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 11:23:04 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.

ENCRYPTION SECURITY IN A HIGH TECH ERA

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTERNATIONAL ECONOMIC POLICY AND TRADE

OF THE

COMMITTEE ON
INTERNATIONAL RELATIONS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

TUESDAY, MAY 18, 1999

Serial No. 106–108

Printed for the use of the Committee on International Relations



Available via the World Wide Web: http://www.house.gov/international relations

---

U.S. GOVERNMENT PRINTING OFFICE
64–674 CC WASHINGTON : 2000

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

ISBN 0-16-060699-3

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

COMMITTEE ON INTERNATIONAL RELATIONS

BENJAMIN A. GILMAN, New York, *Chairman*

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVEN J. CHABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JOHN M. McHUGH, New York
KEVIN BRADY, Texas
RICHARD BURR, North Carolina
PAUL E. GILLMOR, Ohio
GEORGE RADAVANOVICH, Califorina
JOHN COOKSEY, Louisiana
THOMAS G. TANCREDO, Colorado

SAM GEJDENSON, Connecticut
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
MATTHEW G. MARTINEZ, California
DONALD M. PAYNE, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. McKINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
JIM DAVIS, Florida
EARL POMEROY, North Dakota
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

RICHARD J. GARON, *Chief of Staff*
KATHLEEN BERTELSEN MOAZED, *Democratic Chief of Staff*

SUBCOMMITTEE ON INTERNATIONAL ECONOMIC POLICY AND TRADE

ILEANA ROS-LEHTINEN, Florida, *Chairwoman*

DONALD A. MANZULLO, Illinois
STEVEN J. CHABOT, Ohio
KEVIN BRADY, Texas
GEORGE RADANOVICH, California
JOHN COOKSEY, Louisiana
DOUG BEREUTER, Nebraska
DANA ROHRABACHER, California
TOM CAMPBELL, California
RICHARD BURR, North Carolina

ROBERT MENENDEZ, New Jersey
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
STEVEN R. ROTHMAN, New Jersey
WILLIAM D. DELAHUNT, Massachusetts
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

MAURICIO TAMARGO, *Subcommittee Staff Director*
JODI CHRISTIANSEN, *Democratic Professional Staff Member*
YLEEM POBLETE, *Professional Staff Member*
CAMILLA RUIZ, *Staff Associate*

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) ii 2002

CONTENTS

WITNESSES

	Page
William Reinsch, Under Secretary of Commerce, Bureau of Export Administration	9
Barbara McNamara, Deputy Director, National Security Agency	11
Ron Lee, Assistant Attorney General, National Security, Department of Justice	13
Gene Voegtlin, Esq., Legislative Counsel, International Association of Chiefs of Police	15
Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation	41
Jeffrey Smith, General Counsel, Americans for Computer Privacy	43
David Weiss, Vice President of Product Marketing, CITRIX Corporation	44
Alan Davidson, Staff Counsel, Center for Democracy and Technology	45
Dinah Pokempner, Deputy General Counsel, Human Rights Watch	47
Ed Black, President and CEO, Computer and Communications Industry Association	48

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) iii 2002

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) iv 2002

ENCRYPTION SECURITY IN A HIGH TECH ERA

Tuesday, May 18, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTERNATIONAL ECONOMIC
POLICY AND TRADE,
Committee on International Relations,

WASHINGTON, D.C.

The Subcommittee met, pursuant to notice at 2:15 p.m., in room 2172, Rayburn House Office Building, Hon. Ileana Ros-Lehtinen [Chairwoman of the Subcommittee] presiding.

Ms. ROS-LEHTINEN. [presiding] The Subcommittee will come to order.

I apologize for arriving late. I had to give a brief remark on a luncheon that Congressman Menendez, Mr. Gilman, and I are hosting for Cuban political prisoners tomorrow. So I hope that all of you could join us in room 2200 at 1 p.m. So I was speaking on the Floor and I was unavoidably delayed. Thank you so much for your patience and I apologize especially to my Ranking Member.

Someone once said I used to think that cyberspace was 50 years away. What I thought was 50 years away was only 10 years away. What I thought was 10 years away, it was already here, I just wasn't aware of it yet. This applies to the debate today on encryption where it seems our policy is trying to play a game of catch up with our technological advancements.

The Internet has rapidly expanded as a form in which to conduct business transactions, and millions of messages are transferred in a matter of seconds across oceans and continents, over barriers of languages and culture. Information that used to take hours to transfer can now be sent in a matter of seconds. Contracts are completed in minutes. Mergers in what seems instantaneously. In an increasingly diverse and globalized marketplace, the availability and efficiency of electronic businesses is becoming more appealing for companies hoping to keep a competitive advantage in international trade, maintaining their dominance in or seeking to capture the market of brain-power industries.

As these types of information transfers become more common, fear has emerged about their security and about the interception of messages and transactions by those who seek to steal or sabotage. Technology to prevent these types of invasions and violations of personal, corporate, and government security by encoding digital information already exists. It is what we call encryption. A need for commercial encryption rapidly developed with the growth of the global economy and, with it, so did concerns over exporting this technology to our overseas counterparts. The business community,

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

the Administration, and law enforcement entities have been at odds as to how to best promote American technological products abroad while ensuring that our security, both national and economic, are not threatened by the export of American-designed encryption products.

The Administration has stated its concerns about possible threats to U.S. national security and to public safety, which they feel would arise if criminals and terrorists were to use encryption that the U.S. Government could not penetrate. They fear that if there were no export controls on encryption and no key recovery features on the products we sell in overseas markets, it would further complicate and impede law enforcement efforts at tracking down terrorists or other criminals who use computers in their efforts to promote violent terrorist acts or who commit economic sabotage.

Opponents of the Administration's view argue that export controls cannot prevent access to strong non key recovery encryption by criminals because it is widely available elsewhere, including over the Internet where it can be easily downloaded from foreign company sites. They add that the one thing these controls are ensuring is U.S. companies losing market shares to foreign competitors. Currently, there are no statutory restrictions on the domestic use of encryption, but the industry argues that restrictive export controls have hampered technological development and will continue to thwart U.S. efforts until American companies will lose their current technological dominance. There is a need for strong encryption for domestic use and cross-border communications and transactions.

While the Administration argues that it has continued to promote stronger encryption products of greater than 56 bits, it has done so under the condition that these be designed with key recovery features where a third-party would have access to a key to decrypt the information. Further, the Administration's decision to liberalize exports for certain industries ignores the security needs of other sectors left unprotected by current restrictions.

Privacy advocates contend that the Administration has been utilizing the export control process to influence whether companies developed key recovery encryption products by facilitating the exportation of these products and making it more difficult to export unrecoverable encryption products. They further state that the national security arguments fail any test of logic that strong encryption serves as a deterrent to criminal activity by making it difficult for those who engage in espionage to penetrate the system.

Aside from the fact that all parties agree about the important role of encryption in electronic commerce, little consensus has been reached on the issue of export controls. The SAFE Act is one of the several legislative attempts at codifying existing domestic use policy and at liberalizing U.S. export control regulations to compete successfully in the global arena. This will be one of the issues we hope to cover today as we attempt to debate the future of encryption and the effects of controls on our technological market.

I would like to recognize our Ranking Member, Mr. Menendez of New Jersey for his opening statement. Mr. Menendez.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

Mr. MENENDEZ. Thank you, Madam Chair Lady, and I am happy to see that we are having this hearing which I think is an incredibly important one the Committee has jurisdiction over, and one that I think is going to be a part of making sure, along with the Export Administration Act and a few other issues that this Committee has jurisdiction in, that continues to fuel America's competitiveness in the future. The decisions that we make are going to affect American industry and American competitiveness in this new millennium.

Now anyone who has been on the Internet and purchased a book from Amazon.com or ordered an airline ticket online is familiar with encryption technology. In the information age, encryption technology is like a Wells Fargo truck. It keeps your information under lock and key and delivers it only to its intended end-user. Encryption technology is crucial to the development of electronic commerce, which is growing by leaps and bounds. According to Under Secretary Reinsch's testimony, electronic commerce transactions in 1996 were $12 million, but are projected to reach $2.1 billion by the year 2000.

So I think we need to be clear, from the very outset, that the encryption debate is not about who does and who does not support our national security interests. None of us who support moving encryption technology forward believe that we would do anything to risk the national security of the United States. I do not care for those who would suggest that, in fact, we do. No one is advocating a policy that would intentionally compromise U.S. national security or the safety of American citizens. The encryption debate is more about whether or not it is too late for the U.S. Government and law enforcement to control the spread of non key recovery encryption products in the U.S. and abroad.

Clearly, we should consider the value of controlling only the strongest encryption technologies. However, the value of controlling anything over 56-bit technology when 128-bit technology can be downloaded from the Internet, is questionable. American industry is rightly concerned about losing market shares to foreign competitors who have no restrictions on their products. We can be certain that if the United States cannot offer non key recovery encryption technology overseas, that consumers will buy it from the French, Japanese, and Israeli companies who are making similar products. Or from American companies who establish companies overseas, produce the intellectual property there, and that ultimately means job losses here at home as well as revenue losses here at home.

Now the goal of the FBI, NSA, and law enforcement agencies is well-founded. The key recovery system would ensure that they have access to the requisite data to snag criminals or track suspected criminal activities. Yet the proliferation of non key recovery technology within the United States and abroad and the rapid speed at which this industry is developing leads me to believe that the Administration's policy is too little, too late.

I look forward to hearing the testimony of our witnesses, in particular, the representatives from the FBI and NSA. I would very much like to hear your views on current policy and your concerns with the Goodlatte legislation. I will do so with an open mind, but

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

I believe we cannot turn back the clock as we move forward into a new millennium. Thank you, Madam Chairwoman.

Ms. ROS-LEHTINEN. Thank you so much. Mr. Menendez. We are thrilled to have the Chairman of our Committee, Congressman Ben Gilman of New York, join us. It shows the high level of importance that he gives to this issue of encryption. Welcome, Mr. Gilman.

Mr. GILMAN. Thank you, Madam chairman. I want to thank you for arranging this hearing with these experts who are all prepared to testify before us today. You certainly have a good cross-section of views assembled. I welcome this opportunity to attend this very important hearing on security in the high-tech era and on the Security and Freedom through Encryption Act, the SAFE Act, H.R. 850, sponsored by the gentleman from Virginia, Mr. Goodlatte, and the gentle lady from California, Ms. Lofgren.

I am pleased that the witnesses before us today come from a broad cross-section of the law enforcement community, export control and intelligence agencies, human rights and privacy advocates, and the private sector representatives. I would like to compliment you, Madam Chair, for your holding this hearing at this time and taking a leading role on this vitally important issue.

I would like to remind my colleagues that on Thursday of this week at 9 a.m., the Chairman of the Intelligence Committee, Mr. Porter, and I will be co-hosting a members-only classified briefing on the implications of decontrolling the export of encryption products. I urge our colleagues on this Committee to attend if they would like to have a full perspective on the national security and intelligence aspects of the encryption issue.

In my view, before we begin the process of making sweeping changes in our export control laws, Congress should avail itself of all the information we can obtain in all venues available to us. With the United States participating in a NATO-led military operation against Serbia, we should be doubly cautious in this respect because of the possibility of terrorist attacks on our interests. I am very concerned that the enactment of a SAFE Act would make strong encryption all the more available to our adversaries and would undermine international efforts to modernize and improve multilateral export controls under the Wassenaar arrangement.

I draw the attention of the Subcommittee Members to the recent statement of the International Association of the Chiefs of Police. "Unchecked proliferation of encryption technology poses an enormous danger to both law enforcement and to society as a whole." In a May 12th letter that we received from B'nai Brith International, its president Richard Heideman noted that—and I quote—"Unlimited proliferation of nonrecoverable encryption products may result in their use by terrorist groups, by narcotics traffickers, by members of organized crime, and other dangerous criminals to the detriment of our Nation's national security and public safety." Mr. Heideman concluded that his organization has strong reservations about the Security and Freedom through Encryption Act and urges that Congress maintain meaningful export safeguards.

Unlimited proliferation of this technology only makes the street-corner drug dealer further immune from the consequences of his and others' actions. The drug trade costs us billions each year in

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

crime, in health care costs, lost worker productivity, destroyed families, and lost young lives. Let us not contribute to that carnage under the guise of greater trade and commerce.

For those who say that this encryption technology is already readily available abroad, they often fail to remind you that foreign governments, in most cases, have also retained the right to access in protection of their national security interests. Those governments are not naive, nor should we be. While we are still waiting for the final version of the Cox report on high-tech exports to China, many of their recommendations are already public. Among them are concrete suggestions on how to strengthen the successor regime of the Cold War COCOM export system. Its modern-day equivalent, the so-called Wassenaar arrangement has just agreed to modernize our multilateral encryption export control system, yet the enactment of the SAFE Act would undercut that arrangement and the findings of the Cox report.

Accordingly, I urge my colleagues not to rush to judgment on an issue such as this which directly affects our national security and our law enforcement needs. I thank the gentle lady for recognizing me.

Ms. ROS-LEHTINEN. Thank you so much, Chairman Gilman. Mr. Delahunt.

Mr. DELAHUNT. I thank you, Madam. I just would welcome my colleague from the Judiciary Committee and acknowledge the presence of Mr. Goodlatte, one of the primary sponsors. I want to personally welcome him.

Ms. ROS-LEHTINEN. Thank you, Mr. Delahunt. Mr. Bereuter.

Mr. BEREUTER. Madam Chairman, it is an important hearing today. I have been following this issue for quite some period of time now. I agree with many of the comments made by Chairman Gilman. We do need to be concerned about the implications for law enforcement and national security and a lot of the best information we have in the way of documentation of its importance is classified. On the other hand, we need to make sure that we do in the way we control things does not have an unnecessary anti-competitive factor which is brought to bear. So I will say nothing further, but look forward to the testimony of two large and important groups of panelists.

Ms. ROS-LEHTINEN. Thank you, Doug. The sponsor of the bill, Mr. Goodlatte. We are honored to have you with us today.

Mr. GOODLATTE. Madam Chairman, first let me thank you for holding this hearing and for being very gracious in allowing me, a non-Member of the Committee, to participate. I would also like to thank the Ranking Member, Mr. Menendez, and Chairman Gilman for their participation in this and for allowing me to participate as well.

I do have a statement that I would ask to be made a part of the record.

Ms. ROS-LEHTINEN. Without objection.

[The information referred to appears in the appendix.]

Mr. GOODLATTE. I also have an article written by Congressman Chris Cox, the Chairman of the Cox Commission, who advocates a strong export policy with regard to exporting encryption, making it more available, entitled "China: Export of Technology Would be

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

Liberating Force," in which he advocates the export of strong encryption.

Madam Chairman, this much-needed bipartisan legislation currently has 253 cosponsors, about 110 Democrats, about 140 Republicans; a majority of the Republican and Democratic leadership in the House are cosponsors as are two-thirds of the Members of the International Relations Committee and all but 4 Members of this Subcommittee, and it accomplishes several important goals. First and foremost, strong encryption in the hands of the good guys, if you will, helps to prevent a number of the concerns that have been raised by some of the Members of the Committee, which are legitimate concerns by law enforcement and national security, but making sure that we have strong encryption to protect e-mail, medical records, financial transactions, copyrighted material, industrial trade secrets, and a whole host of other areas, as well as preventing major terrorist and criminal activities such as breaking into the New York Stock Exchange or the Chicago Board of Trade or a nuclear power plant or the electric power grid of the United States are all very positive purposes that are hindered by a policy that discourages the use of strong encryption and which is the policy that we have today.

The gentleman from New Jersey mentioned the use of encryption by companies like Amazon.com and others who do business on the Internet. Amazon.com cannot use the 128-bit strong encryption that they use for domestic sales internationally, unless they acquire it from a foreign vendor. This, to me, seems to be a ludicrous consequence of the policy that we currently confront in this country.

I'll give you another personal experience that I came across recently when I led a congressional delegation to Europe to deal with electronic commerce issues. In Brussels, in meeting with the deputy chief of the U.S. mission there, he indicated to me that he has worked with the National Security Agency and the FBI and other agencies on a regular basis on issues like this. But his own personal experience colored his view of the need for significant change in our export control laws when he told me that he bought a $2,000 computer system which was shipped to him from the United States and he then received a phone call from the company that sold it to him telling him they could not send him the software because it violated American export control laws. So he went down the street to a little shop in Brussels and purchased the software that he needed there.

Today there are more than 20 significant strong companies in Europe creating encryption software that are major competitors to the United States that did not exist just a few years ago. What we are confronted with is a circumstance in which we are already beginning to see significant erosion in the U.S. dominance of the software and hardware computer industry because of the fact that most major software and hardware today has strong encryption built into it, and if you can't export it out of the United States, you are better off dealing with a company overseas because if you are, for example, a company with branches in London. Paris, Tokyo, New York, and San Francisco, you can buy these products domestically—there is no limitation on the domestic use of strong

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

encryption—and use them in your New York and San Francisco offices, but you can't send them to your London, Paris, and Tokyo office.

However, if you buy it from a German company, to use an example, there are no import restrictions on strong encryption. So you can import the German products, use it at your New York and San Francisco offices and also send it to your London, Paris, and Tokyo offices. This is the crux of the problem that we have in not facing up to the fact that encryption is not like other items that are strongly suitable for export controls.

Bombs, jets, mainframe computers are all products that are manufactured in a few places, sent to a few places, and the export of the products from this country can be a choke hold on making sure they don't go to inappropriate places. But encryption is not a tangible thing. It is a mathematical algorithm. It is little ones and zeros going through fiber-optic wires and by satellite all over the world. So it is my hope that we will be able to move forward with this legislation, which will help to create and protect American jobs, which will help to fight crime in a whole host of ways, and which will protect the privacy of law-abiding American citizens and I very much thank you for the opportunity to participate today.

Ms. ROS-LEHTINEN. Thank you so much, Bob. Congressman Burr.

Mr. BURR. Thank you, Madam Chairman. Let me just say that, my good friend Mr. Goodlatte, I had hoped that after we dispensed with this in Commerce last year that law enforcement and the technology businesses would find the agreement that could move forward together. Unfortunately, I don't have the impression that we are there. That as you talked about the inability to export software, I think a year from now, with the new chips, we will, in fact, find ourselves not exporting the computer. I think we have some bigger problems to deal with.

I would suggest today to my colleagues that the way to find the answer is not to dig our heels in the sand and say we can't move from where we are. In fact, the challenge to each of us is to find where that balance is, to move there, and not to find new ways to drive technology offshore where, for a short-term gain, we do significant long-term damage to not only the development of business in this country and the creation of jobs, but to our national security which is an area that we are all sensitive to.

Technology has few boundaries, as my good friend Mr. Goodlatte referred to, and our ability to understand technology's flow around the world is, in fact, a significant key to our understanding of where we move with legislation. Madam chairman, I am only hopeful that all Members will encourage not only the business sector, but the law enforcement sector to work a little bit harder to try to find a compromise, one that facilitates the business needs of the future, the development of technology, and also provides some assurances of law enforcement's access. Clearly, if technology is that advanced in intelligence, I am hopeful that somebody will transmit an updated map to our intelligence agencies. Maybe we won't have quite the problem that we have had over the past week.

Technology is a tremendous tool. It is a tremendous tool for every person in the world. It will become more the tool for opening up not only closed markets, but closed societies in the future. We have

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

to find a way to make this work, to make it work for all who have a concern and to utilize this tool to its fullest. I am confident that this hearing and many others that we will have this session of Congress will help us to get to that legislation. I thank the Chair and I yield back.

Ms. ROS-LEHTINEN. Thank you. Mr. Radanovich.

Mr. RADANOVICH. Thank you, Madam Chair, I will be brief. I would like to submit a statement for the record.

Ms. ROS-LEHTINEN. Without objection.

[The information referred to appears in the appendix.]

Mr. RADANOVICH. Thank you. But do want to state my wish that we get a bill forward sometime this session that would open up markets for U.S. business and, at the same time, preserve our security. I appreciate the chairwoman for having this hearing and hopefully we can move this issue forward and get it dealt with. Thank you very much.

Ms. ROS-LEHTINEN. Thank you so much. Mr. Rohrabacher.

Mr. ROHRABACHER. I would just like to say that Mr. Goodlatte has put a lot of effort into this and is a very patriotic American and where we have had our disagreements in the past, I think that he is using good judgment here and I am very happy to be a cosponsor of this bill.

Ms. ROS-LEHTINEN. Thank you. Thank you so much for your patience, all of you in the audience and our panelists as well. We will first hear from Bill Reinsch, who currently serves as the under secretary for export Administration in the Department of Commerce. As head of this bureau, Mr. Reinsch is charged with administering and enforcing the export control policies of the U.S. Government. Before joining the Department of Commerce, he served on the staffs of several Members of Congress who are extensively involved with international trade issues. He has testified before this Subcommittee many times and we are glad to have you back, Bill. Thank you.

Next will be Barbara McNamara, who is Deputy Director of the National Security Agency. From 1995 to 1997, Ms. McNamara served as the Deputy Director of operations, National Security Agency of the Central Security Service. Prior to that, she served as the NSA representative to the Department of Defense, as well as chief of the Office of International Economics and Global Issues in the Operations Organization. Ms. McNamara began her career in the National Security Agency as a linguist and served in a variety of analytical and management positions in the Operations Office. Thank you so much for being with us.

Ronald Lee is the associate deputy attorney general for the Department of Justice. He is currently the Acting Director of the Executive Office of National Security at the Department. He has served as the program manager for the development of the Administration's 5-year counter terrorism and technology crime plan. In 1994, Mr. Lee was appointed as general counsel of the National Security and served as their chief legal officer representing the NSA in all legal matters. Welcome, Mr. Lee, to our panel.

We also have a representative from the International Association of Chiefs of Police, who is pro-export controls, but he does not represent the Administration. Mr. Gene Voegtlin is the legislative

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

counsel of the International Association of Chiefs of Police. In this position, he is responsible for directing the day-to-day implementation of the Association's government affairs program. Prior to joining the Association, Mr. Voegtlin served as the Director of legislative and political affairs for the National Federation of Federal Employees. His prior experience also includes serving as a legislative representative of the Federal Managers Association and the American Chemical Society. We welcome you, Mr. Voegtlin, today.

We will begin with the Honorable Mr. Reinsch. Thank you, Bill.

STATEMENT OF WILLIAM REINSCH, UNDER SECRETARY OF COMMERCE, BUREAU OF EXPORT ADMINISTRATION

Mr. REINSCH. Thank you very much, Madam chairman. It is a pleasure to be here with you again to testify on the direction of the Administration's encryption policy. I would appreciate, Madam chairman, if you would put my full statement in the record.

Ms. ROS-LEHTINEN. Correct. Without objection, we will glad to put all of your statements into the record.

Mr. REINSCH. Thank you. Notwithstanding the comments of some of your colleagues, Madam Chairman, I think we have made a great deal of progress in this area since the last time I was here. But it is still, nevertheless, obvious that 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 policy that provides that balance in a way that also reflects the evolving realities of the marketplace. The Internet and other digital media are becoming increasingly important to the conduct of international business. Mr. Menendez used one of my better statistics and so I think I will skip over the other ones in my statements and you can read them. But I think there is no disagreement over that point, in any event.

Clearly, many service industries, which traditionally required face-to-face interaction, such as banks, other financial institutions, and retail merchants, are now providing cyberservice. 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 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 digital communications, transactions, and networks.

Developing a new policy in this area has been complicated because we do not want to hinder encryption's 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. During the past 3 years, we have learned that there are many ways to assist in lawful access. There is no one-size-fits-all solution. On September 22nd of last year, we published a regulation implementing our decision to allow the export under

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 9 2002

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 which have effective anti-money laundering laws.

The further result of our ongoing dialogue with industry was an update to our encryption policy which the Vice President unveiled last September 16th. 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 update reduced controls on exports of 56-bit products and, for certain industry sectors, on exports of products of unlimited bit length, whether or not they contain recovery features.

In developing our policy, we identified key sectors that can form the basis of a secure infrastructure for communicating and storing information: banks, a broad range of financial institutions, insurance companies, online merchants, and health facilities. Many of the updates permit the export of encryption to these end-users under a license exception. The policy also allows for exports of 56-bit software and most hardware 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; and approval under a licensing arrangement of recovery-capable or recoverable encryption products of any key length to recipients located in 46 countries. Such products include systems that are managed by a network or corporate security administrator.

In December, through the hard work of Ambassador David Aaron, the President's special envoy on encryption, the Wassenaar arrangement's members agreed on several changes related to encryption controls. Specific changes to multilateral encryption controls included removing them on all encryption products at or below 56-bits and on certain consumer items regardless of key length.

Most importantly—and I want to take a moment on this, Madam chairman—the Wassenaar members agreed to remove encryption software from Wassenaar's general software note and replace it with a new cryptography note. Drafted in 1991 when banks, governments, and militaries were the primary users of encryption, the general software note allowed countries to permit the export of mass-market encryption software without restriction. The GSN was created to release general purpose software used on personal computers, but it inadvertently encouraged some signatory countries to permit the unrestricted export of encryption software. It was essential to modernize the general software note and close a 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-key length or below has been set as an appropriate threshold. This will result in government review of the dissemination of mass-market software of up to 64-bits. 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 as does the policy of most

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 10 2002

other Wassenaar members. It does mean, however, that such exports must be reviewed by governments consistent with their national export control procedures.

Finally, Madam chairman, 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 want to reiterate that this Administration does not seek 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 provisions contained in the bill.

Second, once again, we must take exception to the bill's export provisions. In particular, the references to IEEPA, as I understand them, might have the effect of precluding 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.

The Administration does not seek encryption export control legislation nor do we believe such legislation is needed. The current regulatory structure provides for balanced oversight of export controls and the flexibility needed so that it can continue to promote our economic foreign policy and national security interests while adjusting to advances in technology. We believe this is the best approach to an encryption policy that promotes secure electronic commerce, maintains U.S. leads in information technology, protects privacy, and protects public safety and national security interests.

Thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much.

Ms. McNamara.

STATEMENT OF BARBARA MCNAMARA, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Ms. MCNAMARA. Good afternoon, Madam Chair. Thank you for 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 de-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 11 2002

rived from foreign signals to a variety of users in the Federal Government. It is the signal's intelligence role that I want to address today. NSA intercepts and analyzes the communications signals of foreign adversaries to produce critically unique and actionable intelligence reports 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 provides the same kind of intelligence support today in the former Yugoslavia and other locations around the world wherever 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 national security areas of terrorism, weapons proliferation, and narcotics trafficking. Today, many of the world's communications are still unencrypted. Historically, encryption has been used primarily by governments and the military. It was employed for confidentiality and hardware-based systems and was often difficult to use. As encryption moves to software-based implementations and the infrastructure—and I underline 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. As a result, much of the crucial information we are able to provide today could quickly become unavailable to the decisionmaker.

As you will hear from my colleague from the Department of Justice, it is important to understand that the needs of national security and the needs of law enforcement are different and must be addressed separately. At NSA, we are focused on preserving export controls on encryption to protect national security. As you consider the SAFE Act, it is very important to 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. 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. This bill would also deprive us of the opportunity to conduct a meaningful review of a proposed encryption export. 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.

The SAFE Act would permit exports of encryption based on products comparable to those being exported for foreign financial institutions. But using the special treatment afforded banks and financial institutions which are well-regulated and have a good record

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 12 2002

of providing access to lawful requests for information, 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. The criteria for exporting encryption to these institutions should not be the basis for decontrolling other encryption exports.

The SAFE Act also eliminates control for computer hardware with encryption capability if it is found that the product is available in the overseas market. The apparent availability of a product in a country without regard to its actual performance capabilities or without restrictions on end-users or end-uses will have the practical effect of forcing the decontrol of such exports, a condition that is unacceptable to national security.

We believe that 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. You will hear from others that industry is prohibited from exporting anything greater than 56 bits. That is patently wrong. Last year's update allows vendors to export unlimited-strength encryption, even 128 bits, to specified market sectors in a set of countries that represents approximately 70 percent of the world's economies or did at the time and that redresses the issue of Amazon.com that Congressman Goodlatte referred to.

This is an example 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 that 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 that allows U.S. industry to continue to be the world's leader, but that also protects the security of our Nation. Thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much.

Mr. Lee.

STATEMENT OF RON LEE, ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY, DEPARTMENT OF JUSTICE

Mr. LEE. Madam Chair, I would like to emphasize some of the points in my written statement for the Subcommittee in my brief remarks this afternoon. I would like to be clear, because the views of the Department of Justice on encryption and export controls are often caricatured or misrepresented.

The Department of Justice supports the spread of strong recoverable encryption to protect the privacy of American citizens and to protect the security of our information infrastructure. This is not, after all, a debate about whether the U.S. national interest is served by the success of U.S. companies abroad. We fully accept

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 13 2002

and support that premise. We are, however, deeply concerned about the threat to public safety posed by the widespread distribution and use of nonrecoverable encryption. Law enforcement agencies, both in the United States and abroad—and we work closely with many law enforcement agencies abroad—have already begun to see cases where encryption has been used in efforts to conceal criminal activity. The number and complexity of these cases will certainly increase as encryption proliferates and, I emphasize, as encryption increasingly becomes an integral part of mass-market software items and network-based information services.

Thus, we cannot just extrapolate from past examples where encryption has posed a problem. We must, as a government, in partnership with the Congress, take this moment to realize that encryption is becoming a part of our commerce and make responsible public choices.

Faced with the use of nonrecoverable encryption, agents would not be able to make effective use of search warrants. wiretap orders, and other legal processes that have been authorized by Congress and ordered by the courts. These tools are absolutely essential to effective law enforcement investigations today. Without these tools, law enforcement would find it increasingly difficult, if not impossible, to obtain important evidence of criminal activity and to gather and develop and present the evidence needed in criminal prosecutions.

In the face of these challenges, the Department of Justice supports the carefully balanced approach to export controls that the Administration is actively pursuing. The Chair asked about progress in the last year. I would like to report that the Attorney General, along with the Director of the Federal Bureau of Investigation and other government officials have been actively engaging industry leaders in a continuing, cooperative, and positive dialogue. This dialogue has continued throughout the Department and the FBI at several different levels.

We have gained a lot from the dialogue. We have both explained the public safety concerns that we have from the spread of nonrecoverable encryption and we have learned about innovative solutions that industry has presented. It was in part this collaboration and dialogue that led us to be able to participate in the active report in the export control updates announced by the Administration last September. We thank the Members of Congress who have helped to facilitate this dialogue and we will work hard to make sure that these discussions continue. We believe that the current balanced approach is the most conducive approach to continuing this open dialogue with industry.

In this connection, the rapid elimination of export controls, as proposed in H.R. 850, the Security And Freedom through Encryption Act, would upset this balance dramatically. We believe that passage of the SAFE Act would cause the further spread of unbreakable encryption products that will be used by terrorist organizations and others for criminal purposes.

Of course, we recognize that law enforcement is already coming across nonrecoverable encryption by criminals. We are not standing still. In order to protect public safety, we are continuing to develop our own technical expertise. The Department of Justice has begun

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 14 2002

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 posed by unbreakable encryption when used by criminals.

We look forward to working with Congress to develop this resource. However, I must emphasize that no technology, no set of technologies, no tool box offers a silver bullet. The widespread use of nonrecoverable encryption by criminals would quickly overwhelm whatever technical response and capabilities we could develop. In summary, we believe that the Administration's approach balances the need for secure private communications and electronic commerce with the equally important need to protect the safety of the public against threats from terrorists and criminals. We look forward to working with you on this important issue. Thank you.

Ms. ROS-LEHTINEN. Thank you so much.

Mr. Voegtlin.

STATEMENT OF GENE VOEGTLIN, ESQ., LEGISLATIVE COUNSEL, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Mr. VOEGTLIN. Thank you. Good afternoon, Madam Chair, Chairman Gilman, and Members of the Subcommittee. I am pleased to be here today on behalf of the International Association of Chiefs of Police. Our president, Ronald Neubauer, had hoped to be here today, but, unfortunately, he is out of the country and therefore cannot attend.

I would like to briefly tell you about the IACP and then summarize our statement. Founded in 1893, the IACP, with 17,000 members in 112 countries, is the world's oldest and largest association of law enforcement executives. Our mission throughout the history of the association has been to identify, address, and work to provide solutions to urgent law enforcement issues. As I appear before you today, it is clear that robust, nonrecoverable encryption technology and the threat it poses to the ability of law enforcement agencies to perform their mission looms as one of the most urgent and important issues facing our members in the communities they serve.

The IACP's position on the encryption issue is clear. We strongly believe that the unchecked proliferation of robust nonrecoverable encryption technology poses an enormous danger to effective law enforcement, public safety, and to society as a whole. Therefore, the IACP believes that any encryption legislation that is enacted must protect the ability of law enforcement agencies to perform court-authorized electronic surveillance and the search and seizure of criminally related information stored in computers.

In addition, the IACP believes that it is of vital importance to maintain the stringent export controls on robust nonrecoverable encryption products. The relaxation of export controls would likely result in the widespread proliferation of unbreakable encryption products which would severely limit if not completely destroy the ability of law enforcement agencies to effectively investigate and apprehend international terrorists and criminals. This is why the IACP was pleased last December when 33 nations signed on to the

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 15 2002

Wassenaar export control agreement to impose or expand existing controls on encryption and other data scrambling technologies.

I would like to note, however, that the IACP's position on the need for law enforcement access does not mean that we oppose all uses of encryption technology. The IACP certainly recognizes that there is a legitimate need to use encryption products as a tool to protect electronic commerce and individual privacy. Indeed, law enforcement agencies themselves have a need for secure communications and information storage. Nevertheless, we must balance these legitimate concerns with the threat we face by providing criminals, drug lords, and terrorists with an impenetrable means of communicating to their criminal associates.

In addition, the IACP is aware of the economic issues involved in the manufacture and sale of encryption technology and products. However, we believe that we must consider the enormous economic damage that is being done to the United States economy as a result of crime and related consequences. For example, experts have estimated that the economic loss to the United States as a result of drug-related crime, accidents, medical care, and the loss of productivity reaches upward to $50 billion a year.

Finally, I would like to stress that providing law enforcement with a means to access the plain text of encrypted information would not represent an expansion of the police power to conduct searches or infringement on the Fourth Amendment protections against unreasonable searches. Law enforcement agencies would still be required to follow the current procedures that are necessary to gain access to other information that is used in the commission of crime. Providing for law enforcement access is entirely consistent with the constitutional safeguards of the Fourth Amendment.

What we would be doing by ensuring that law enforcement can access the plain text of encrypted criminal information is simply modernizing our current search warrant laws to keep pace with advances in computer technology. It is imperative that Congress take immediate steps to protect the capabilities of law enforcement. Electronic surveillance and wiretaps are two of the most effective tools in law enforcement's arsenal. Over the years, numerous arrests, prosecutions, and convictions have been secured against criminals because of court-authorized surveillance and wiretaps operations.

It is our belief that if Congress allows a robust encryption technology to be sold without providing for a means of law enforcement plain text access, it would effectively be stripping law enforcement agencies of their ability to successfully perform electronic surveillance, wiretaps, and the search and seizure of criminal information stored in computers. Therefore, before any legislation is enacted, the IACP urges Congress to ensure that it contain provisions that would provide law enforcement with immediate and complete plain text access to information encrypted in the furtherance of criminal activity. The inclusion of such provisions are absolutely vital if we are to preserve the investigative capabilities of our Nation's law enforcement agencies.

If Congress fails to provide law enforcement with this necessary access, law enforcement agencies will be further behind the technology curve. Terrorists, drug lords, and other criminal elements

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 16 2002

will have the upper hand over law enforcement and, as a result, the personal safety and security of all Americans and their property will be endangered. Thank you.

Ms. ROS-LEHTINEN. Thank you so much to all of our panelists and we are proud to begin our series of questions by our Chairman of the International Relations Committee, Mr. Gilman.

Mr. GILMAN. Mr. Lee, how many major organized crimes cases have made without court-authorized wiretap evidence? Can you give us a rough estimate?

Mr. LEE. Chairman Gilman, each major organized crime case, like any other investigation of a major crime, is done with a combination of law enforcement investigative tools. Law enforcement brings to bear the entire set of tools to investigate, apprehend, and prosecute these criminals. In each of these investigations, court-authorized wiretap operations and the evidence derived from them are absolutely essential to the success of the enterprise. By that I would mean both the successful investigation of the organized crime matter and also the successful prosecution and marshalling of evidence against the defendants.

Mr. GILMAN. Thank you. Mr. Voegtlin, do you agree with that assessment?

Mr. VOEGTLIN. Yes, absolutely.

Mr. GILMAN. How often in cases such as kidnappings and planned terrorist bombs has the court-authorized wiretap prevented the loss of life? Mr. Lee.

Mr. LEE. Mr. Chairman, there have been numerous cases where court-authorized wiretaps have been used by law enforcement officials to prevent and solve—to prevent loss of life and to solve the cases. I would add to that list not just terrorism and kidnapping, but also cases such as child pornography and other exploitation of children. It is an absolutely essential tool.

Mr. GILMAN. What about the timing of information that you receive from wiretaps, too? Is that critical to the cases involved?

Mr. LEE. Mr. Chairman, the timing, the ability to quickly derive the plain text, the meaning from the wiretaps on a real-time instantaneous basis is absolutely critical, both to saving lives and also to apprehending criminals and furthering the investigation.

Mr. GILMAN. Thank you. Mr. Reinsch, what effect would the implementation of the SAFE Act have on the Wassenaar arrangement?

Mr. REINSCH. Mr. Gilman, first it would put us in violation of it. It is inconsistent with it and, second, I believe it would undercut our efforts to obtain stronger multilateral controls. It would probably result in our allies abandoning their efforts to control these products.

Mr. GILMAN. Could you tell us, Mr. Reinsch, do the provisions in the SAFE Act relating to terrorist countries provide effective control for the Administration to stop the export of encrypted products to those countries?

Mr. REINSCH. That is a more complicated question than the Wassenaar question, Mr. Gilman. We believe generally no, but it is a more—that they do not help us provide effective control, but it is a more complicated legal analysis. The bill contains two provisions that contradict each other. One which addresses this question

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 17 2002

specifically and one which generally removes licensing authority for what we believe would be most mass-market products. Even if we were to try to reconcile those conflicting provisions by construing the stricter one as ruling, we have some concerns about the way that it is drafted. It imposes, not with respect to countries, but with respect to individuals—individual terrorists or individual terrorist organizations—a substantial evidence test which is quite a high test, an unusual one for the kind of system that would make it much more difficult for us to identify and list, meeting the standards of the Act, terrorist organizations and proscribe exports to them.

Mr. GILMAN. Just one last question: Mr. Voegtlin, what would encryption without access do to local law enforcement's ability to fight the drug war?

Mr. VOEGTLIN. Basically, we are concerned that it would all but eliminate our ability to fight the drug war. Currently—and it is becoming on an ever-increasing basis—State police directors and local law enforcement agents are coming across encryption in an ever-increasing fashion. Right now what we are looking at are situations where you have drugs being imported into this country and the command and control is taking place overseas and they are using encrypted communications to talk to the subordinates in this country, to talk about distribution and other coordination efforts. Without being able to access this information through wiretaps, the ability for State and local law enforcement agencies to work in cooperation with the Federal agencies on the drug issue will be severely limited if not completely destroyed.

Mr. GILMAN. Thank you and thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much, Mr. Gilman, for being with us. Mr. Menendez.

Mr. MENENDEZ. I thank you, Madam Chairlady, I appreciate this panel's testimony. Before I ask my questions, I want to ask Mr. Lee, is your division of the Justice Department National Security? Is that my understanding?

Mr. LEE. Sir, I am a Senior Member of the Deputy Attorney General's Office. One component of the Deputy Attorney General's Office is called the Executive Office of National Security. I am the acting head of that component, but I also have other responsibilities in the Office of the Deputy Attorney General.

Mr. MENENDEZ. That is not the same division of the Justice Department that declared the air space over Camden Yards to banners talking about freedom and democracy our national security risk, is it?

Mr. LEE. I am not familiar with that matter.

Mr. MENENDEZ. Because that really colored my perception of what national security is. Let me ask the panel the following. My friend and colleague from New Jersey, a new Member of Congress, Rush Holt, is a rocket scientist. His constituents have a bumper sticker in his district that says, "My Congressman is a rocket scientist." Now, I am not a rocket scientist. I am just a poor old country lawyer. What I don't have an understanding about——

I am not a professor either of the law. But what I really have a problem listening to the testimony here about is one basic set of

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 18 2002

circumstances which seems to be glossed over and maybe all of you can help.

No. 1 is, there is no domestic control of encryption. Is that a correct statement?

Mr. REINSCH. That is correct.

Mr. MENENDEZ. So I, as an American, or for that fact, someone from abroad who is visiting here could buy this domestically. I guess taking it back home might be a violation of the law. Is that the case?

Mr. REINSCH. Yes, in general. There would be a personal use issue, but if you were taking it back to give to somebody else or to sell that would——

Mr. MENENDEZ. If I wanted to buy and use it and take it back. But I don't even have to do that, as I understand it. This technology exists by a variety of countries—the Japanese, the Israelis, French, others—who have all of this capacity at its highest levels, as I said in my opening statement, in the Internet, you can download 128 bits. Now I heard Ms. McNamara say that we don't control, we, in fact, permit under the new regulations over 56 bits. But that's if you have, in fact, a key recovery system. If you have a non key recovery system, you can't do that, can you?

Mr. REINSCH. No. Maybe I can clarify that part. I would like to have Ms. McNamara talk a little bit about the availability issue if we have time for that. The policy permits the export in a variety of circumstances that my statement went over fairly quickly of more than 56-bit encryption. In fact, encryption without bit length limit and without key recovery features can be exported to U.S. subsidiaries, for example, to health care organizations, to banks, to financial institutions, and so on.

Mr. MENENDEZ. Yes. Outside of that specific category—and I have a chart here: the banks, financial, health insurance, health care——

Mr. REINSCH. Right.

Mr. MENENDEZ. Outside of that category.

Mr. REINSCH. No.

Mr. MENENDEZ. If you want to, you could not.

Mr. REINSCH. Except via—there is a whole list in that category, more than the ones I mentioned, but outside of what I assume is on your chart, the only way high-level encryption, 128-bit or whatever, could be exported would be pursuant to an individual license that we would issue. An exporter can apply for anything they want and we will consider any application they submit, but it would take an individual license outside of those categories.

Mr. MENENDEZ. My point, Mr. Secretary—and for members of the panel, maybe you can help me here, elucidate to me—the point is whether you buy it here or domestically and you have this capacity and you illegally—because we are talking about illicit activities that we are concerned about and national securities and espionage and all of that—bottom line is whether you buy it domestically or whether you buy it abroad and use it for an illicit purpose here in the United States, what is it that we accomplish in terms of controlling the technology that is readily available and that can be used by anyone who seeks to do so illicitly for espionage or terrorism, for anything. I listened to the line of questioning of our dis-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 19 2002

tinguished Chairman and, all of those things can be accomplished by someone who wants to break the law and use and seek the technology abroad. Tell me what it is that—how do we circumvent all of that?

Ms. MCNAMARA. Let me try and answer that question and then any of my colleagues can chime in behind, sir. Let me first address the issue that you raised about nations overseas. As you heard Mr. Reinsch say and I said as well, in December of last year, 33 nations signed up to the Wassenaar agreement. What that does is permits those 33 nations to have an umbrella arrangement or agreement which allows them then to invoke export controls in their own individual countries. They are doing that and they are abiding by it.

Some of those nations without Wassenaar had their own export control regime and they are abiding by that. The 33 nations that signed up to the Wassenaar agreement are the 33 nations which are today the world's predominant producers of encryption, save one or two, and even those, although not members of Wassenaar, do have their own export control regulatory regime which they invoke for the export of encryption from their own national producers.

The export of, or the individuals who, as you point out, illegally use or apply for the use of encryption, on an individual basis, we are never going to stop all of that. What we are attempting to talk about here is the actual broad use of encryption or the incentive for the broad export of encryption from this country.

Encryption today is not being used broadly. Encryption today is, for the most part, being used by individuals for applications that are approved under our export control regime for business, for banking, for online commerce. All of that export, without requiring key recovery features, I might add, is available under today's export control regime from this country as of last September. That was reinforced and reendorsed by the Wassenaar agreements.

When we look at the international use of encryption, I will tell you that we expect to see the broad use of encryption internationally when three conditions are met. Those three conditions are it becomes inexpensive—and I will grant you, it is becoming inexpensive—it becomes easy to use—and, in some cases, it is in fact easy to use. In other cases it is not—and what will be required for the broad international use of encryption is a security management infrastructure which will allow the registering of keys, the authentication of users, and the free and open exchange of encryption across international boundaries. Those international security management infrastructures do not exist today, globally. So we are not seeing the broad use of encryption.

Mr. MENENDEZ. I appreciate your answer. My concern, however, remains, I think, unanswered. That is, maybe you cannot answer it. Not that you don't want to answer it. Maybe it cannot be answered. That is this, that, listening to your answer, Wassenaar, as I understand it, is ultimately not binding, but even to the extent that, while it is predominate of the countries, it is not exclusive. To the extent that you have access in those countries, domestically, as we would have access here domestically; and to the extent that you have acknowledged that it is becoming more and more inexpensive and easier to use, ultimately it just seems to me that those—

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 20 2002

forgetting about the broad base appeal that we seek to divert for the time being—ultimately, those who want to use such encryption opportunities to do something illicitly, to do something in terms of how this panel has described their concerns about it, ultimately have the wherewithal to do it now. So I don't know exactly what we stop here except American companies from being competitive in the world because those who want to do it will do it.

Last, even to those that you have given presumptions of approval to, to American subsidiaries abroad that have foreign nationals working for them. It does not give me a sense of rhyme or reason. I get the sense that, we want to try to stop what we cannot stop and we are just hoping to buy time here at the end of the day. I may be wrong in that perception, but that is certainly the perception I have.

Mr. LEE. Mr. Menendez, if I may address that briefly from the law enforcement perspective, our position is not that the policy is a failure if there is one single illicit or bad person using encryption. We fully understand that people are going to go to great lengths to use encryption that we probably will never be able to read. The issue for us is that we are starting to get into a world where everyone will be using encryption and the policy issue, both for the world of exports and for the United States, is what will that world look like? Will it be a world where there is some possibility that the wiretaps that Mr. Voegtlin and I have spoken about will have some value, some meaning to protect public safety? Or will it be a world where those wiretaps are completely useless? That is the overarching policy issue, not whether a criminal or a terrorist could—indeed they can and they do. We are seeing that increasingly—not whether they can, in an isolated case, find encryption that frustrates us. The question is, as encryption becomes much more pervasive so that people don't have to go to any effort whatsoever to use it, what kind of a world will we live in?

Mr. MENENDEZ. My concern, Mr. Lee, is that what you are concerned about already is becoming a reality, notwithstanding anything that we are doing right now. I thank the Chair Lady.

Ms. ROS-LEHTINEN. Thank you so much, Mr. Menendez. Mr. Bereuter.

Mr. BEREUTER. Thank you, Madam chairman. Thank you for your testimony. Mr. Reinsch, the reference has been made to the dialogue the Administration had been engaging in with the industry. I believe it may have first been started or at least noticeably progressing when it was initiated by John Deutsch, the Director of the Central Intelligence Agency. It seems to me that he maintained a successful back channel communication with the group of top industrial CEO's. They were moving ahead in what appeared to be very useful negotiations to strike a useful balance. When Deutsch left, Deputy Attorney General Jamie Gorelick continued that process and she has been now for well over a year.

It seems to me, looking at it from the outside, that the discussions have withered away and do not appear to have the attention or the focus of the necessary officials in the Administration. In its place appears to be unilateral declarations. The Administration, through a new policy unveiled by Vice President Gore, implemented new regulations. Industry, not satisfied with this action, is

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 21 2002

lobbying for enactment of the SAFE legislation. I was always interested in the past to see representatives, actual employees of the software companies, coming up here, and lobbyists paid by them to represent those software companies on this issue oftentimes unaware of what had happened with negotiations with the top-level CEO's in their own companies.

I think this matter of encryption control is a very serious matter, yet it appears the issue has been left to drift off the legislative cliff. We need, I think, to find a balance, an option that works in the real world. That would entail intense, very high-level negotiations and compromise. it seems to me, much like the negotiations were leading to, I thought, that Deutsch was leading.

So my questions, to begin with, are what steps are being taken to reengage at the highest level industrial CEO's to find a realistic, workable balance, or is something going on that you can't talk about here or that you can talk about here? Who is the Administration's point person in this dialogue? When was the last dialogue meeting with top leadership of the software companies? When is the next meeting? Is anything like this happening?

Mr. REINSCH. I can make some comments, Mr. Bereuter, without going into all the details of 2 of 3 years of history on this which I see in some respects similar to your points and in some respects, I think, different than the points you have made. I don't think we have become unengaged, if you will.

I think after Mr. Deutsch's departure from the government, the dialogue has ensued really on two levels. There was a direct dialogue with law enforcement and with the Justice Department and the FBI, which I think Mr. Lee could comment on separately, which was designed to put those two groups in direct contact for discussions, in many respects, at a technical level of how they could help each other and how they could try to advance the ball from that point of view.

Mr. BEREUTER. With the industry? A dialogue with the industry?

Mr. REINSCH. That is correct. I am sorry. Yes, with the industry.

In addition, we have continued the dialogue at senior levels, both with individual executives and also with several large groups, both hardware and software, that have become the representatives, if you will, of that point of view. Throughout this dialogue, whether before or after Mr. Deutsch's departure from the government, at no time has the industry abandoned or dropped its goal of passing Mr. Goodlatte's bill and we don't assume that there is anything that we can do that will cause them to change their mind. When Mr. Goodlatte is offering them the whole pie, I wouldn't expect them to deny the opportunity.

At the same time, I think that what we have done with them has been very successful in addressing a lot of the problems they have identified, and I think if you go back and look at their reaction, you can ask the following panel. Ask Mr. Smith, who will be on after me and some others about their reaction after the Vice President's announcement in September. I think you will find that it was quite a positive reaction and a welcoming reaction as a product of some constructive dialogue we had at that time. Their final sentence was, this is great, we want more. We respect that. But I think it has been a successful relationship. It goes on.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 22 2002

I think the next encounter is likely to be the 10th of June when we have a group of CSPP CEO's coming to town on several subjects. Computers is probably at the top of their agenda, but I am sure encryption will not be far behind and I am sure they will be meeting with representatives of the Administration. I understand they will be up here as well. I think that will be a chance to renew the dialogue collectively, but there are frequent opportunities for one-on-one or smaller group discussions. My secretary, Mr. Daley, has been to California several times in the last 3 or 4 months, as have I. We have these discussions every time we go.

Mr. BEREUTER. Secretary Reinsch, I would expect that seeking the whole pie, Mr. Goodlatte's legislation, would be a good negotiating tactic. I wouldn't deem it impossible to find something that is balanced despite their almost unanimous support for it.

Director McNamara, my understanding is that the Wassenaar agreement still allows the export to countries that set different standards. I can't understand really, in that situation, how you are able to achieve your purposes in protecting the national security or how law enforcement is able to pursue at the local, national, or State level their objectives when you have got this differential under Wassenaar. What am I missing here? Is that a problem or am I wrong about the impact of Wassenaar on the exports to the various countries?

Ms. MCNAMARA. The existence of Wassenaar allows countries to actually have something to connect an export control regime to in those countries that didn't have a regulatory underpinning in their countries. It is all up to national discretion, as it is in our——

Mr. BEREUTER. It is differential in its application, isn't it, Director McNamara?

Ms. MCNAMARA. I am sorry, sir?

Mr. BEREUTER. It is differential in its application, country-to-country?

Ms. MCNAMARA. Yes. Country-to-country, as it is here. But it is fundamentally based on end-use and end-user and there are agreements that are in common, like preventing the export of encryption to terrorists and we can do, actually, a comparison for you, sir, if that would be helpful.

Mr. BEREUTER. It does seem to me that the end-user approach is unenforceable in reality. Secretary Reinsch, one final question. You mentioned in your written testimony at least that you believe the Goodlatte bill, as drafted, could inhibit the development of key recovery even as a viable commercial option for those corporation end-users that want it in order to guarantee access to their data. Could you elaborate on that?

Mr. REINSCH. Yes, Mr. Bereuter, if I can find the provision. I think if you look at—I wouldn't say, by the way, that—I tried to phrase that statement in my testimony carefully because I wouldn't say that the problem is as big in this bill as it is in some other ones that have been introduced, but I think if you look at, in general, the provisions on page—in my draft, which I think is the one with all the cosponsors on the front, the provisions on page five and page six of the bill. We would interpret them as significantly discouraging the use of key recovery. I would not go so far as to say the bill prohibits that, but we think it has an inhibiting effect.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 23 2002

Mr. BEREUTER. You did say inhibit and that is the word I tried to use in your quote. I will look at those. Thank you very much. Thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you. Mr. Goodlatte, we are going to recognize you in a moment even though you are not a Member of our Committee. Mr. Delahunt.

Mr. DELAHUNT. Yes, thank you, Madam chairwoman. I have had the benefit of this testimony in my capacity on the Judiciary Committee and I have had an opportunity to engage in some dialogue. I would just make some observations. I think that both Mr. Bereuter and Mr. Menendez have articulated some of the concerns I know that you have heard from me in terms of those who are sophisticated and have an intent to indulge in illicit activity, you simply can't deter them, given the realities of foreign availability. I think this is the problem that we are wrestling with. I think, if I am correct, Director McNamara, I think you just acknowledged that earlier in your testimony? I don't want to put words in your mouth, but that was the conclusion that I draw.

Ms. MCNAMARA. We are never going to stop everyone from breaking the law. That is true, sir. But coming down in the car, I happened to be thinking that just because somebody speeds through a school zone doesn't necessarily mean we raise the speed limit in the school zone.

Mr. DELAHUNT. Right.

Ms. MCNAMARA. There are some products available overseas. I would appreciate it if you accept Mr. Gilman's earlier offer when he announced the classified session on Thursday and I would be happy to talk about this in more detail at that session.

Mr. DELAHUNT. I hope to accept that invitation, but I am just saying for those who are unable to go to that particular briefing. I think that the concern that I have from a national security perspective, if the development of encryption technology in this country is impeded—put aside for a moment the adverse impact in terms of our balance, in terms of our economy—what we are going to have is these cutting-edge encryption technologies far surpassing what we have available to us. If the marketplace is really driving this issue. I think I understand where you are heading. I think, particularly, I am addressing this to Ms. McNamara, not just because you are a former resident of Massachusetts, because I know you have strong feelings about this particular issue.

Ms. MCNAMARA. About Massachusetts, sir.

Mr. DELAHUNT. About Massachusetts, obviously. Don't worry, they won't tear down Fenway Park. I can assure you that.

But my point is, particularly from a national security perspective, we are dealing with a level, I presume, of sophistication in terms of potential adversaries where they will take advantage of cutting-edge technologies that are available in the marketplace. This is the bottom line in terms of the concerns that I have and, at the same time, disadvantaging our, commercial interests as far as competing in the global economy.

Ms. MCNAMARA. As Mr. Reinsch said, if I may, as Mr. Reinsch said and I said in my testimony, we do not want to impede the creativity of U.S. industry. That is not our goal. We want to see U.S. industry succeed and we want to see them succeed overseas. What

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 24 2002

this bill does, though, is eliminate all control mechanisms on exports.

Now when we say that, what we want to see is a regulatory process where, outside of those sectors who have broad relief and therefore have—they can sell their products anywhere in certain sectors and for electronic commerce for certain purposes, we want to see a review process and we want to see who the end-user and the end-use is going to be so we can understand the product.

Mr. DELAHUNT. I don't disagree with what you are saying in the stated goal. But, at the same time, I think what we have to remember—you refer to Wassenaar and it is discretionary and I don't think we ever level off that playing field until we have an enforceable multilateral export control regime. I just don't see—that all nations will respect and that do not disadvantage commercial interests and we are not going to do this with an agreement, that is related to the Wassenaar compact.

Mr. REINSCH. I think—if I could comment, Mr. Delahunt—what intrigues me about this line of argument—and it was similar to the one that Mr. Menendez was putting forward—is the interesting question is what do we do in the interim before we reach that point. We may never reach that point, but let us assume that we are striving for an effective multilateral arrangement, which would deal with this.

Mr. DELAHUNT. Right.

Mr. REINSCH. I think that is a fair statement. What do we do between now and then? It seems to me that the suggestion you are making is almost that because we cannot succeed completely, we should give up. I think we are not prepared to give up simply because we are not going to be perfect.

Mr. DELAHUNT. Again, I think you have got to deal with the realities on the ground. Mr. Lee and Chief, you say there are incidents that have occurred in terms of encryption. Can you quantify them? Give us some hard data in terms of—Chief.

Mr. VOEGTLIN. Actually, like, Mr. Menendez, I am not a rocket scientist nor am I police chief. I just represent the police chiefs. As a matter of fact, in preparing for this testimony today, I was on the phone with State police directors in some of the largest States in the country asking them to quantify the number of incidents. It kind of goes to the point that you are making. What they told me is that right now, since this is in a growing area, most of the evidence that they could give me is anecdotal, but I think it speaks to the larger issue of what you are talking about, that it is already out, that the cow has left the barn or the horse has left the barn on this issue.

But—and this is going back to me not being a rocket scientist—from what we understand here, there are questions about reliability, as Chairman Gilman mentioned, with foreign-made products, that there is not a whole lot of robust nonrecoverable encryption out there right now that is being used.

Mr. DELAHUNT. Let me just regain my time and I know my time is expiring and I just would ask for a minute's worth of followup here. The reality is, I compared it during the hearing in the Judiciary Committee to an imaginary line. You simply buy it here. You don't even have to get on the plane and go across, the ocean. Just

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 25 2002

download it and it is available instantaneously all over the world. The criminal element that most chiefs of police deal with on a regular basis—I served in the law enforcement community for 21 years and when they start using encryption, that comes as a surprise to me.

Mr. VOEGTLIN. That is——

Mr. DELAHUNT. These violent criminals—and I think that is the concern that most Americans have in terms of traditional street crimes which local chiefs of police and State police and local prosecutors deal with—God forbid they start using encryption because we are in real trouble.

Mr. VOEGTLIN. Congressman, and if I can——

Mr. DELAHUNT. I am talking about the, you know——

Mr. VOEGTLIN. I know who you——

Mr. DELAHUNT. Most of us aren't rocket scientists.

Mr. VOEGTLIN. Right.

Mr. DELAHUNT. Most of us have difficulty logging on.

Mr. VOEGTLIN. That is exactly the point that we are trying to make in that when encryption, highly robust encryption, becomes widespread, when the United States—which is a market leader in this area and would be with this legislation—takes the lead in the manufacture and distribution of this robust, unbreakable encryption, it will become easier for those street-level thugs to use encryption. The problem will become more widespread and——

Mr. DELAHUNT. With all due——

Mr. VOEGTLIN [continuing]. Let me just finish.

Mr. DELAHUNT. OK.

Mr. VOEGTLIN. In the opinion of the International Association of Chiefs of Police, what you are facing is a choice: whether or not you want to take this kind of software, make it available widespread to increase its use, to allow people on a low-level of crime—I know we are always going to be dealing with folks who are drug lords who have unlimited resources—but when you start putting it on the street level, it becomes more widespread and that is our concern.

Mr. DELAHUNT. With all due respect to your position, I wasn't a chief-of-police, I was a chief prosecutor in a major jurisdiction. I daresay, that, availability to the street-level criminal simply is an argument that is disingenuous, with all due respect. I can't accept that argument. I know better. I know better. I yield back and thank the Chair.

Ms. ROS-LEHTINEN. Thank you so much, Mr. Delahunt. Mr. Goodlatte, if we could recognize Mr. Gilman for one question before we turn to Mr. Goodlatte.

Mr. GILMAN. Just one question in response to what the testimony has been. The gentleman made the point that there are always people willing to do illicit acts and use means to conceal them, but is that a reason to throw in the towel and see encryption devices on every street corner in the hands of every petty drug dealer? Isn't the issue here proliferation of unaccessible encryption?

Mr. VOEGTLIN. Absolutely. That is exactly what we are talking about—is when this becomes proliferated. When this is widespread, the problems will multiply and State and local law enforcement, which is only dealing with it on an anecdotal level at the moment,

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 26 2002

will deal with it over and over again. The resources of the State and local law enforcement agencies are obviously less than the Federal Government. If they are already dealing with it, imagine what it will be in 10 years when even local dealers dealing with distribution networks on the street level are able to communicate in absolute security that law enforcement has no idea what they are talking about.

Mr. GILMAN. Mr. Lee, would you care to comment on that issue?

Mr. LEE. I would only add, Mr. Chairman, that I think you have really pinpointed the issue and the public policy dilemma for all of us. One of the things that I mentioned in my opening statement is that we have been having very productive discussions at a number of levels with law enforcement, arising from the CEO interaction and, in large part, it is to look at where industry sees the marketplace going and how we can better understand their needs, how they can better understand public safety needs, and what the possibilities are for a convergence of those interests. That has been a very productive dialogue and I think it is one way that we are, with industry, addressing the question: How are we going to shape the way the market looks? How are we going to stand up together and make sure that all of the interests that Mr. Reinsch has mentioned here as having to be balanced, make sure they are all balanced? That is the challenge for all of us.

Mr. GILMAN. Thank you.

Ms. ROS-LEHTINEN. Thank you, Mr. Gilman. Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Madam chairman. First, I would like to note that, as someone who was born and grew up in the Commonwealth of Massachusetts, I am glad to find that I have something in common with Ms. McNamara. I am sorry we don't agree on this legislation, but we do agree on something that Congressman Menendez said earlier, and I think it is absolutely correct—and that is we are all concerned about national security and law enforcement issues.

The issue here is not whether or even when strong encryption is going to be available. It is available now and it is going to be widespread very soon. The issue is how we are going to deal with it and whether we are, as a nation, going to cede this market to dozens of foreign countries and literally hundreds of foreign companies who are already starting up and producing this product. There are 650 strong encryption products available in the United States from foreign sources that could not be exported if a U.S. company made the same product and attempted to sell it overseas. That is a serious problem and one that our competitors overseas are well-aware of.

The problem with the Wassenaar agreement is that it is Swiss cheese. It is something that is loaded with loopholes. The gentleman from Nebraska is exactly right. It can be applied differentially in different countries. It is being done. The aspect of this related to recoverable encryption is one that is being rejected. Madam chairman, if I may, I would make a part of the record an article from the National Journal of Technology Daily pointing out that the French who were previously cited in previous hearings as one of our strongest allies in this effort to control encryption have abandoned key recovery.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 27 2002

Ms. ROS-LEHTINEN. Without objection.

Mr. GOODLATTE. Then the following day an article, also in Tech Daily, pointing out that the British government has abandoned key escrow or key recovery, leaving us with a situation where, as more and more countries do this—and I don't know of any that has attempted to implement a key recovery scheme—we are going to be put in a position where we are holding back the ability to make strong encryption available to people who want to use it, except if they want to download it from the Internet, buy it from foreign sources and the only folks who are going to be impacted negatively by this are the U.S. companies who aren't going to break the law. They are not going to violate our export control laws, but dozens of great companies from IBM to Microsoft to Sun Microsystems to the list goes on and on and on, they are going to be competing with one hand tied behind their back. So the effect is going to be they either send the business offshore or they cede this business to foreign competition.

Now, with regard to recoverable encryption, the gentleman from the Commerce Department has indicated that you are not calling for a key recovery system, but the gentleman from the Justice Department keeps referring to recoverable encryption. During the hearing in the Judiciary Committee, I asked him what he meant by recoverable encryption if it wasn't key recovery and he said that there are many technologies that aren't strictly speaking key recovery that do promote the interests of law enforcement as well as other government interests.

If you are not referring to key recovery, Mr. Lee, what are you referring to? You have still, in spite of having agreed to respond to that, not responded to that in any substantive way to give us other ideas of what you mean, if it is not key recovery. It might be the Clipper Chip, which is a notorious proposal of the Justice Department of a few years back where the chip was embedded into the computer itself and was thoroughly rejected by everybody involved in the process. But what are you referring to?

Mr. LEE. It is not the Clipper Chip. I was referring to a variety of technologies which are going to depend on the application, on the market sector, on the end-user, on the business need. What each of those technologies have in common is that they provide some capability to provide plain text upon presentation of a lawfully authorized court warrant.

Some of the examples that we have given—I obviously don't want to get into proprietary information or favoring particular companies, but—for example, the consortium of private doorbell companies that came to us and proposed a method, which Secretary Reinsch can elaborate on, which would allow the export of strong encryption while also meeting law enforcement needs. There are many others. They are detailed on various web sites. I don't have an exhaustive catalog of them here, Mr. Goodlatte, but there are a variety of different products.

Again, no one of them is—there is no such thing as a key recovery system. That is a term that we were using to refer, perhaps unartfully, to the concept that a product which is designed and marketed to meet a business need also supports the needs of law

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 28 2002

enforcement. That is all we are after. We are not wedded to any particular technology or product or application.

Mr. GOODLATTE. But you would mandate that every company that wants to manufacture and export a product in the United States for sale overseas have that type of device attached to it in spite of the fact that we are confronted with a flood of foreign competition that would not have that mandated to it and, in fact, would be advertising that they have a product that is secure that U.S. companies cannot offer. In fact they are advertising that fact right now.

Mr. LEE. Sir, we would not mandate that. As Secretary Reinsch and the other panel members have testified, in pursuant to the encryption export updates last September, there were a number of encryption products for a number of very important sectors, very significant parts of the world economy where encryption does not have to provide those kinds of capabilities. Also——

Mr. GOODLATTE. So you would not object to the provisions in this bill which prohibits the government from mandating key recovery or key escrow?

Mr. LEE. That wasn't my testimony, sir.

Mr. GOODLATTE. Please clarify then.

Mr. LEE. We have testified, both in our written statements and in our verbal testimony, that we are concerned that provisions in H.R. 850 would inhibit the government from encouraging the use of key recovery, key escrow, other types of plain text availability systems, both for its internal use and for people seeking to do business with the government. You also have Secretary Reinsch's testimony on that point.

Mr. GOODLATTE. What do you mean by the word "encourage?"

Mr. LEE. The government has a number of statutory obligations to make information available to its citizens: document retention programs, government public-right-to-know information, all the information that the government has is held in trust. If that information is encrypted, we have a responsibility, which is set out in statute, to make sure that, at the appropriate time, that information will be made available to the public. So that is the kind of obligation where some kind of plain text recovery system is going to be necessary to meet that obligation. Again, contractors, others who are collecting information for that purpose would——

Mr. GOODLATTE. There is nothing in the legislation which prohibits the government from having its own key recovery system for its own record keeping purposes. But we do prohibit the government from mandating that anybody who does business with the government, which is virtually every business and every citizen in the United States, from using a system that requires a key recovery system to be attached to it. If they prefer for their own security and their own privacy to not have a key recovery system, as many people do, we do not allow the government to mandate that. But we do not prohibit the government from having its own key recovery system for its own purposes. Nor do we prohibit any private business from doing that for those who choose to do it. It is not the business of the government to mandate to people whether they should have key recovery or not have key recovery.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 29 2002

The problem with it is if you mandate it and other creators of products in other countries do not. They have a tremendous market dominating advantage in selling a whole array of hardware and software products that are going to be using strong encryption when they can say that they can guarantee you that no one, the U.S. Government or anyone else has a key to that system.

Mr. LEE. The government does a number of its business through contractors and one of the concerns we have is that this would prevent the government from doing its business in the way that the government deemed most appropriate when the contract is——

Mr. GOODLATTE. So you would insidiously put key recovery into the entire country by saying that if you want to do business with the U.S. Government, you have got to have key recovery. That is what you mean by encourage. When you say you really don't want to mandate key recovery, but you want to encourage it by saying if you want to do business with the government online—which everybody will be doing in the near future—you are going to require that they have a system that, if they do business with the government, has a key recovery feature. Is that what you are saying?

Mr. LEE. I guess, a couple of points in response, if I may. It wasn't my testimony that the government is going to be seeking to do those things. I have testified what the government's position is, as have the other panelists. The government's policy, the Administration's policy, is that there are not restrictions on the use of encryption. What I did testify, Mr. Goodlatte, was that, to fulfill its statutory obligations in the way that it deems best, the government may decide, if it is necessary, to have some form of key recovery.

Mr. GOODLATTE. Require contractors doing business with the government to use key recovery as well?

Mr. LEE. In order to fulfill statutory obligations such as record keeping, that may be a possibility. I wouldn't——

Mr. GOODLATTE. When you say contractors, would that be other people doing business with the government like taxpayers filing tax returns?

Mr. LEE. I was dealing with the situation of contractors. Again——

Mr. GOODLATTE. Where would you draw the line? I just want to make it clear why this bill draws the line at saying we are not going to be mandate because of the fact that this is an all-encompassing thing. Once you start down that road of saying, if you want to do business with the government, you have got to use key recovery, you can, very shortly, require that virtually every system of communications that we have in the country have key recovery, not by mandating it, but by, to use your phrase, encouraging it because if you want to communicate with the government in this fashion, you have got to do that.

Mr. LEE. I think with the possible exception of Washington, D.C., we may have a difference of opinion of the impact of the U.S. Government on the overall economy.

Mr. GOODLATTE. I don't know many law-abiding citizens who don't file tax returns or don't have to communicate with the government on a whole host of other issues that are vitally important to them from social security and Medicare to census taking to—the list goes on and on and on.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 30 2002

Mr. LEE. I also respectfully disagree that the government is trying to do something insidious here. What we are trying to do is to make sure that we fulfill our statutory obligations.

Mr. GOODLATTE. I don't—certainly there is no statutory obligation to impose key recovery because, at this point in time—and I hope forever in the future—we do not have any kind of domestic limitations on the use of strong encryption or the requirement that you use a key recovery system to protect your privacy, to protect your property, which is what strong encryption is designed to do. Thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much. Mr. Sherman.

Mr. GILMAN. Madam chairman, before I go——

Ms. ROS-LEHTINEN. Yes, Mr. Gilman.

Mr. GILMAN. Can I just make a unanimous consent——

Ms. ROS-LEHTINEN. Absolutely.

Mr. GILMAN [continuing]. The May 11th letter from the president of B'nai Brith, Richard Heideman, on encryption issues be made part of the record.

Ms. ROS-LEHTINEN. Without objection.

Mr. GILMAN. Thank you, Madam.

Ms. ROS-LEHTINEN. Thank you.

Mr. SHERMAN. Madam chairman, I would like to pick up on the questions being asked by the honorable gentleman from Virginia. Mr. Lee, maybe you could just put our minds to rest. Will this Administration ever say that, in order for a bank to have any deposits of the U.S. Government, that it must divulge the key recovery information as a condition for having U.S. Government deposits? Are you keeping open that hammer that you would use to deprive Americans of their privacy?

Mr. LEE. I have testified, as have my fellow panelists. that it is the Administration's policy not to seek mandatory regulation of key recovery.

Mr. SHERMAN. I am not talking mandatory. I am saying, as you may know, the U.S. Government sends out an awful lot of social security checks. Those are being sent out by wire to banks across this country. Will the Administration ever tell banks that they must divulge the key information in order to be eligible to receive such wired social security deposits?

Mr. LEE. I think the wise thing for me to do would be to defer that question to Secretary Reinsch.

Mr. SHERMAN. You've shown tremendous wisdom.

Ms. ROS-LEHTINEN. He's a country lawyer.

Mr. SHERMAN. Now let us see whether the Secretary will show wisdom. Can you put our minds to rest or are you going to——

Mr. REINSCH. All I can say, Mr. Sherman, is that I have been involved in, as far as I know, most of the discussions that have gone on this issue for the last 3 years and nobody has even thought about that. Nobody has even——

Mr. SHERMAN. Nobody has thought of it. Can you tell us how——

Mr. REINSCH. Nobody has thought of that. Nobody has suggested it.

Mr. SHERMAN [continuing]. That gentleman from Virginia has thought of it. Can you put our minds to rest or could we face that mechanism of trying to force the divulging of key——

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 31 2002

Mr. REINSCH. I can only tell you what I have said because I am not in the bank regulatory business. If you want to know what is contemplated with respect to bank regulation, you will have to have ask the bank regulators. I haven't talked to them about this. As far as I know it has never occurred to them and it is not on their agenda, but I certainly wouldn't presume to speak for them.

Mr. SHERMAN. But you are representing the Administration here in terms of a desire to have access to a key that would allow you to decode encrypted information. In that capacity, will you be pressing to use all of the levers of the Administration to try to compel domestic organizations doing domestic business with American citizens, will you try to penalize them or take away their right to do business with, for example, social security recipients because they do not divulge the key?

Mr. REINSCH. As far as I know, we have no intention of doing that. But let me stress, at the same time, what Mr. Lee said. The issue here isn't keys, from a law enforcement point of view, the issue here is data and access to data. Key recovery and the existence of the key is one means of achieving the objective. The Department of Justice and other law enforcement entities have, as far as I know—and have said this many times and I think Mr. Lee said it today—have no interest in trying to expand their capacity to obtain private information beyond what existing laws and existing courts permit them to do.

What we are trying to deal with here is simply a means of how do you apply existing court rulings and legislation with respect to law enforcement access to private information to a new technology? We are not trying to expand the right of access. I think the best way to look at this debate is to focus on the information and——

Mr. SHERMAN. Excuse me, I have a limited amount of time. You have gone well beyond the question I asked.

There is, I think, no prospect of getting Congress to give the Administration or any Administration domestically what you are seeking internationally. Do you disagree or will you be proposing legislation that would prevent someone from buying encryption, strong encryption, at their local software store?

Mr. REINSCH. We have testified to that many times and it is in my statement. We have no intention of doing that.

Mr. SHERMAN. So what we have is a situation where you can't go after what you would like domestically, so you want to punish the U.S. software industry by putting it at a disadvantage vis-a-vis its foreign competitors. Not surprisingly, our foreign competitors and their governments have welcomed this effort and have engaged in a little dance at Wassenaar where they pretend to be interested in preventing their companies from marketing strong encryption worldwide and we fall for it and are now in a process of giving away what may be the world's most important industry to our foreign competitors. Then you come to us and you show us how beautiful our economic competitors' dance at Wassenaar and give us that as a reason why we should bludgeon our own industry and make it more difficult for them to compete worldwide.

I know there is a question in there somewhere.

Mr. REINSCH. Was there a question in there, Mr. Sherman?

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 32 2002

Mr. SHERMAN. There will be a question, I assure you, Mr. Secretary.

Mr. REINSCH. All right.

Mr. SHERMAN. That question is: For Mr. Voegtlin—Gene, I am mispronouncing your name.

Mr. VOEGTLIN. Voegtlin.

Mr. SHERMAN. Voegtlin. That is: You talk about how you don't want street thugs communicating with each other, using encryption you cannot decode. Is there any prospect of preventing that when, in fact, your colleagues here representing the Administration won't even propose legislation that would prevent any American, criminal or otherwise, from getting all kinds of encryption from their local software store?

Mr. VOEGTLIN. As you say, they represent the Administration. I do not.

Mr. SHERMAN. Will you be proposing the legislation that they are unwilling to propose?

Mr. VOEGTLIN. If I could, I don't know if we would. But I will say this and I would like to get this as clear as I can. The folks that I represent view this as an issue of great importance and, to them, a simple choice. You have a choice—they understand the need for encryption. They agree that it has legitimate uses. But they are more concerned about trying to—and trying to do their jobs and how encryption prevents them from doing it.

If they had the answer to this issue, I wouldn't be up here. Actually, I would be a very rich man. I am not, so they don't. But what I think you are all confronting here is a basic choice. You need to find some kind of balance between strong recoverable encryption that can fulfill the vast majority of legitimate uses and strong unbreakable encryption that could be put to insidious, dangerous, frightening uses.

I know that is an answer that doesn't answer. But, again, I don't have the answer for you. All I can try to tell you is that we are facing——

Mr. SHERMAN. I agree with you completely. I agree with you completely. I don't have the answer. You don't have the answer. There are elements of the Administration so angry that there isn't an answer that they would just like to bludgeon the hell out of the U.S. software industry. They are, of course, encouraged by our foreign competitors. But it is certainly not an answer to say that we are going to allow something to be purchased at every software store in America, but we are going to prevent legitimate people from exporting that same software.

Because I will ask you, speaking on behalf of the police chiefs, do you know of any mechanism that the police chiefs can use to prevent anything that is purchasable at every software store in America from being exported, either physically or over the line to criminal figures in other countries? Do you have any prospect at all of preventing that?

Mr. VOEGTLIN. I have no information myself. I would be glad to check with our Committees that deal with terrorism, international crime, and organized crime and see if any of those experts have an answer.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 33 2002

Mr. REINSCH. Actually, Mr. Sherman, if I could comment. That is my job. The other half of what BXA does is enforce the Export Administration Act and that is what we try to do. The answer to your question is, in the circumstances you have described, it is extraordinarily difficult. There is no question about that.

Mr. SHERMAN. Is extraordinarily difficult, is that Washington talk for completely impossible?

Mr. REINSCH. It is not.

I try to avoid Washington talk.

Mr. SHERMAN. Again, if I were to walk into Egghead, buy something, and send it over the Internet to somebody in Canada, wouldn't you think that would be like completely impossible for you to stop me?

Mr. REINSCH. What we have said about this many times and what Ms. McNamara said earlier is, if somebody wants to defeat the system, they can do that. There is no question about that. We have never denied that. I would not go so far as to say it is clearly impossible. We have a number of investigations going on. We do catch people. Never underestimate the stupidity of some of the people we have to deal with.

I didn't say that.

Mr. SHERMAN. It is a shame that you do have to deal with Congress.

Again, I think that you are——

Ms. ROS-LEHTINEN. He is not going to name names.

Mr. SHERMAN. I think my time has expired.

Ms. ROS-LEHTINEN. Thank you, Mr. Sherman.

Mr. Burr. Let us move on.

Mr. BURR. Mr. Secretary, your comments are shared.

Mr. REINSCH. We may be talking about different people, though, Mr. Burr.

Mr. BURR. I feel confident we are. Mr. Secretary, I would like to read some statements to you and ask you some questions relevant to those statements. The first is, and I quote, "As the line between military and civilian technology becomes increasingly blurred, what remains clear is that a second-class commercial satellite industry means a second-class military satellite industry as well. The same companies make both products and they depend on export for their health and for the revenues that allow them to develop the next generation of products." If we replaced the word satellite with the word encryption, do you think that statement would still stand?

Mr. REINSCH. First of all, Mr. Burr, I am delighted to see that Members of Congress are reading my speeches. It warms my heart. I encourage you share that with some of your colleagues. I would love to have them look at it.

I think, as a general statement, yes. I think that statement would stand. I think there are a lot of similarities. I was thinking when you made your opening comments, which I felt were quite thoughtful on this subject, that it would be appropriate to apply the comments you made to some other situations as well. That does not mean, however, in either of those cases, this one or the other one, that the answer is no controls. I think it means that the answer is balance and a realistic view about what is controllable and what is not and what the national security implications of both are.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 34 2002

Mr. BURR. I hope, from my opening statement and from my line of questions, you will understand that I think the difficulty that we have or the disconnect with all of our witnesses and many of the Members here and I think what we struggle to understand is we see this reality of the access that the domestic market has today, our inability to limit in any way encryption products, yet some belief on the part of the Administration and others that there is a way to do it. If there is, then share that with us. If there isn't, then, as Mr. Sherman said, let us find the best balance to allow our United States companies to compete in this global marketplace.

Let me go on one more statement. "Some of these satellites bring telephone, television, and Internet services to the Chinese people. I believe such services are an integral part of any effort to bring democracy and freedom to China." Could the same be said of strong encryption products, which might provide those movements for democracy in China to stay behind the prying eyes of the Chinese government?

Mr. REINSCH. Mr. Burr, that is—I would say two things about that. I think that is certainly true. I think, at the same time, some of your colleagues, particularly those on the Armed Services Committee, would make exactly the other point here and that is do we want to sell strong encryption to the People's Liberation Army so it could be further used to protect their own communications from our intelligence and to further oppress the Chinese people?

Mr. BURR. Do we currently allow encryption products to be placed on the satellites that we export?

Mr. REINSCH. The satellites that are launched have encryption which might best be described as—and it is an outdated encryption—it is encryption that allows us to encrypt the signals that control the movement of the satellite.

Mr. BURR. Does it limit one's access to the information off of the satellite?

Mr. REINSCH. I will defer to our satellite export.

Mr. BURR. It is not a proprietary question.

Ms. MCNAMARA. The encryption that has been used on U.S. satellites that have been sold overseas, when there is encryption used, it is, as Secretary Reinsch describes, for telemetering the satellite itself and, for the most part, in fact, I believe in all cases with regard to China, always remain in the hands of U.S. persons. It does not have anything to do with the actual transmission of information over that satellite. It is for the control purposes of the satellite and when the U.S. persons were there at launch, the U.S. encryption that was used was, in fact, retained in the hands of the U.S. parties on the ground.

Mr. BURR. But there is no encryption product in the satellite which protects the security of the data that is transmitted from the satellite?

Ms. MCNAMARA. In fact, these are dumb satellites. It is what—it is the medium over which people communicate. If the communications or the originator of the communications uses encryption, then the information being passed over that satellite is encrypted. But it is encrypted from the ground, not because it transmits over the satellite.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 35 2002

Mr. REINSCH. If I could comment, Mr. Burr, though, Mr. Goodlatte's bill, You have touched on a very central dilemma. Mr. Goodlatte's bill would, in effect, permit the sale of strong encryption both to Chinese individuals who want to encrypt their communications in order to, do things that their government would probably rather have them not do and it would also permit the sale of that same encryption to other forces in the Chinese government who don't want that to happen.

Mr. BURR. I think the part that possibly Mr. Goodlatte is frustrated over is the willingness for the Administration to understand the frustration that currently exists when that product is available here in this country, can be transmitted sold, carried out of the country to be used by people that we restrict U.S. companies from marketing like product to. I think, to some degree, we are like the ostrich with the common practice of the head in the hole. When we have our head in that hole, we believe nothing goes on while we are there. The fact is, in reality it is, isn't it?

Mr. REINSCH. If it will make Mr. Goodlatte feel any better—and I think he knows this—I am at least as frustrated as he is, perhaps for different reasons. But we are working very hard to try to prevent the situation that you have described from occurring. I have testified in other circumstances, I think, in the past before this Committee, that I, for one, would say if we were to reach the point at which you, in terms of commercial consequences, that you are anticipating, I would hope that the Administration would be wise enough to see that and adjust its policy.

I think the disagreement we might have is whether or not that point has arrived now and, if not, how quickly it will arrive. I think what Ms. McNamara suggested is that, for a number of reasons, we find that point somewhat more distant than the Members of this Committee probably do.

Mr. BURR. I hope you understand that my questions are more broad than specifically to the encryption issue. If my understanding is correct, this time next year, with the Merced chip in computers, the off-the-shelf leader model with exceed the M-top standards that we currently have requiring export licenses. Is that accurate?

Mr. REINSCH. Oh, no question. In fact, I can tell you, I think my latest sound bite on that is if we don't change what we are doing by the end of the year, we are going to be controlling Sony Play Stations. It is moving that fast. This is also something the Administration is working quite hard on and we expect to be able to consult with you all and share something with you shortly. But I think it is going to come as no surprise to you that there will be a substantial number of Members in your body who will oppose any changes, notwithstanding the point that you have made.

Mr. BURR. I would agree with your statement that there will be quite a few people who oppose it.

Mr. REINSCH. I am delighted to hear the consistency of your point of view. Not all of your colleagues are consistent on these two sectors.

Mr. BURR. My hope is that that consistency is something that becomes contagious with the Administration.

Mr. REINSCH. We strive for it every day.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 36 2002

Mr. BURR [continuing]. As it relates to the need for these technology companies to, one, compete; two, compete on a level playing field for the effort to grow to the next generation. With that, I will yield back.

Ms. ROS-LEHTINEN. Thank you. Mr. Rohrabacher.

Mr. ROHRABACHER. Yes. Speaking of consistency—and I will just put it right out front—I find it a bit appalling that representatives of this Administration would be here so adamantly arguing for something they claim to be, based in national security, like this encryption debate, while, at the same time, labeling Communist China, which is, at the very least, a potential hostile power—if most of us believe that it is a hostile power—by continuing to insist that we call Communist China a strategic partner of the United States. So I don't want to hear much about consistency in this debate on the national security concerns of our country because the overall policy toward China is doing far more damage to our national security than any of this type of regulation that we are talking about today. In fact, if there isn't a change in the basic, fundamental approach to China, all of your talk about national security is irrelevant.

What I see here is a lot of activity and a lot of effort being put into this effort to—let us, I will just put it right out—you are trying to strengthen government's control, not of other people who are hostile to the United States, but trying to strengthen government's control of ordinary Americans and American enterprise. I don't want to—you hear this all of the drug dealers are going to do this and the bad guys are going to do this, but what do we end up with? Those guys are going to end up with encryption anyway. This is the message I am hearing all around me is these guys are going to end up—and I realize that this is taking to it to absurdism, you might say, but the fact is that when encryption is outlawed, only outlaws will have encryption. Sorry to put it that way, but after listening to the arguments today, I have just come to the conclusion that the only impact you are going to have is on honest people and on enterprisers and not on people who are hostile to the United States.

You are going to have the doctors in this country. You will have their electronic files open and available. You are going to have the lawyers, the bankers. I am a former journalist—trying to tell me that you are going to say you are not making it mandatory, but you are going to say it is going to be conditional, these restrictions are going to be conditional on whether or not people are dealing with the government? Journalists have to get up on their computer and dial in to get their automatic press releases now. The press releases aren't handed out on paper. They come over the electronic processes. So in order to get those, the journalists, in order to get information from the government, they have got to say that they understand that their computers are going to be open to government snooping? All in the name of getting the bad guys?

Let me just note: The government for the last 20 years has had all of this control and the ability to go in and snoop as you wanted to snoop and the drug war is a joke. You go down into any city in the United States of America and any kid can get drugs. This is telling us that we have got to open up the possibility in the years

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 37 2002

ahead in the new millennium to have this type of power in the hands of the government in order to fight the drug war? It is a joke. You have been unsuccessful with all that power already. Again, the only people you are really going to affect are honest citizens like the doctors and the lawyers, the journalists and the rest.

Let me just note this. In the years ahead, the computer systems that we have are going to serve as the basis of American prosperity. Like it or not, that is the world that we are heading into. The Internet system will be used for enterprise and purchases that are the foundation—look at our stock market today. Where is the growth? Where is the faith in the investors? It is in these Internet stocks. What you are talking about is a threat to that foundation in order to make sure the government has the power to snoop. Yes, we need certain powers in the hands of the government to tackle the bad guys. But, as I say, I don't see this as any type of threat to the bad guys because the bad guys will be the ones to get it and the good guys will be the ones who follow the law.

Here is my question. That is my statement. Here is my question? I want to ask Mr. Lee this. Now your title, Mr. Lee, is what?

Mr. LEE. I am an associate deputy attorney general at the Department of Justice.

Mr. ROHRABACHER. For?

Mr. LEE. The titles don't actually say for X or Y, but I work in part on national security and international matters.

Mr. ROHRABACHER. Was it you or your office that denied the effort to get a wiretap on the suspect in the Los Alamos theft?

Mr. LEE. As other officials of the Department of Justice have testified, there is a process set up where the counsel for the Office of Intelligence, Policy, and Review reviews requests from the FBI for that kind of search warrant.

Mr. ROHRABACHER. Yes. So was it you or your office that denied that request for a search warrant for a wiretap? I understand that Mr. Lee who was the suspect in the case was the only wiretap that was denied. Is that from your office?

Mr. LEE. Again—sir, I was not involved in that decision.

Mr. ROHRABACHER. Was that your office?

Mr. LEE. There has been public testimony which, again, I don't have the transcript in front of me, so I want to be careful not to be inaccurate in any respect, but there has been public testimony that the Attorney General asked a member of the deputy attorney general's office to review that matter. That was not me. I don't have any further firsthand information.

Mr. ROHRABACHER. That wasn't my question. Was it your office? You are the head of an office. Was it your office that denied that request?

Mr. LEE. Again, the public testimony is that the prior incumbent of my office had a role in evaluating that request. I do not have firsthand information and so I don't think it would be appropriate for me to try to characterize it any further.

Mr. ROHRABACHER. I will take that as a yes. Let me suggest, as I did in my opening statement, when you have a wrong headed Administration that has wrong headed policies toward people who are hostile to the United States of America, no matter what we do on this encryption, no matter what powers that we grant to the gov-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 38 2002

ernment, we are not going to be safe. I feel, in fact. very hesitant to grant the type of enormous powers, as we come into this new age of electronics and computers, to grant this enormous power to the Federal Government, especially one that is represented by an Administration that is totally going the wrong way on national security issues.

With that, I yield back my time.

Ms. ROS-LEHTINEN. Thank you. Mr. Cooksey.

Mr. COOKSEY. Thank you, Madam chairman. Earlier today, I believe there was a question about the effect of H.R. 850 on local law enforcement. It was mentioned that there was concern about this effect.

I have a letter here from the Louisiana Sheriffs' Association specifically endorsing H.R. 850 and rejecting the escrowing of the encryption keys. I will ask this question of any one of you that is willing to answer it. Can anyone explain to me why the sheriffs in my area are not concerned about the effect of this bill? I will take a response from any one of you or all of you.

Mr. VOEGTLIN. I can't speak to the rationale of the Louisiana Sheriffs' Association. Perhaps if you talk to folks at the National Sheriffs' Association, they would be able to fill you in. I can't speak to their concerns. I know, on behalf of my membership, the 17,000 members that make up the IACP, that they have expressed, both through numerous Committee hearings and numerous membership resolutions that have been passed, that they are very concerned about this issue and its impact on their ability to perform at the State and local level. I can't answer for the sheriffs.

Mr. COOKSEY. Would anyone else like to try? In their resolution—and I will read a couple of them—they said the legislation proposed by the FBI would require all users of an encryption to deposit a key with a key escrow agent that would be available to FBI access. The FBI access would create and maintain a dangerous and unnecessary vulnerability to Louisiana's information computer infrastructure while failing to offer any increased level of protection these systems require. While the FBI's efforts toward recovering information about criminal cases through high security encryption are well-intentioned, the key escrow plan poses too many severe threats to public safety, confidentiality, and legitimate computer users that far outweigh the isolated benefits it may provide.

There is another resolution. Does anyone want to answer it now?

Mr. LEE. Sir, it is hard to answer without having read the letter which I have not had the benefit of doing. Again, the Administration is not proposing some massive central data base where everyone's keys would be kept. We have been quite clear and consistent that, really, a variety of private agents who would be serving people's whole range of security services for business needs is what is envisioned and that is what we want to work with industry on developing. One of the needs that we think this set of services will have to address is the needs that businesses have for the recovery of their information and plain text.

Mr. COOKSEY. Do you think each one of those could be subject to hackers, to being broken into? Is that possible?

Mr. LEE. It is certainly possible.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 39 2002

Mr. COOKSEY. Is it probable? I see someone out in the audience shaking their head yes.

Mr. LEE. I don't have the information to answer that, sir.

Mr. COOKSEY. Let me just state that I feel very strongly on law enforcement. I have a very close working relationship with law enforcement people in our area. We have some real professionals, particularly some people from the Department of Justice, the FBI. We have got some top people. But I quite frankly don't feel that you see the same level of loyalty to the principles of law enforcement in some of the political appointees in your Department and it is really a disappointment to me.

I am not a career politician. I am a physician. I don't want to be a career politician and I quite frankly hold a lot of the politicians in real contempt because of the inconsistencies I see. Here I see the potential for some more inconsistencies, but, that said, thank you, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much. Mr. Campbell.

Mr. CAMPBELL. Madam chair, out of courtesy to the next panel and the fact that I haven't heard all of the testimony, I will yield and thank you and thank the panel.

Ms. ROS-LEHTINEN. Thank you so much. I will also furnish my questions in writing in courtesy of the second set of panelists. But we thank you very much for your patience and we appreciate you being with us today and we will look forward to continuing this dialogue as this bill goes through the process. Thank you so much to all of you.

I would like to introduce the second set of panelists. We will start with Ira Rubinstein, who is senior corporate attorney for Microsoft Corporation. Prior to joining Microsoft, Mr. Rubinstein was an associate with different law firms and is currently a Member of the President's Export Council Subcommittee on Encryption and serves on the Steering Committee for Americans for Computer Privacy. Mr. Rubinstein is the author of numerous publications addressing export controls and encryption software.

Mr. Jeffrey Smith is a partner at the firm of Arnold and Porter in the firm's Legislative and Government Contracts Practices Division and serves as general counsel for Americans for Computer Privacy. From 1995 to 1996, he served as general counsel of the Central Intelligence Agency. Prior to that, he was appointed by then-Secretary of Defense William Perry to the Commission to Review the Roles and Missions of the Armed Services. Mr. Smith has also served in various capacities within Congress, including general counsel of the Senate Armed Services Committee.

David Weiss is Vice President of product marketing at CITRIX Systems. In this capacity, he is responsible for mapping the company's long-term product strategy and direction. He was instrumental in the release of the industry's first Windows application and launching Internet technology and, prior to joining the firm, he was a founding Member and Director in marketing for Business Matters, Inc., a financial modeling software company. This corporation, CITRIX, I am proud to say is located in my hometown of South Florida and we are happy to have David with us today. Thank you.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 40 2002

Mr. Alan Davidson is the Staff Counsel for the Center for Democracy and Technology, a nonprofit, Washington-based organization that works to promote civil liberties on the Internet. Mr. Davidson is currently leading the efforts to promote encryption policies that protect privacy and, prior to joining the legal profession, Mr. Davidson was a computer scientist. He worked as a senior consultant and designed the information systems for NASA's space station freedom projects. He also worked on technology and policy issues at the U.S. Congress Office of Technology Assessment.

Ms. Dinah PoKempner is the Deputy General Counsel of Human Rights Watch, one of the largest human rights monitoring organizations in the world. Ms. PoKempner has performed field research in Cambodia, Vietnam, Hong Kong, Bosnia, and Croatia for the organization and currently directs institutional policy in various areas, including electronics, communications, and international law.

Mr. Edward Black is the President and CEO of the Computer and Communications Industry Association, an international trade association comprised of leading computer, communications, and networking equipment manufacturers, software providers, telecommunications, and online service providers. Prior to being named president in earlier 1995, he served as vice president and general counsel for CCIA since the mid-1980's. He currently serves as the Chair of the State Department's Advisory Committee on International Communications and Information Policy.

We thank all of you for being here today. We will be glad to put all of your statements in the record and we ask you to please be as brief as possible.

Mr. Rubinstein.

STATEMENT OF IRA RUBINSTEIN, SENIOR CORPORATE ATTORNEY, MICROSOFT CORPORATION

Mr. RUBINSTEIN. Good afternoon, Madam chairman. I greatly appreciate the opportunity to appear today before the Committee on behalf of Microsoft and the business software lines of BSA. I especially wanted to thank you, Madam chairman, for your support of the SAFE Act in this and prior Congresses. I also want to thank the other Committee Members who cosponsored the bill this year.

American software and hardware companies have succeeded because we have responded to the needs of computer users worldwide. One of the most important features users are demanding is the ability to protect their electronic information and communications securely. American companies have innovative products that can meet this demand and compete internationally, but there is one thing in our way: the continued application of over broad and restrictive U.S. export controls.

BSA strongly supports the SAFE Act because it modernizes and liberalizes U.S. export controls. We urge the Committee to report the SAFE Act without amendment and we look forward to its passage in the House this year.

I want to emphasize three points today. First, any effort to control mass-market products based on key lengths is doomed to failure. Eight years ago in a 1991 study, the National Academy of Science discussed the nature of mass-market software and the fu-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 41 2002

tility of trying to control it. The NAS concluded, "The widespread availability of such software, coupled with its difficulty of detection and ease of reproduction makes any attempts at controls impossible,".

These observations and conclusions were true in 1991 and remain true today. If anything, they are even more true, given the rise of the Internet and the other means for electronically distributing software to mass-market customers on a worldwide basis. The addition of encryption functionality to mass-market products does not somehow alter these characteristics. Products that are not controllable at 56-bit key length do not become controllable at longer key lengths.

My second point is that export controls create competitive advantages that foreign firms have been very successful in exploiting. Their entry point is U.S. export controls. Because U.S. firms are unable to satisfy customer demand for 128-bit encryption, non-U.S. firms create and freely distribute so-called step-up software whose sole purpose is to increase the key lengths of U.S. products from 40 bits or 56 bits to 128 bits. At the same time, these foreign firms develop powerful service software and related applications for Internet banking, e-commerce, and secure messaging. They also develop consulting expertise to service key customers such as banks, ISP's, telcos and online merchants. These are all the pieces needed to offer a complete package of 128-bit encryption to foreign customers and U.S. firms can't compete with this.

This approach has spawned several of the fastest growing and most successful non-U.S. software firms focusing on the Internet market. In the interests of time, I will just highlight one of them, a firm called Baltimore Technologies, which is an Irish company which recently merged with Zergo, a U.K. company, and now offers a complete line of e-commerce and enterprise security products. At this point, I would like to show you exactly how Baltimore markets its products over the Internet.

[Slide.]

These slides, these are slides of what you would see if you visited their web site. It is not a live connection, in the interests of making it go quickly. The first page is their homepage. You see in the upper lefthand corner that it is the Zergo homepage and it lists products and services and other information that you can find there.

[Slide.]

The next page includes in its marketing materials the very statement of the problem that we are here today to discuss. I will read it quickly. "U.S. export restrictions dictate that most web service and browsers cannot perform 128-bit encryption for security. Instead, export versions of browsers, like Internet Explorer and Netscape Navigator and export versions of web servers like Netscape Enterprise Server and Microsoft Internet Information Server, are limited to 40 bits of encryption, which is not secure enough for most applications." So here is the marketing material of a very successful foreign firm citing U.S. export controls.

The success of these foreign companies threatens the growth of U.S. software firms and their contribution to the U.S. economy. It also threatens American technological leadership, the loss or dimi-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 42 2002

nution of which directly threatens U.S. national security and law enforcement objectives as well.

Let me conclude with a final point and that is that the SAFE Act strikes the right policy balance by promoting the use of encryption for several purposes: to prevent crime by protecting sensitive communications data; to promote national security by protecting the nation's critical infrastructure; to protect e-commerce; and to protect individual privacy. Thank you, Madam chairwoman.

Ms. ROS-LEHTINEN. Thank you so much for your testimony. Mr. Smith.

STATEMENT OF JEFFREY SMITH, GENERAL COUNSEL, AMERICANS FOR COMPUTER PRIVACY

Mr. JEFFREY SMITH. Thank you, Madam chair, and Members of the Subcommittee for the opportunity to testify on H.R. 850, the SAFE Act, sponsored by Representatives Goodlatte and Lofgren and cosponsored by a bipartisan group of over 250 House Members. I serve as counsel to the Americans for Computer Privacy, a coalition of 3,500 individuals, 40 trade associations, and over 100 companies representing a wide range of companies. We support policies that allow strong encryption and we specifically endorse the enactment of the SAFE Act and we respectfully urge the Subcommittee to report it without amendments 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. Strong encryption is essential to protecting our Nation's infrastructure, ensuring the privacy of electronic communications, protecting our national security interests, safeguarding the public, and maintaining U.S. leadership in the development of information technology.

The challenge is how to do that. The question this Subcommittee must address is what is the best policy to achieve these objectives? It is the firm view of ACP and its Members that, given the breathtaking pace at which information technology, including cryptography, is developing around the globe. the only way to achieve these goals, in the long run, is to adopt policies that will assure American industry continues to lead the world in information technology.

It is often said that the first responsibility of government is national defense and it seems to us that the President, Congress, and industry collectively have a responsibility to ensure that in the future our law enforcement and intelligence agencies have the ability to continue to protect this nation as they do today. Indeed, they will probably need additional resources and technical help to meet the challenges of the next century. But those challenges are far greater if they are forced to face a world in which the majority of communications pass-over systems that are foreign-designed, foreign-built, foreign-installed, and incorporate foreign encryption. We are concerned that the current policy of this government risks just such an outcome.

We have worked hard over the last couple of years with the Administration to help fashion its new policy and we are grateful for

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 43 2002

the new policy, but we think further steps are needed and we urge the enactment of the SAFE Act. With that, I will yield the rest of my time, Madam chairman.

Ms. ROS-LEHTINEN. Thank you so much. We appreciate it, Mr. Smith.

Mr. Weiss.

STATEMENT OF DAVID WEISS, VICE PRESIDENT OF PRODUCT MARKETING, CITRIX CORPORATION

Mr. WEISS. Thank you. I will try to be as brief. Good afternoon, Madam chairwoman, and greetings from the Sunshine State, and Members of the Subcommittee, thank you for the opportunity to speak with you this afternoon regarding this important topic. My name is David Weiss. I am the Vice President of product marketing for CITRIX.

Ms. ROS-LEHTINEN. Now, because you are a constituent, take all the time you like.

Mr. WEISS. Thank you very much. I am pleased to be testifying this afternoon 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 1,400 member companies engaged in every aspect of electronic commerce and has long supported efforts to liberalize encryption export controls and H.R. 850, the SAFE Act.

CITRIX is the worldwide leader in server-based computing. Our products enable individuals to access applications which are running on their corporate networks while traveling at home or from anywhere in the world. Since 1989, we have worked hard to ensure that we provide cost-effective products to allow businesses to deliver access to their mission-critical applications to their employees and partners reliably and efficiently. Our products allow companies and organizations to share their corporate network resources with all of their employees, regardless of their physical location.

In today's fast-paced economy, companies must be able to communicate and share information with their employees securely. Companies like mine have worked hard to develop technology and products that meet these critical needs, providing both individuals and businesses with the tools they need to remain competitive. Encryption has become a requirement for the technologies we developed. Without these capabilities, we cannot assure customers that our products incorporate reliable security to protect their corporate communications and proprietary information. Encryption helps individuals and businesses meet the challenges that we face in the online environment, while assuring that we are able to take advantage of its key benefits.

CITRIX products enable communications and information sharing, usually within a company and generally involving vital applications. For most of our customers, the ability to communicate privately with business colleagues is critical. Many use CITRIX products to share sensitive information and require our products to protect that data from misappropriation by unauthorized parties or misuse by otherwise authorized but negligent or malicious parties.

Encryption is the only practical means by which parties to an online communication can trust that each is who he claims to be and

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 44 2002

that the information is only available to its intended recipients. It is the only practical way to guarantee that the communication between those parties remains protected. Such capabilities are critical for both businesses and individuals seeking to take advantage to 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 rapidly integrating these capabilities into their everyday lives. To ensure that this market continues to grow, consumer concerns like security, authentication, and privacy 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. In order for our customers to be able to communicate securely, our products offer a variety of encryption technologies, some of which cannot be exported under the current regulations.

The impact on our company and all of U.S. industry is significant. Companies are forced to choose between incorporating encryption into their products to meet the consumers' requirements or creating multiple product lines. If the company does not incorporate the strong security features that so many businesses demand, their products will fail in the marketplace. If the manufacturer does choose to incorporate strong encryption, it forgoes the lucrative foreign marketplace and many companies, especially many young Internet startup firms that are shaping the electronic commerce marketplace cannot afford to create multiple product lines.

Given the time constraints, I just want to say that on behalf of CITRIX and the SIIA, we strongly endorse H.R. 850 and I will yield the rest of my time.

Ms. ROS-LEHTINEN. Thank you so much, David. To the panelist and our Congressional Members and our visitors, I have asked that Congressman Campbell be kind enough to Chair the remainder of the hearing. I have to go to the Floor and await my turn to speak on the Central America aid package so I have read your testimony and I look forward to sending you some questions in writing. Thank you so much. Thank you, Tom.

Mr. CAMPBELL. [presiding] Mr. Davidson.

Mr. Davidson.

STATEMENT OF ALAN DAVIDSON, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DAVIDSON. Thank you. Good afternoon and I would like to thank you for this opportunity to testify in front of the Subcommittee on behalf of the Center for Democracy and Technology. CDT has supported the SAFE Act since it was first introduced in the 104th Congress. While we are pleased to be here testifying once again in front of this Subcommittee, it is unfortunate that we are here making many of the same arguments that we were making 2 years ago. I would like to take the chance to thank the Chair and Mr. Goodlatte and the other sponsors of the SAFE Act and supporters of the SAFE Act for their continued support for privacy online.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 45 2002

I would like to make, briefly, three quick points today. The first is that the current U.S. policy harms personal privacy, that U.S. policy is failing in the international marketplace and that it is time to move on because a new, more comprehensive encryption relief package like SAFE offers is ultimately going to be better for public safety and individual privacy.

CDT is here today because current U.S. policy does violence to our constitutional liberties here in the United States and to individual privacy around the world. We live in an era of eroding personal privacy where more and more of our personal data is available in electronic form and particularly on the Internet. Encryption is the essential tool to protecting the security of our data in this open, decentralized, global network. The U.S. export controls keep people from getting the encryption they need and protecting their privacy online. Most directly, export controls limit the availability of good, U.S. encryption products around the world, particularly in the mass-market products that most individuals use.

Export controls also affect the security of people in the United States when they communicate abroad with people who don't have access to those strong products. Finally, encryption products affect the security of the infrastructure by dumbing down our security infrastructure and keeping us from making encryption something that is easily available to people around the world, including in the United States. In summary, encryption leaves us in the worst of both worlds. Sophisticated criminals, terrorists, rogue governments have access to it, but law-abiding individuals do not have security and privacy protected by the tools that they need.

The second point I wanted to make was that U.S. encryption policy is failing in the international arena. We were told 2 years ago that the world was on the verge of adopting key recovery and export controls. In fact, the marketplace has failed to embrace key recovery. The world community has failed to embrace export controls and key recovery as well. In fact, as we have heard in testimony, many countries, including countries like Ireland, Canada, and Finland, are moving in the opposite direction. Even some of the staunchest U.S. allies, the U.K. and France, have failed to completely embrace U.S. encryption policy.

U.S. encryption policy is failing in the courts. Just earlier this month, the Ninth Circuit Court of Appeals found that export controls on encryption source code were unconstitutional violations of the First Amendment. The court ruled that these were prior restraints on free expression that rest boundless discretion in government officials. I think that the court recognized something that the Administration hasn't, that you can't stop the spread of ideas at the border and that especially you can't do it without doing violence to our First Amendment.

I think it is time for our U.S. encryption policy to move on. We are setting the ground rules today for how much privacy people will have as they move their lives online. On balance, we believe that strong encryption both serves individual privacy and protects public safety and that kind of change is not going to happen without your help. While we remain concerned about certain criminal provisions in the SAFE Act, we believe that, on the balance, the bill is a dramatic step forward for individual privacy and public

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 46 2002

safety and I would encourage you all to support its rapid passage without any weakening amendments.

Mr. CAMPBELL. Thank you, Mr. Davidson.

Ms. PoKempner.

STATEMENT OF DINAH POKEMPNER, DEPUTY GENERAL COUNSEL, HUMAN RIGHTS WATCH

Ms. POKEMPNER. Thank you. I appreciate very much the opportunity to come before this Committee. I am Dinah PoKempner, deputy general counsel of Human Rights Watch, one of the largest human rights research and reporting organizations in the world. We have used encryption for many years and I am going to present two examples from my testimony. There has been a great deal of discussion at this hearing about, on the one hand, the economic interest inherent in encryption and, on the other hand, law enforcement and national security.

I am going to tell you a little bit about human rights applications of encryption and, in particular, dwell on two examples. Now the Internet revolution changed human rights advocacy dramatically. We can now report on things in real-time. We can reach massive audiences very inexpensively and really mobilize popular opinion and action as never before. But we have a problem. Electronic communications are inherently insecure and this can have deadly consequences for human rights activists. Every year, human rights activists are attacked, jailed, disappeared, and killed. We document this in our world report. In 1998, we counted 10 such killings before the report went to press.

So, for this reason, our researchers routinely use encryption when they are in dangerous places like Bosnia, China, Lebanon, Rwanda, Kashmir, Hong Kong, and Belgrade. I am going to give you a couple of examples. We have had a researcher who was arrested last year in the Kinshasa airport and detained for 24 hours while guards threatened to beat him. Fortunately, all of his research was encrypted. By the way, he was on a human rights investigation mission for which he had obtained a visa. It was perfectly transparent and obvious what he was doing. Yet, the government arrested him to get his information. Fortunately, because he felt secure his information was safe, he was able to delay until his release could be secured.

We have a situation where the lack of security produced absolutely devastating consequences. For example, last year in April, a Member of the United Nations Secretary General's investigation team who went to gather evidence of massacres of Rwandan refugees in the eastern part of what was then former Zaire was arrested when he returned to Kinshasa. The Congolese authorities meticulously copied his research notes, as well as maps and reports that had been given him by local human rights activists. This information set off a man hunt for all of this official's informants. Many of these human rights activists had to go underground to emerge later as refugees and one, Gallican Ntirivamunda, has disappeared and is presumed dead.

In contrast, our researcher, who had gone the year before, took pains to every night burn his notes after he had typed them into his lap top, encrypted them, and transmitted them. So, as this ex-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 47 2002

ample might give you an idea, global access to strong encryption is vital, not just access for United States residents and citizens.

I am going to give you one more example that will point out some of the problems that export controls can bring up and that is what is going on in Kosovo. It is very difficult. The strong encryption is available right now, but it is really difficult to master it, download it, familiarize yourself, and exchange keys when you are in the middle of a war. That is what is going on right now in Kosovo. People who want to report abuses can't communicate securely. The Serbian government is believed to have sophisticated Russian technology that enables them to crack code.

So privacy advocates teamed up with a private company called the Anonymizer to create a gateway that allows people living in former Yugoslavia to access the Anonymizer and, through the Anonymizer, have confidential and encrypted communications. But there is a problem which one of the other panelists alluded to. If you have a browser that is export strength, this is not secure. Your communications can be intercepted. So you have to still do yet another step of going to another site, downloading yet more software to upgrade your browser. It still doesn't solve the problem of secure communications in the most difficult circumstances, in crisis situations.

This is what I wanted to point out is that export controls, among other things, inhibit the development of products that would be most useful to human rights activists. That is, mass-market strong encryption that is ubiquitous, that is built-in, that is easy-to-use, that you don't have to be a computer expert or adept to use. I am certainly not one and most human rights activists aren't adept either.

I am going to end that with the thought that when we talk about the kinds of policies the United States is going to adopt, it is going to be looked at as a global leader. It is going to be looked at as a model. Will we adopt policies that will allow our government to continue to protest abuses of human rights advocates and suppression of human rights abuses? Are we going to hold encryption hostage to the fear of sophisticated terrorists and criminals who are going to use it no matter what the legality is and then deprive law-abiding citizens and human rights activists of its benefits.

I will just finish by saying that what I would like you to keep in mind is that what is at stake is more than just our market share, more than abstract principles of privacy and free expression against, say, the tangible reality of terrorism. There are actual lives of human rights advocates at stake and that is what I would like you to keep in mind.

Mr. CAMPBELL. Thank you very much. I only regret that the Administration spokespersons are not here to listen to you as you listened to them.

Mr. Black.

STATEMENT OF ED BLACK, PRESIDENT AND CEO, COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

Mr. BLACK. Thank you for the opportunity to testify before you today and I apologize for my not-yet-disappeared laryngitis. Encryption is a subject of vital importance to the members of the

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 48 2002

Computer and Communications Industry Association and to all of our industry. I have to take a quick aside and say as a citizen, however, I think Dinah's comments are just so right-on and that is a key part of this that we should never focus on. We will focus on the business aspects, but it is hard not to think of the importance to freedom and democracy of real meaningful encryption available to people around the world.

Like the current key recovery requirements, the Administration's original Clipper Chip proposal would have mandated that all encryption products contain a back door for law enforcement and national security agencies to give them access to the plain text of any communication or computer file upon request. Not surprisingly, CCIA members continue to oppose the Administration's policy, as do most of the high-tech industry, most of the broader business community, and privacy groups. The Administration supporters on the Hill, we think, are also few and dwindling in number.

Because of CCIA's members support for the SAFE bill, which we think is an excellent bill which we congratulate Mr. Goodlatte and Congresswoman Lofgren on, we believe that it is possible that—we will use the word "proliferation"—proliferation of encryption is going to happen, is important to happen. We think the use of strong encryption around the world is essential to reaching the full potential of electronic communications and commerce. We all recognize that the relaxation of encryption export restrictions is of critical importance if we are to fully realize the information age we have just entered.

I want to address quickly the Administration's contention that it does not control or seek to control domestic use or sale of encryption. The National Security Agency has testified on numerous occasions that the full implementation of the Administration's key recovery plan would have no impact on their ability to carry out their national security mission. The only logical inference is that the key recovery export policy is designed to benefit domestic law enforcement agencies while avoiding the political and constitutional pitfalls of direct domestic restrictions.

Another fallacy of the government's policy is that the United States has some monopoly on the science of cryptography or the production of encryption tools. This is hard to justify in light of the government's own efforts to replace the current DES encryption standard with a new advanced encryption standard, AES. Of the 15 logarithms submitted in the NIST competition, 10 were from organizations outside of the United States, including countries such as Australia, Belgium, Canada, Costa Rica, England, France, Germany, Israel, Japan, and South Korea. At least half of the five finalists are likely to be foreign competitors and it is very possible that the next U.S. Government standard for encryption will be designed outside of our borders.

To further illustrate the international nature of this industry and the futility of our export controls, let me give you an example of how the Administration policy has affected just one of our member companies. Integrity Solutions is one of the world's leading vendors of secured application technologies. They are based in San Jose, California. Because of our export laws, nearly all of their recent

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 49 2002

growth in staffing and development has been in overseas locations in Sweden and the United Kingdom. This was not by design. They originally only intended to be based in the U.S. and Sweden, but it was a response to the continued restriction of U.S. exports on encryption.

Later this month, it will announced that Integrity, its partnership with Major Systems Integrators, will be awarded a contract for all certificate authentication technology for the Special Administrative Region of Hong Kong. They expect that this contract will reap millions of dollars in annual revenues and eventually expand to include other Asian nations. Unfortunately, none of the revenue will come to the United States and none of the jobs that this contract will create will go to Americans. Because of our export laws, all of these products and services will be shipped out of the United Kingdom division. Had the contract not gone to Integrity, it would have gone to an Irish company, which would have been the alternative winner of the contract.

My question is: How does our current policy support important U.S. interests? We are driving American companies and jobs overseas and driving their customers to foreign competitors without any significant impact on our national security or law enforcement capability. It is just nonsense.

I wish that I could say that if we experienced further relaxations in export controls or even enacted The SAFE bill, we would somehow regain these lost jobs and revenue; however, Integrity has already established a critical mass of overseas presence. They are beyond the point of no return. They will continue to derive a majority of the revenue and experience nearly all of their growth in foreign countries regardless of what we do to our laws. I can only hope that we take quick action to prevent this scenario from becoming even more common and repeated over and over again until we reach the point where a huge portion of this industry has migrated overseas. Chairman, Members of the Committee, thank you again for the opportunity to testify today.

Mr. CAMPBELL. Thank you, Mr. Black. The first questioner will be Mr. Goodlatte.

Mr. GOODLATTE. I thank you, Mr. Chairman, and I would like to echo your observation that it would have been very helpful if the Administration's witnesses had been here to hear this excellent testimony and, not only that, but the members of the media. I think that the intensity of the debate has gone out of the hearing because I think we are in great agreement with what you have to say.

I would like to ask you about some of the points that were made by the Administration witnesses. First, they made the statement that this legislation would not be in compliance with the Wassenaar agreement. I would note that the Wassenaar agreement has never been ratified by the U.S. Senate. It is purely a voluntary effort of the Administration only, but it seems to me that the way it is drafted the legislation, which provides for an application of export controls in real national security instances, does comply. I would ask first, perhaps, Mr. Rubinstein if he would comment on the impact of this legislation on the Wassenaar agreement.

Mr. RUBINSTEIN. I think the earlier testimony was that it violated Wassenaar by not having adequate review provisions and I

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 50 2002

think that is an incorrect reading of the SAFE Act. There is a provision in all of the key export control sections allowing for technical review of products prior to export and I think that is the key requirement. If there is any difference, really, between the SAFE Act and the positions that have already been taken by some of the foreign countries that are signatories of the Wassenaar arrangement, it is that the SAFE Act requires review, but then, otherwise, does not restrict export.

What other countries have done in technical compliance with the Wassenaar is to simply impose a licensing requirement, but that licensing requirement is one that says strong encryption may be exported under general license. So that is, I think, a very limited form of compliance and hardly achieves the results that were trumpeted when this announcement was first made, namely that it levels the playing field. All it really does is allow these other countries who already have strong encryption vendors in their jurisdictions to comply in appearance by saying there is a general license requirement, but then the companies are able to export the same products they did prior to that arrangement.

Mr. GOODLATTE. Anyone else? Mr. Black?

Mr. BLACK. I will pass. I will take some other questions, but, for the moment——

Mr. GOODLATTE. Anyone else care to comment on that? If not, let me go on to the next—Mr. Davidson.

Mr. DAVIDSON. Just to say that I think our reading is very much the same that it certainly seems that SAFE, on its face, does not necessarily come into conflict with Wassenaar, both in letter and in spirit. That I think that it was particularly interesting to me that Ms. McNamara was careful to say that Wassanaar merely permits nations to adopt export controls. It does not necessarily require them to adopt export controls and are reading is that SAFE does not violate either the letter or the spirit of Wassenaar.

Mr. BLACK. Maybe if I could take my turn and just respond. We have a long experience in the Association of export controls and everything from computers to telecom. We have a lot of experience with what national discretion means. What we think the adoption of your legislation here would in fact put us in the position that for decades every other country was in, which we would have a standard which might be a little saner and less restrictive than other countries. We think it would be very consistent with certainly what is the spirit of Wassenaar as it will be interpreted by most other countries, which is they are going to go off and sell whatever they want without any restrictions. So certainly the spirit, we think, would be complied with.

Mr. GOODLATTE. Thank you. The Administration's witnesses seemed to be divided into two camps: Law enforcement folks concerned about recoverable encryption—and I think we have pretty well addressed that. The questions asked of that panel. Why that will not work. Although we failed to mention the enormous cost of it. The cumbersome, perhaps even unworkable nature of having a system where billions of keys are stored by somebody under some very costly and bureaucratic system.

But the other issue wasn't touched on as much. That is that the National Security folks seemed to be concerned about the imme-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 51 2002

diate decontrol—the words used by Barbara McNamara—and I think the effort on their part seems to be to delay the implementation of strong encryption, and I wonder if you might comment on the effect of such a delay. Mr. Smith.

Mr. JEFFREY SMITH. I will take that one if I may. It is our sense that NSA is aware that sooner, perhaps rather than later, they will face a world of ubiquitous encryption perhaps produced outside the United States. I cannot speak for them, but my guess is that they recognize that and are hoping that delay will somehow permit the market to develop in such a way that it permits them to continue to do what they do.

Our concern is that, as I said in my statement, the current policy is driving us much more rapidly toward a world where there is, in fact, ubiquitous encryption, but it is not ours. I think the consequence of that for the nation, for everything that we are trying to achieve, is quite substantial and is why the SAFE Act is, in our view, such an important vehicle.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. CAMPBELL. Thank you, Mr. Goodlatte. The Ranking Member of the Committee, the gentleman from New Jersey.

Mr. MENENDEZ. Thank you, Mr. Chairman. I want to thank the panel. I had to step out for a few minutes, but maybe you can help me. I was glancing through some of your written testimony of that which I may have missed. Is it fair to say that the synthesis of your respective testimonies is that, in fact, what I was asking the previous panel in terms of what can you really control here at the end of day, that the consensus is, I think Mr. Smith has just said, that this is available. It is available outside. It is available domestically. It is available abroad. Ultimately, all those who wish to have access for the purposes of doing that which the previous panel is concerned about presently have that access right now. Is that a fair statement?

Mr. BLACK. Yes.

Mr. JEFFREY SMITH. Yes.

Mr. WEISS. Yes.

Mr. DAVIDSON. Yes.

Mr. RUBINSTEIN. Absolutely.

Mr. MENENDEZ. Second, could you—any of you who choose to do so—quantify the potential loss this year if we do not move in a manner that would, for example, on Mr. Goodlatte's legislation, the regime that would be established there, if we don't move in that direction, what are the potential losses to American companies? Do you have any sense of quantifying that?

Mr. WEISS. I can take a very small attempt, looking internally at my own company. We are a relatively small software company at $250 million. While encryption has not been a significant issue in the first 7 years of our existence, over the past 3 it has been and I would quantify our loss last year due to our inability to either develop or supply strong encryption technology to our customers, multinational customers or customers outside the United States, as approximately 10 percent of our revenue. I expect that to grow as a percentage substantially as we begin to build the infrastructure surrounding the digital age of which my company hopes to partici-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 52 2002

pate. So that number will only increase as a percent and really put a cap on the markets that we can play in.

Mr. MENENDEZ. Is there any other industry sense of——

Mr. RUBINSTEIN. It is hard for me to quantify, but I would make two observations. One is that a pronounced trend in the last few years is the use of PC's for ever more complex and demanding computer applications so PC's networked together have begun to replace minicomputers and mainframe computers and really run the infrastructure of many large organizations and I think that has made encryption and security a much more important aspect of software sales even for mass-market vendors like Microsoft and other members of the BSA.

Mr. MENENDEZ. Let me ask another question. This is hypothetical, but I would like to get a sense of what the industry might say. If we were to, the U.S. Government, were to fund the appropriate United States agency to work with the private sector to do decryption technology, what would the industry's response to that be?

Mr. JEFFREY SMITH. If I might address that. Industry has acknowledged that the law enforcement and National Security Agencies face a real challenge in the future and recognize that they may not have the technological skills possessed by industry. So as the Administration panel said and as we have said in several of our statements, industry is working with government to help them reach that understanding. I can't comment for how industry would react to a specific proposal to provide specific funding to that, but there are some suggestions like that, including one from Senator Bob Kerry in the Senate that I, as a personal matter, find intriguing. But whether industry as a whole would be prepared to support that, I certainly can't speculate.

Mr. BLACK. If I could, I think we would all like to think that there would be a solution like that. In all honesty, I think the reality that it is sand going through the fingers and I don't think you pick it back up again with open hands. The idea of brute force, attack, is there. It is possible at the edges, but most of the folks we talk to it really is probably not a viable result. Key recovery is not—we have all looked for years for some magic bullet that goes down the middle and takes care of everybody's concern. We just don't find it.

Mr. DAVIDSON. I would just like to echo and say that I think, first of all, most people in the technical community don't think that brute force attacks are going to work at these high-strength encryption products. I wanted to address a comment that was made by the Justice Department representative earlier about the fact that they were still searching for new—that we are not talking about key recovery anymore. That it is really about new kinds of access technologies and I would just like to say that, we have been playing the name game on this from key escrow to commercial key escrow to key recovery and now it is plain text access.

All of those systems have the same problem which is that the same system that allows surreptitious access by government also creates a huge vulnerability that allows surreptitious access by the people that you are trying to protect yourself from by encrypting to begin with. There are a series of real security and economic con-

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 53 2002

cerns that have been raised about the viability of these systems that have gone—are being completely unaddressed.

There is a report that we submitted to the Committee—and hopefully you folks have seen this—on the risks of key recovery. I would encourage people who are concerned about the national security and law enforcement aspects of all of this to ask particularly in those classified briefings, perhaps, ask to have the questions raised in this report answered because I think the problem has been that they can't be answered and that we don't have a viable system that provides access and protects security and that is why these systems haven't caught on.

Mr. MENENDEZ. I thank you all for your patience and your—yes.

Mr. RUBINSTEIN. If I could add just one point there, there was some discussion in the earlier panel of whether the dialogue between industry and law enforcement had withered away over the last year and I would agree with Mr. Reinsch that it has not and, in fact, there has been some very productive dialogue going on and going on, quietly, but taking place. At the heart of that dialogue, I think, is the recognition by law enforcement that there is no magic bullet.

The precondition for a constructive dialogue is the recognition that there is no single solution that industry can offer but, instead, what is most important is that law enforcement devote more resources to learning about the new technology to understanding how it is used and, of course, in order to effectively use that, that technology has to be developed and produced in the United States.

Mr. MENENDEZ. Thank you for your testimony. Thank you, Mr. Chairman.

Mr. CAMPBELL. Thank you, Mr. Menendez. It is my turn. I have three specific questions and they are first directed to Mr. Rubinstein. This example you gave us of Zergo.

Mr. RUBINSTEIN. Yes.

Mr. CAMPBELL. Did they cooperate with Microsoft or with Netscape in developing their solution?

Mr. RUBINSTEIN. No. Let me also apologize. When I was showing those slides, I failed to show the last slide which was the download page and which listed a number of tool kits and add-on products that were available from Zergo. In no case did Microsoft supply technical assistance nor was it even asked to do so because—if I can try to explain this simply as possible—if you have a browser that is signing onto a web server, what you do is you insert two pieces of software between that communication so that the browser talks to this first piece, the first piece to a second piece, and then the second piece to the existing server. It is those two intermediate pieces that secure the communications at 128 bits. It just takes that flow and inserts this new connection and it decrypts it again.

Mr. CAMPBELL. I follow.

Mr. RUBINSTEIN. So there is no need for U.S. cooperation to accomplish that.

Mr. CAMPBELL. Although, at some point, the company, Zergo, must have access to Microsoft's code in order to—they just have to decompile what Microsoft is using in that first of the four steps in order to make a good interface, I assume.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 54 2002

Mr. RUBINSTEIN. Right, although one of the very significant changes in this whole debate that has occurred results from the fact that Internet products are built according to international standards so, regardless of the specific company implementation, as long as those standards are met, the standards are readily available. Even reference code is available on a worldwide basis.

Mr. CAMPBELL. Thanks. Let me ask a hypothetical question then of any of the panel, but particularly of the attorneys. Would it be a violation of the Export Control Act in this situation for Netscape or Microsoft to have assisted Zergo in that it—you see my question. I am not sure of the answer. You tell me you didn't. That is fine. I am pleased.

Mr. RUBINSTEIN. The answer would be yes. There is a specific provision that deals with providing technical assistance to a foreign person in the manufacture of encryption——

Mr. CAMPBELL. Thanks for answering. It was the answer I was afraid I might get. A question to Mr. Black and Mr. Smith. This is a technological question of which I am ignorant. Does the ability to deencrypt develop as the ability to encrypt or are they different disciplines?

Mr. BLACK. They are really the same coin. The skills are, there are differences but it really is the ability to do one is the same set of skills and you will find the same people able to do the other.

Mr. CAMPBELL. Would you agree, Mr. Smith?

Mr. JEFFREY SMITH. Yes.

Mr. CAMPBELL. I hit a wall in mathematics at differential equations. They didn't make any intuitive sense to me. That is when I stopped. I have a sense there is a point of complexity at which encryption can become like those differential equations so that when it goes to a certain level, the ability to deencrypt is just lost. Am I wrong or does deencryption actually follow right along with the ability to encrypt so that if we go to longer and longer bit length, we will have industry capable of eventually breaking that?

Mr. BLACK. In the real world, we have seen the development of technology that is more and more powerful and, whatever NSA says, I think many of us think they have a lot more capability than is there. But it still lags behind and lags behind substantially and I think we are—most of us think we are at point where, for all practical purposes, the ability to use brute force deencryption is just not going to be available in the future.

Mr. DAVIDSON. If you will forgive the mathematical terminology, the difficulty in decrypting increases exponentially with the increase of the bit length. So, for example, the difference between a 56-bit key and a 64-bit key, it is only 8 bits longer. But it is 256 times more difficult to decrypt in terms of the time it takes to do a brute force attack. So when you move to something like 128-bit keys, which are widely available outside of the United States, you reach a point where people start to measure the amount of time it would take to decrypt this using, technology that we——

Mr. CAMPBELL. Thanks.

Mr. BLACK. We have a number which is 256, the number of possibilities at that level equal the number of particles in the universe.

Mr. CAMPBELL. Subatomic? And 256 is 2 to the 8th power? Is that where that came from? I was wondering——

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 55 2002

Mr. DAVIDSON. 256-bit length. I think you are talking about keys that are 256-bits long.

Mr. CAMPBELL. Let me just understand the algorithm. So if you increase bit length by X bits, what is the effect on the——

Mr. DAVIDSON. Two to the X. So, for example, each bit doubles the amount of times.

Mr. CAMPBELL. That is what I thought. Two to the eighth. That is what I was asking. 256 is 2 to the 8th. You are measuring that in terms of time difficulty of deencryption.

Mr. DAVIDSON. Right. The number of steps; the number of things you have to check.

Mr. CAMPBELL. The number of steps.

Mr. DAVIDSON. It is really like doing a combination lock and trying all of the combinations.

Mr. CAMPBELL. OK.

Mr. BLACK. There is always a chance you will stumble on it right at the beginning, but you have to assume you don't.

Mr. CAMPBELL. Thanks. My last question is to Ms. PoKempner. Understand, I am entirely on your side of this. Nevertheless, it seems to me the logic of your position would oppose a universally accepted agreement, a Wassenaar that really worked, whereas every other member of the panel might be able to live with that because it would not put an American firm at a competitive disadvantage, the burden of your testimony is the value of encryption so strong that no government can break into it. Am I reading you correctly?

Ms. POKEMPNER. I am reluctant to sound like an absolutist because I do believe that there are genuine national security and law enforcement issues here, but the problem is that virtually unbreakable encryption exists. We use it. We use 128-bit encryption. For practical purposes, no one is going to break that very fast. So we live in a universe where that is already out there and my concern is that U.S. attempts to either influence the Wassanaar arrangement countries policies or its own domestic export controls ultimately have the effect of taking strong encryption out of the hands of the law-abiding people like ourselves who need to use it but don't have any deterrent effect on all of the bad guys that are constantly paraded before us as the reason for these controls.

It is a difficult equation. I think that there is a balance and a difficult judgment call that has to be made at the point where encryption becomes ubiquitous, which I do believe is an inevitability. It is just a question of whether the U.S. is going to be part of that.

At that point, obviously, computer-challenged people like myself can use it easily and so can the stupid criminals that were referred to earlier. So everyone can use it. Then you have a question of, in terms of deterring street crime versus protecting human rights activists, people who want to communicate from totally repressive situations. People who want to, preserve their privacy, their medical records, their commerce, then you have a very complicated balancing task.

But I think that is really where the level of debate should be. We are not talking about international terrorists versus, all the other interests because the international terrorists already have access.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 56 2002

Believe me, if my colleagues can use it, the international terrorists are much more capable.

Mr. CAMPBELL. I would like you to come back in another occasion and tell us what you and Human Rights Watch found in the Democratic Republic of Congo. I'm going to be polite to my colleague and yield to him in just 1 second. Though if you would be—and indulge me, Brad, I didn't speak before and I just wanted to kind of put on record my own thought. I will take about 30 seconds.

It would amaze me if the founders who wrote the Fourth Amendment were presented with Congress passing a law compelling Americans to make their communication more easily intercepted by the government. Would it not? That is, it seems to me, what we are asking. As to those who say national security and crime, I would say—and this is my one polemic, forgive me. Then I yield to my friend. My one polemic for today—I can give you safe streets, just get rid of that pesky Fifth Amendment and I will beat some confessions out of people and I will give you a safe a major city in America, every major city safe from street crime. But get rid of this warrant requirement because it is too tedious; probable cause is a heck of thing——

So it isn't that we who believe in freedom ignore the other side. We believe that our country made that compromise 200-plus years ago. I yield to my colleague from California.

Mr. SHERMAN. Mr. Chairman, thank you. Thanks especially for your technical questions. Like you, I hit a wall in mathematics. In my case, I hit it at long division.

It seems like we are confronted with three levels of criminals. There are the street criminals who aren't going to use lap tops, let alone encryption. There are the semi-sophisticated criminals who pretty much transact domestic crime—and I would like anybody on the panel to correct me if I am wrong—these folks can get all the encryption they want at the local software store today and, if they can't, it is just because you folks haven't made it yet and you will and you don't need to change the law to put really great encryption in every Egghead store in America. I see a lot of heads nodding. Then you get up to the international criminals who you would think would be sophisticated enough to send the encryption that they need over the line, buy it from a foreign source.

I am at a loss to try to figure out who we are trying to protect ourselves from. Now, as I understand it, if they get a warrant. they can look at your bank records and if you sent a message to your bank by encryption, the bank knows how to unencrypt it. I see some heads nodding. So this whole—the Administration effort is, I think, as the Chairman pointed out, an effort to make sure that when we send messages to each other we do it in a form that is most easily wiretappable and then understandable. Which is—now one could imagine that that would be argument. That we would really say we want everything that goes over the wire to be interceptable and decipherable. But that is not what we are doing. We are saying, well you can encrypt, you just can't do it internationally.

Which seems to—and I will go back to what I said before because I thought it needed a little explanation when I thought that the Administration was just trying to punish the software industry, but

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 57 2002

it seems like they are just angry that domestic messages will be encrypted in ways that they cannot decipher and the only handle they have under our legal system is to try to punish that industry or throw a temper tantrum by saying, we have got this law where we won't let you export it. I don't think there is a question in there anywhere.

Yes, my more senior colleague from California illustrated and explained to me just earlier today how I should deal with this and that is, I say, don't you agree?

Mr. BLACK. Your questioning actually earlier was, I thought very much on point where you were trying to get some people in the Administration to acknowledge that the concept of mandatory and voluntary that there is something in between which is called coercion, extortion, and that is really what we see going on. They are using the export control rules to try to force, coerce people into adopting practices because they don't want to say domestically that some people in the Administration really want to have the controls. It is really disingenuous, in our view, for them to be saying that this kind of heavy leverage, put a gun to your head, let us make a deal is not really pushing and forcing and mandating it. It is not any semblance of voluntary.

Mr. SHERMAN. Let me sneak in one more question here and then this is really the question: What would it take for a foreign company to produce encryption that works well with Microsoft and other U.S.-created products and to sell that encryption product around the world? Is there any prohibition on us importing encryption? Everybody's saying no. I do that so the record will actually reflect your head shakes. Mr. Davidson, you were about to say something?

Mr. DAVIDSON. I was going to agree with your earlier comment and say I think you are right and your second question gets to that also, which is that really what this is about seems to be an attempt to slow-down the spread of encryption. That is the best that we hope for in this policy and, to some extent, it has worked so far. I think what you are hearing from us is that now the costs of that policy far outweigh any incremental benefits of continuing it, that the costs not only to business, but to privacy interests of individuals, to the human rights workers around the world and others, you know are too high for continuing to pursue this.

But I will say one other thing which is that I think we remain concerned domestically about the ultimate goals of the Administration in this area and what I mean by that is that it was only 1½ years ago that the Administration was testifying on Capitol Hill and the FBI director was testifying that he would like domestic controls on encryption, mandatory, key recoverable, and the House Intelligence Committee, in fact, passed a version of the SAFE Act that would have imposed that.

Although it is somewhat reassuring, I guess, to hear the Administration officials say that is not current policy, we don't feel that this is far off the table. That remains our concern and I think the interchange between Chairman Gilman and the Justice Department witnesses was about domestic criminals using encryption and the only way that they are ever going to stop that is by some kind of domestic control. I think that is what we remain very fearful of.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 58 2002

Mr. SHERMAN. I would like to comment that domestic control at least has the advantage of being a logical action—I think inconsistent with the Fourth Amendment—but a logical action where you are actually achieving a law enforcement purpose other than punishing an industry for coming up with technology. I yield back.

Mr. CAMPBELL. I thank the gentleman. We are at the end of our hearing, but I would like to offer each of the panelists 1 minute, if each wishes, to add anything that he or she did not have the opportunity to add heretofore. Is there anyone who wishes to avail himself or herself of this opportunity? Mr. Rubinstein.

Mr. RUBINSTEIN. Yes. I would like to add one point which is that I think the hope of the Administration policy was that key escrow or some form of it would become so ubiquitous that everybody would use it and only the very small substratum of very sophisticated criminals would escape from that and, as the Administration readily admits, they can never really do anything about that.

But as the market has rejected that type of key escrow for reasons that Congressman Goodlatte alluded to earlier—its cost, its complexity, its vulnerability—as the market has rejected that and as the Administration has begun to soften its message on key recovery and say we are not insisting on any one technology; there are many different approaches; et cetera, the very logic of their position begins to erode because if there are no mandatory controls and if nonrecovery encryption is available overseas, then it is no longer apparent what the ongoing controls would achieve.

Mr. CAMPBELL. Read you loud and clear. Anyone else wish to speak? Mr. Davidson.

Mr. DAVIDSON. First of all I would like to say to the Chair, I think that the Chair is right about the Bill of Rights and the Fourth Amendment as it applies to this area. You are very much on point. While we will see and are hopeful about how it moves in the courts, I think that that should inform Congresses decisions in terms of thinking about encryption. I would also commend this Bernstein decision to you from the Ninth Circuit. It is quite interesting. The last thing I would just say very briefly is I am noticing that Mr. Goodlatte's attendance here at the bitter end of this hearing, and his commitment to this issue for the last several years and I would like to thank him for that because this has been very important for individual privacy.

Mr. CAMPBELL. Appropriate and so noted. Mr. Smith.

Mr. JEFFREY SMITH. One more minute to go back to a point Mr. Bereuter made about the conversations between industry and the Administration, initially done by John Deutsch when he was the Director of Central Intelligence. That dialogue has continued. I think my colleague Mr. Rubinstein made the point but I think it is important for this Committee to understand that there is a continuing dialogue, but it is a very difficult one to maintain because one is reluctant to discuss it too much in these public sessions. So I think it is something to be explored offline.

Second, to urge this Committee to take the long-run view of this policy. Our concern is that the Administration's policy is a short-term policy and our strong view is that both the law enforcement and national security interests need to be seen by Congress in the long-run and that only the kind of solution that is proposed by this

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 59 2002

bill, in our judgment, strikes the balance, gives the government what it needs, gives industry and citizens what they need.

Mr. CAMPBELL. Thank you. With that, the meeting of the Subcommittee on International Economic Policy and Trade stands adjourned.

[Whereupon, at 5:35, the Subcommittee was adjourned.]

O

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 60 2002

Document No. 32

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002