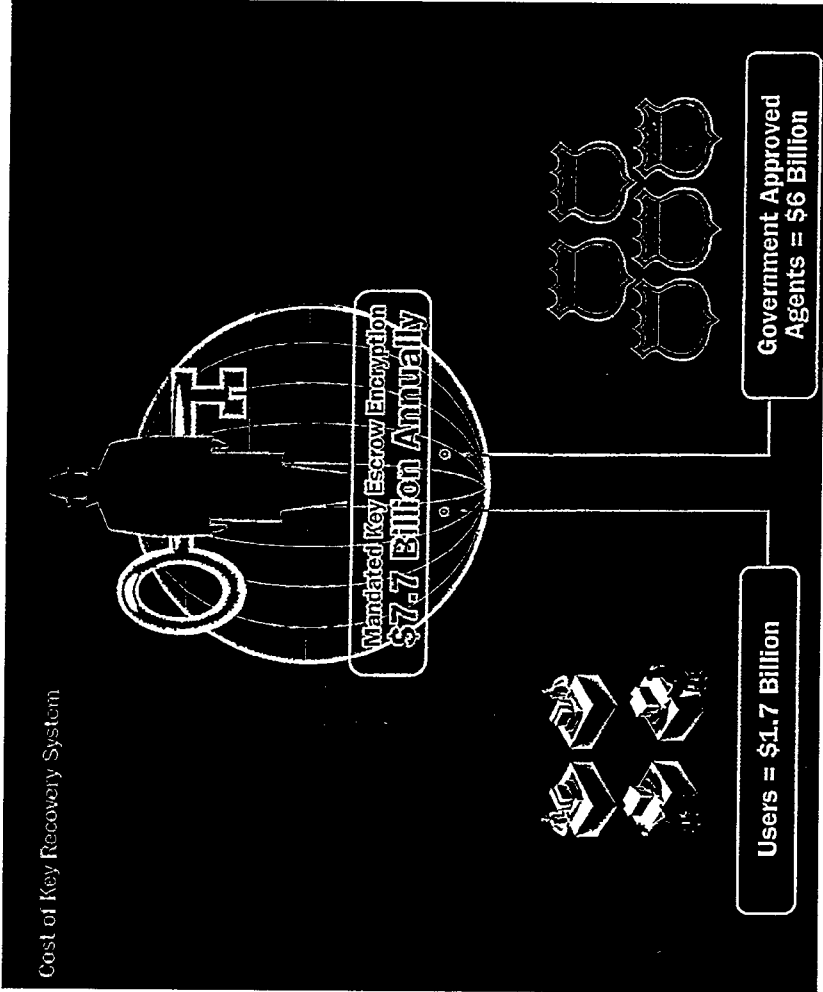
¹⁷ Based on information reported by DataSecurities International and Sourcefile.

¹⁸ Based on set-up fees reported by Fort Knox Escrow Services, International Escrow Corp., and Timberwolf Systems, Inc.

¹⁹ Based on information provided by DataSecurities International.

²⁰ Neil Munro, "TECHNOLOGY What Bugs The FBI," *National Journal*, May 9, 1998, p. 2.

²¹ International Escrow Corp. reported a cost per request of \$75. Sourcefile, a provider of software escrow services, reported the cost could range between \$25 and \$100, which yields an average of \$62.50.



You state in your testimony that amendments such as those introduced in the last Congress to impose domestic regulations could upset the delicate balances among our national interests.

Would you please specifically describe the amendments to which you are referring? Are you talking about the Oxley-Manton amendment at the Commerce Committee and the domestic provisions of the substitute amendment adopted by the Intelligence Committee?

Ms. DENNING. Yes, I guess that was maybe 2 years ago. I was not in favor of those.

Mr. GOODLATTE. You also argue that the SAFE Act would remove industry incentives to accommodate law enforcement and national defense interests. Is it your position that industry will not cooperate with Government in addressing its law enforcement and security needs unless coerced by export controls?

Ms. DENNING. It was more just as I see it over the years because of the export controls. I think it was an incentive for industry to look at recovery, look at different ways of doing it, addressing it, coming together to try to develop standards for it, looking at what the cost of it would be; and so I think that a lot of that activity might not have taken place if there hadn't been export controls.

Mr. GOODLATTE. Mr. Parenty, you are here on behalf of some of America's largest software manufacturers, and Mr. McCurdy on behalf of almost all of America's largest hardware manufacturers, who make a whole host of products that rely upon the use of encryption to protect copyrighted materials. I know that one of Mr. McCurdy's members is located in my State, Circuit City, which has developed a machine called DIVX, dealing with DVD technology and using encryption on a per-use basis to protect motion pictures that are—basically, it is a new way of being able to rent movies without going to the rental store.

Would you comment on, one, the need for relaxed controls to deal with these literally thousands of hardware and software applications that we want to be able to export and, in many instances, cannot now; and two, your willingness to cooperate with law enforcement and national defense folks in the future if this legislation were passed?

Mr. PARENTY. I can start.

With respect to your second question, that regarding cooperation on the part of the U.S. computer industry with national security and law enforcement interests if one talked genuinely to reps of NSA and the Justice Department, they have no real problems dealing with U.S. companies. U.S. companies have a long history of cooperation with the Federal Government to try to aid our national security. In point of fact, many of the people in industry who are involved in security are like myself, products of the National Security Agency as well as other agencies.

And so I think that in terms of the means of motivating companies to cooperate with our Federal Government, the best motivation is that we are loyal Americans. It is nothing more complex than that. Attempts through export provisions such as what happened for key recovery products a few years ago is a bludgeon that does not effectively work.

As Professor Denning mentioned, there has been an effort on the part of industry to look at key recovery and that was in part

prompted by a carrot with respect to export controls. However, the essential lesson that came from that is key recovery, as espoused by the Administration, would never sell. It would never be used, and so it was never produced on a wide scale.

What American industry does do is provide products which satisfy customers' needs and insofar as that does, with the encryption of stored data, provide for some kind of recoverable mechanism, we will do that and we welcome law enforcement to take advantage of that.

Mr. McCURDY. Mr. Chairman, I think you raised a very good point. Let me take the second question first.

U.S. manufacturers of computers and electronic systems have long been not only close supporters of U.S. law enforcement and national security agencies; in most instances, we are the ones that actually produce the capability they have to conduct their activities. Recently we saw the passage of CALEA, and the telecommunications industry was extremely cooperative with the FBI in trying to develop proper implementation of that act. What we have seen is that they have overreached again in trying to have requirements that far outstripped the capability of industries, so I think there has to be balance on both sides.

I think there has been a reasonable debate. That is why I again commend you for trying to place pressure on the Administration to come forward with an updated policy.

You are correct in saying that manufacturers of consumer electronics, all kinds of systems that now are facts of life in the digital age, are very concerned about privacy. They are concerned about their intellectual property. They are cognizant that this is an extremely competitive era and that they need encryption capability to protect the valuable investment that they have made in order to improve the quality of life of not only U.S. citizens, but citizens abroad.

Mr. GOODLATTE. Thank you.

The gentleman from California, Mr. Berman.

Mr. BERMAN. Thank you, Mr. Chairman.

Mr. McCurdy, Mr. Norquist, before he left, could not resist the temptation to at least subtly paint this a little bit in partisan terms—the revered and great President Reagan on the one hand and King Newt's emissaries in this Administration.

Actually though, I think you and I both recommend a Reagan Administration with a Richard Pearl in charge of export controls who for availability and issues like that, and spreads of technology, were not very compelling arguments against massive efforts to regulate—that terrible word—regulate the flow of technology to other countries.

So it may be more of a governmental tendency than an ideological one.

Mr. GOODLATTE. I agree.

Ms. LOFGREN. And I agree.

Mr. BERMAN. But the Cold War is over, and you said something that is very interesting, this issue of slowing down, I think in the context of trying to stop proliferation of nuclear technology or missile technology. Slowing down may just be the best we can get in this very imperfect world.

If we can find one Russian company that has been selling the kind of steel that is necessary for a long-range ballistic missile that is—that Iraq or Iran is seeking to produce, it might delay by a year or two or four their ability to have that independent production capability. They are going to get it in the end, or they are going to get it with a less perfect kind of steel; and therefore it is not going to be quite as operational for them as they might want, but there is some inherent value in slowing it down. And when I hear the talk, I am curious, the talk of the good Americans cooperating with the Government.

Mr. Davidson, just from the point of view of your center or of the civil libertarian or privacy concern, the notion of American companies cooperating with any of the variety of local, State or Federal law enforcement agencies on how to decrypt things which perhaps those—where the people sending and receiving the messages have no knowledge that that cooperation has taken place and that improper, noncourt-ordered, far beyond the legitimate interests of those agencies where decryption is taking place, that itself raises serious kinds of concerns.

I am not sure that is the total—maybe Americans are both—I guess I would be interested in Mr. Parenty's response, but maybe Americans are both patriots and, in terms of this industry, perfectly understanding of what is appropriate to pass on and what isn't, but that is a pretty wise person in every single situation. I am interested in both of your reactions.

Mr. PARENTY. For a small bit of clarification, the kind of cooperation that I was talking about is when national security or law enforcement agencies would come to companies with specific problems for specific issues they were dealing with, and the companies would help explain how their products actually worked, would explain technology.

I did not mean to imply that U.S. companies would explicitly put back doors into our products that would allow U.S. Government access.

Mr. BERMAN. Haven't you in the past?

Mr. PARENTY. There are many products throughout the country. I have never been involved with any companies who deliberately put a back door in. If U.S. companies were to do that and it were found out—and things like this are always found out—it would absolutely ruin whatever credibility we would have, both domestically and overseas; it makes no business sense to do that.

One of the needs or the goals of the tech center was to have industry help law enforcement understand technology. It is a much bigger problem than how do you decrypt a particular message. And as Professor Denning pointed out, security is a lot more than encryption, and law enforcement has a much bigger problem in dealing with technology as a whole than they do with decrypting any particular message.

Mr. BERMAN. Mr. Davidson.

Mr. DAVIDSON. Yes, thank you. I think that the Congressman makes several excellent points. One, on the question of cooperation, I think civil libertarians and privacy advocates are, of course, concerned about back doors being built that people don't know about and what the rules are for access. That is really what it comes

down to, the question that we need to set ground rules for that kind of assistance.

Mr. BERMAN. Can you privatize that decision?

Mr. DAVIDSON. I don't know that contract law is going to be enough. I think where we are going with all of this is a much broader question. There is going to be a lot of plaintext out there. It is not just all about encryption keys; it is also about all of the other data. Encryption keys are just an example of a much broader category and the fact that a lot of data about individuals is held by third parties and by companies and is available by on-line service providers, by Yahoo, amazon.com and other people. And the question is, what are the rules?

We want good ground rules. If we can come up with ground rules that are consistent with our Fourth Amendment constitutional liberties, that will satisfy privacy advocates. But the danger of what is happening right now is that this is all being done behind closed doors. Right now, keys don't have those kinds of strong legal protections. A key can be gotten with a mere request to somebody. What we are very worried about is a situation where companies don't have ground rules that they can fall back on.

If I might just add one quick comment, because I think your comment about the goal is maybe just to slow it down is an excellent question. Let us assume for a second that that has been the goal and we have been successful. We have slowed the spread of encryption up until now. There is going to be a point at which the cost of doing that outweighs the benefits, and I think we have gotten past that point.

Mr. BERMAN. Thank you.

Mr. GILLESPIE. Just in terms of the export policy aspect, the analogy that you mentioned in terms of the Russian steel firm and the manufacture of a missile and, I think, terms of export policy. I think it is important to distinguish where you have with encryption, as Mr. Reinsch noted today, 656 products on the market today from 29 different countries; and it is hard to imagine a happy outcome from the use of a missile by any stretch of the imagination, but clearly, in terms of encryption, the use of that in the marketplace has many happy outcomes that are much more positive than some of the negative outcomes that are a potential.

Mr. MCCURDY. Congressman Berman, if I could, in my experience in this body, there has never been anyone as balanced and fair as you, and you bring a great deal of intelligence and integrity to the process, and I always commend you and admire you for it.

I think the point that you raise is a very good one. The point you raise is that this should not be an ideological debate. I think what you have seen is the bipartisanship that has actually developed around this proposal. It is those who are often fearful of not being able to defend their position who have taken the highly ideological line, and I think that is regrettable. What we have is a need for a new paradigm, if you will, a new way to look at some of these problems.

In addition to my day job, which seems to be all day, I am also a commissioner on the congressionally mandated commission appointed by this Administration to assess the organization of the

Federal Government to combat the proliferation of weapons of mass destruction. That is the name of the commission.

What we are finding is that—and what we have seen for over a year, and a number of years before that in some other work that we are looking at, trying to contain something that has already gone so far—that it is very difficult to pull it back. I am not talking about nuclear threats, we are talking about other kinds of weapons of mass destruction capability.

Our reaction to the problem, I think, was misguided. Rather than address the real problem, which was the brain drain flowing from the former Soviet Union to Iran, Iraq, and places like that, where the knowledge was actually flowing as opposed to the substance itself, whether it is plutonium or some of the other problems—

Mr. BERMAN. I will pay the Iranis not to develop.

Mr. MCCURDY. The fact is that it has already been done.

Mr. BERMAN. I know.

Mr. MCCURDY. As Mr. Delahunt said before about fingers in the dike and he said there is no dike, the only dike that is being built is after the flood has occurred.

I don't fault the NSA for their position. They are trying to do their job and they are trying to do it professionally. The fact of the matter is that the world has changed, and it makes it more difficult for them; and we are all sorry that it makes it more difficult for them, but I believe that there is a higher need now and there is a greater balance. It is now weighted in the other direction, and that is that privacy and protection of individual rights and intellectual property in a highly competitive global economy outweighs the particular concerns that they have now because they cannot effectively control what they say they need to.

Mr. GOODLATTE. In the category of analogies, Congressman Sawyer in the Commerce Committee said it is not like letting the genie out of the bottle; the bottle doesn't exist anymore either.

Congresswoman Lofgren.

Ms. LOFGREN. Thank you very much.

I think this has been a very interesting panel and actually a very interesting day. I think we are all probably weary of sitting at the table, so I will be brief.

I really have just two questions. My first question follows upon Ms. McNamara's testimony this morning that, in her judgment, there were really three elements required for encryption to be broadly dispersed within the marketplace and these had to do with cost, ease of use and infrastructure support. She acknowledged that cost is no longer an issue; acknowledged that ease can still be a problem, although I would note that there are a lot of great products out there that are really easy to use; but she suggested that the third, the infrastructure issue, had not been met and therefore would defer to a later time the broad use of encryption.

To be honest, I didn't understand that point at all, and I am wondering if there is anyone here who can help me understand that point. Tom, we will start with you and just move down the line.

Mr. PARENTY. What the deputy director was referring to has gone by various terms as PKI.

Ms. LOFGREN. Do you think that she meant public key infrastructure?

Mr. PARENTY. She said key management infrastructure, which in the past has been what the Administration has referred to when they are talking about a certificate authority structure that also had some key recovery component involved.

Now, the comment about one of the factors that are delaying the deployment of encryption and its broad use comes from a historical perspective that the way that we would have strong encryption throughout was essentially top down. There would be a small number of, if you will, authorities in the sky that would be the ones responsible for issuing our digital ID and distributing keys and stuff like that. That is not the way that the—

Ms. LOFGREN. It doesn't seem to me that this is the way that this is developing. It is becoming decentralized and it is not governmentally run for the most part and if it works, I think—

Mr. PARENTY. Precisely. It is essentially developing bottom up, where small organizations and companies are building the infrastructures up over time. Those link together, and so while it is true that there is not a global infrastructure or even a national infrastructure, there are countless numbers of individual infrastructures that are being built and will eventually be linked together.

Ms. LOFGREN. Professor Denning is eager to say something.

Ms. DENNING. I was going to say that PKI is, I think, something bigger. It is mainly about interoperability. There is all of this stuff that you can download and use, but suppose I want to send a secure mail electronic message to you. It has got to be compatible, and that is the part that is hard. There are a lot of people I would really like to send a secure e-mail to, and it is complicated. The complication has not very much to do with export controls, but an agreement on standards and then getting that integrated into the e-mail package and other things that we use.

Ms. LOFGREN. Mr. McLaughlin, you have been remarkably silent following your statement. This is your business. Would you like to comment on this?

Mr. MCLAUGHLIN. I would agree and disagree with just about everyone who has already spoken today. It tends to be actually part of my nature to be that way. Sorry.

With regards to is there an infrastructure in place today that will support strong crypto across the Net, the answer is really yes. Mr. Parenty hit it right on the head in that it was originally designed to be a top-down approach, but in reality it has been a bottom-up approach.

Earlier this week there was, in fact, a conference in San Jose, and one of the organizations or associations of individuals got together for a key trading party. Essentially this was a party where they could meet, verify that, yes, this is a warm, living, breathing person who really is this individual. I will now validate that this is you. Let's build something that is called the web of trust.

This has been a process which has been around for actually a number of years and is now beginning to do less around certain standards, such as open PGP X-509, which is a digital certificate standard and is being incorporated as companies.

So I would have to say that it has been—there is an infrastructure in place and rapidly growing, and I would disagree that it is not being effective.

Ms. LOFGREN. Unless someone has something that is different than what has been said so far, I would now like to move to my second question.

This really gets into the issue of industry cooperation with governmental entities. I am aware in Silicon Valley that there are many, many companies who have spent considerable time and money providing very talented people that the Government can't afford to hire made them available to Federal agencies as resources. This is not to inform policy but just as technology resource. I think this is a good thing.

But with that I think it has led to, in some segments, a suspicion, that I think is unfounded, that there is something out there that, if these companies would just reveal it, that it would solve this problem. I don't think that is true. I am eagerly awaiting, therefore, Mr. Lee's report. I am wondering if anybody here can think of a generics other than the so-called "clear zone," which is really nothing new anyhow, that we went through last year with Cisco and some others, whether there is actually some technology out there that would be the rabbit we could pull out of the hat?

Mr. DAVIDSON. I would like to take a shot and say what CDT has seen as part of these discussions about what industry has been able to do and has been most helpful in doing. Something that we have been saying for awhile is that people ultimately have to decrypt the things that they encrypt to make them usable, and there may be a lot of different ways for law enforcement and national security to be able to get at the things that they need to see once they are decrypted.

Ms. LOFGREN. That is not necessarily new technology.

Mr. DAVIDSON. It is not necessarily new technology. To the extent that it is new technology, Congressman Berman's point comes into play, which is that before we go out there deploying all sorts of new surveillance technology, CDT is very concerned that we set the ground rules about their use.

Really, I think industry's best role is to try to help law enforcement use the tools out there and see that there are a lot of ways in which surveillance can be conducted without expanding current law enforcement technology.

Mr. MCCURDY. I, too, look forward to seeing his response, and am glad to provide the industry support to your analysis if you like.

But if I could leave just one thought with you: The software business is for many people—and for years before I took this position I represented a number of software companies—software is difficult for people to visualize and understand. One of the challenges you have is explaining to your colleagues the relevancy of this issue or that—or why it is a difficult problem. Explaining the Is and Os is tough.

Just a quick demonstration of how technology has accelerated and is moving so rapidly, this little chip—it is actually a micro storage device, and I think Howard and I, when we came to Congress, we were the ones trying to get computers into the Congress.

This represents 340 megabytes of storage, 246 floppy disks on that little disk, and these are now commercial. That is where the industry is moving and going.

When we talk about Moore's law and the incredible pace of change, I believe in the software world you are seeing comparable changes. It is an explosion. But this doesn't have to be a negative thing.

Those of us who are more optimistic believe that this technological revolution is going to improve the quality of work and life for millions, if not billions, of people. And as you are trying to explain to people that you can't apply the old concrete solution or thinking to this modern-day problem—the paradigm has totally shifted; this is a new and totally different day—it is perplexing.

But for those who come up and just reflexively give an argument, trust me or whatever, I think there is a higher burden of proof today.

Ms. LOFGREN. I know that I am over my time, and this will be my last comment—

Mr. GOODLATTE. We are going to have some more, so go ahead.

Ms. LOFGREN. I think Mr. Parenty said that he does not oppose export controls in appropriate circumstances, and actually I put myself in that category. The question is, what is appropriate, which always comes down to what is effective; and in this case, we have had a substantial dialogue about whether this accomplishes anything of value, and I think not.

I think that there are—I am glad you showed us the chip because the next thing we are going to be dealing with here are Pentium IIIs, where we have now downgraded the power of what we are going to preclude from export to a point where—if you go to the store and buy a few things—it is not going to work. If we think that our rules are going to prevent the export of the Pentium III chips to people who want them, it is just not going to happen.

I am hopeful, as we proceed on this issue and others, we can look to all of you to help us discuss these matters here in the Congress. There are some of my colleagues who are whizzes technologically and some colleagues who are whizzes in other areas. I hope you can help us appreciate where we are and how fast we are moving, so we can make sound decisions based on the facts, rather than speculative what-ifs and we-wish-if-lys.

Thank you all for being here.

Mr. GOODLATTE. Thank you. Congressman McCurdy, as former chairman of the House Intelligence Committee, do you believe that our national security is helped, not hindered, by a marketplace dominated by U.S. rather than foreign encryption products?

Mr. MCCURDY. Absolutely. There is no question.

Yesterday I testified on reauthorization of the Export Administration Act, and there was an interesting debate that occurred about whether the technology or the spread of technology was weakening our ability to defend ourselves vis-a-vis China and elsewhere; and your colleague from California was very vociferous in his position that—he predicted that in 10 years, we will be at war with China.

Mr. BERMAN. He is referring to Congressman Rohrabacher.

Mr. MCCURDY. My statement is, if you treat someone like an enemy, they will become an enemy.

For years—and, again, I think this is one of the frustrations that we now experience if you are in a Government agency—the Department of Defense, when as a member of the Armed Services Committee in addition to Intelligence—the Federal Government was the developer of the high-end technology. The research and development budget led the industry and led the world in development.

In 1999 that is no longer the case. The private sector actually has a faster cycle time, time to market, development cycle and activity, which is leading the world. It is frustrating for those in Government to realize that they are trying to take a policy and catch up with technology.

When you started this debate 2 years ago—and quite frankly, their position probably had a little bit more merit 2 years ago than it does today—you were talking about 40 bit. Then they said, let's go to 56. They are now talking 64; industry is going to 128 and beyond.

So it is moving at such a rapid pace that there is no way that the policy can catch up. That is why it is very difficult to put it in rigid statutory form. That is why, quite frankly, if I had my druthers, I would say to the Administration—whether it is a Democratic Administration or a Republican Administration—you all have the obligation to have a flexible policy that fits the times rather than have Congress impose a standard, because you can't pick that data point out there that you have opened up. They would be better off if they compromised today and said, let's look at some of these technologies, look at some of these other issues and come up with a realistic policy.

That is going to be a continuous cycle and one that, unfortunately, they will probably be on the lagging side of. Technology outpaces policy 7, 8, 10 times to 1.

Mr. GOODLATTE. Let me ask you about a practical problem that they are going to have even with doing that.

That is, there is an absolute explosion in the number of different types of consumer electronic products that you are familiar with, but also thousands of different software programs. Virtually any kind of software that involves communications or data storage is going to use encryption in the future. How are they ever going to be able to, in a licensing scheme, be able to process those applications one at a time in a market where the product becomes obsolete in 6 months, a year, 18 months in many instances; and you are talking about literally tens of thousands of different applications, different products that have to be cleared?

Mr. MCCURDY. The license process is not keeping pace, and it certainly won't if they shift it back to the State Department or put even more restrictions on it. It is bad enough when you have a bifurcated policy which—agencies, in effect, can slow it, but if you give them the veto power, then you really do have problems. And then our policy is not only futile, but it becomes counterproductive; and that is what we want to avoid.

One last thing, Mr. Chairman. There is a demand—you have to realize that there is a supply side and a demand side. Some of the manufacturers actually represent the supply, but in fact they are

responding to the demand. There is an absolute critical need to be able to protect in this Information Age, Digital Age, your product and the content of that product. That now has intrinsic value. Years ago Is and Os didn't mean that much. Today they are the substance of this economy. They are the value of this economy, and that is why it is so critical that we have a means of protecting it.

Mr. GOODLATTE. One of our colleagues, who is not a member of this committee, has argued that foreign encryption products may be widespread, but they are not secure because they have holes, and the intelligence agencies of the manufacturing countries can access the holes.

I wonder if you, Congressman McCurdy, or Mr. Parenty as a former employee of the NSA, would comment on that argument?

Mr. BERMAN. You had better not.

Mr. PARENTY. First off, to comment on that argument, as a former employee of NSA, would not be a prudent thing for me to do.

Mr. GOODLATTE. Since it has been stated publicly by one of our colleagues, comment on his comment.

Mr. PARENTY. That list that gets bandied around of over 600 foreign encryption products is interesting, but not particularly relevant from my perspective, because the number of vendors that my customers deal with is much smaller. It is a smaller number of established companies who have built a reputation for having products that work and have stood the test of time. So it is clearly possible that there are products in the world out there with back doors in them.

The market does have a way of weeding out products that have vulnerabilities. There have been numerous instances where Netscape browsers, not just for the 40-bit problems but because of problems in the security design, could be compromised. They got fixed; Netscape is a responsible company.

Similar things happen with companies overseas. I would say as advice to the consumers of security products that since it is impossible for you to understand how something was implemented yourself, that you should look at products that have been on the market, that have received peer review, that have stood the test of time.

Mr. McLAUGHLIN. If I could add a comment?

Mr. GOODLATTE. Sure.

Mr. McLAUGHLIN. In short, the answer is, are products out there—the question is, are there products out there of foreign origin that have back doors in them? The answer is, yes. The next question is, do these products last more than 5 minutes in the marketplace; and the answer is, not a chance.

Cryptography, in particular, is a very, very interesting industry in that so-called “Cyberpunks” demand peer review. Because something is new and announced as being stronger and unbreakable does not drive droves of people to try it out; in fact, it drives droves of critics to argue with it and demand access to information so they can prove it. Nothing is considered secure unless it has been through extensive peer review.

The actual source that makes up the applications is available for review, and so, essentially, everyone who wants to can guarantee that there are no back doors in there.

Mr. GOODLATTE. Would each of you comment on the extent to which you are encountering foreign encryption products in the marketplace and losing prospective clients because your companies cannot export strong encryption?

Mr. McLAUGHLIN. Privada personally is experiencing a situation where we are in discussions with several foreign telephone companies and network service providers all from a—who—all of whom are very interested in our products, but regrettably have told us, and we have told them, this is good for nothing more than dialogue because we cannot ship a product to them.

Mr. MCCURDY. Mr. Chair, actually I inquired of some of our member companies—hardware companies—on the same point. In fact one very prominent industry representative indicated that they lost a recent government contract overseas not because of the technology—it is clear that the technology was superior. But the one aspect that they had no credibility on, that they could not prove, was the security aspect, because some of the limitations and the requirements of that government were much higher.

Again, it becomes an issue of credibility. It is not just what is in the hardware and what is in the software. There is a broader issue of, can you be trusted and are we limiting the ability of those to use the latest tools to protect them?

Mr. GOODLATTE. Mr. Parenty?

Mr. PARENTY. As sort of a corollary note, a government organization in India, just in the last month or so, actually issued a warning not to use any American encryption products because of the fear of back doors being put in for American intelligence use. There is sort of an entire market where because of the question of whether or not American companies were compromised, by our Government—just a wholesale rejection of an entire market.

Mr. BERMAN. It is too late to help this legislation?

Mr. PARENTY. Fortunately, India is not the entire world.

Mr. BERMAN. But that kind of thinking is contagious.

Mr. PARENTY. That is true. It is something where actually the comments from Alan Davidson are very important.

Mr. BERMAN. Let me ask just a couple—two questions. One of them is explain to me why it is in America's security interest for it to be American-made encryption software. We know we have a high interest in the security of the communications, and we know we have an interest from an economic and technological development point of view in America's dominance, and everything costs. It is the way we are. But why is it in our security interest that it be an American-produced software rather than Irish-produced software or a Canadian-produced software or one of the other countries? Why is that—in other words, in response to the chairman's question, why isn't it in our security interest?

Mr. PARENTY. In our security interest it actually goes to a comment which was just made before with respect to are there holes in foreign products to allow foreign companies to have access to them. It goes back to when I used to work with the Department of Defense, we were very concerned about building a defense sys-

tem based on products that were produced outside of this country because of the inherent unreliability of the source and the inability to know exactly what it was we were getting.

Mr. BERMAN. To the extent that that is true, and taking just what you said so far about that stuff last 5 minutes, and, by the way, here is what the Indians are saying, by definition then our present policies aren't going to destroy our dominance of the market because everybody is so focused on the holes or potential holes in other countries' software. In other words, why isn't it about whether the software has a hole in it and not whether it is made by an American or made by an Irish company?

Mr. MCCURDY. Well, Congressman, first of all, this country has been the primary beneficiary of the technological revolution in the world, and we have—sure, there is an issue of dominance. We no longer have the dominance.

Mr. BERMAN. I think it is real important in the broader sense of economic strength. The security interest point of view, that is what I thought you were asking about. There is a security interest in the DOD being able to send its message with American encryption rather than foreign encryption.

Mr. GOODLATIE. If I can jump in here. Wouldn't it be true that if you have a U.S.-made product that doesn't have such a hole in it, you don't want as an alternative a U.S. company dealing with its manufacturing plant and its engineering office sending communications back and forth using a Russian-made encryption product that does have a hole in it that results in industrial espionage taking place.

Ms. LOFGREN. Can I interrupt on this same point since we are talking about this now? I don't think anyone has mentioned this, and maybe you don't want to discuss it, which is okay, too, but there are different ways to break code. In public sessions usually the defense establishment will refer to just group force breaking, but there are more sophisticated ways to do that. There are angles that you can have on how to do that. If you are the author of the code, you have some ideas on angles to approach it that might not be available if you were not the author. You don't have a company, Mr. Davidson, so maybe you can answer that.

Mr. DAVIDSON. I think that is right from a consumer's point of view. There are a couple of answers to this question. The U.S. software dominates the market, especially the consumer market. We have a great interest in making sure that U.S. software has good encryption in it from the consumer's point of view.

The second is that I think this last comment gets to the point that U.S. consumers ought to be able to find U.S. products that we can trust. It probably doesn't just take 5 minutes for the marketplace to kick out flawed products. It may actually take a little while, because some of these things are very subtle from a consumer point of view. We should be looking for the U.S. Government to help us figure out what products to trust. Right now we can't because people don't trust the Government. Right now the consumers have a big problem.

What products do I trust? I have to listen to the Cyberpunks. Ultimately in the long run it is an open question of whether the

Cyberpunks should be where most consumers are going to look to see if they can trust things.

Mr. BERMAN. You talked about the availability of plaintext. Then I was sort of thinking just in the context of Monica's e-mails and other stories which go around about people being able—you have deleted from your computer the e-mails, but somehow they grab ahold of the computer, and they do something with some part of the computer that I am afraid to mention because I am sure I will be wrong that ends up revealing the message. By the way, is it revealing in the encrypted form or plaintext form?

Mr. DAVIDSON. It depends, but a lot of situations it probably is the plaintext form.

Mr. BERMAN. But it wouldn't have to be the plaintext. It could be—

Mr. DAVIDSON. If you stored it, encrypt it—

Mr. BERMAN. You decrypted to read it. You then deleted it, but you can't find it in its decrypted form.

Mr. McLAUGHLIN. The short answer is you might be able to. My background is in systems administration and security. I don't think you want me to get into the technical details of how it is possible, but in short, when you decrypt something for reading on your screen, that decrypted form is existing in the computer's memory. All modern computer operating systems have a function today, because they are running multiple tasks, to, at times transparent to you, put that memory onto the hard drive. In a well-designed system, that is—that memory is cleared off after the fact. It is, however, possible that your message, the component part of memory holding your message, is stored on the hard drive and thus visible even when you don't think it is.

Mr. BERMAN. But that does get a little bit back to the third point that the NSA had and that Professor Denning was commenting about, interoperability; things getting screwed up so that we can decrypt things that people think are being encrypted.

Mr. PARENTY. A nontechnical analogy for the instance with respect to e-mail you thought was deleted but is actually around is if imagine you have a book and you want to delete a chapter, you rip the page out of the table of contents. So it is hard for somebody just looking at the front of the book to know that it is there. However, with a little bit of energy, if you flip through, you find that the data is still there. Ollie North had the same problem with e-mail.

Mr. GOODLATTE. Anybody else?

Ms. LOFGREN. I think we have pretty thoroughly explored this, and I think you have been a terrific panel.

Mr. BERMAN. The computer hardware issue, part of this is decontrolling not encryption software, but some kind of computer—embedded—but you are decontrolling this. Your legislation will not allow a technology which is otherwise controlled to be decontrolled simply because it has embedded encryption technology.

Mr. GOODLATTE. No.

Mr. BERMAN. A supercomputer is not going to go simply because it has—

Mr. GOODLATTE. Exactly right, and it shouldn't, unless there is—

Ms. LOFGREN. It shouldn't, but we will want to argue that Pentium III is not a supercomputer.

Mr. MCCURDY. It is going to be a definitional issue. But supercomputers will probably be a category unto themselves at some point, and there will be an interesting debate on that issue.

Mr. GILLESPIE. In terms of—Congresswoman Lofgren mentioned a couple of things in terms of Ms. McNamara's point, and I was confused by that, too. I was interested to hear some of the answers, but this notion there was a subtle but significant shift in the Administration's posture this morning which was that they no longer argue availability and that they are trying to—what they are now saying is, oh, it is widely available, but no one is using it. And I think what we are seeing, and on terms of your rabbit also, it may not have to be mandatory key recovery. That may not be the technology, but you have to get something out there, and there is, as you said, no rabbit.

I think what you saw again this morning is that this is a policy in desperate search of rationale, and all of the things that have happened and been talked about here today demonstrated that the current policy has been rendered completely inadequate and ineffective.

Ms. LOFGREN. Along that point I think we have made progress because I think there has been an admission such as you said and we have actually discussed here. I think it is good to discuss what the real issue is, that the current policy will have the effect of slowing the movement into the mass market of easily used encryption. I think that is probably true. It has already happened. The question is for how much longer. None of us know the answer to that and at what price, and whether the price is worth it, because once that price is paid, if it is paid in terms of American dominance of this technology, that in the end will be a very high priced, indeed, not only economically, but also regarding our national security interest.

So that is really the question that faces us, and I suppose reasonable people can reach different conclusions, but that is, in fact, the issue, and I think it is good to have it out in the open.

Mr. GOODLATTE. It is. But I also think—I don't agree with the Administration's assessment that encryption isn't already being widely implemented in a whole host of different technologies. Hardware—

Ms. LOFGREN. Yes, it is, you are right.

Mr. GOODLATTE [continuing]. Software on the Internet, and wireless communications, and a whole host of consumer entertainment-type products, and in addition, it is on the verge of the kind of absolutely prolific use that she still seems to think she can hold back.

Ms. LOFGREN. If I may, Mr. Goodlatte, I agree with you, which is why I am cosponsoring the bill with you—

Mr. GOODLATTE. Finally figured that one out.

Ms. LOFGREN. Finally figured that one out, but I guess the issue is to the extent that there are, as I said this morning, maybe the dumb criminals aren't encrypting their messages, but certainly the smart ones are.

Mr. GOODLATTE. That is right. Without key recovery.

I would like to thank these witnesses for their testimony. The subcommittee appreciates your contribution very much. This has been a very helpful hearing. This concludes the legislative hearing on H.R. 850, the Security and Freedom through Encryption Act, and the record will remain open for 1 week.

I thank you all for your cooperation and participation, and the subcommittee stands adjourned.

[Whereupon, at 1:55 p.m., the subcommittee was adjourned.]



.

•

Document No. 31

