AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE THREAT OF DATA THEFT TO AMERICAN CONSUMERS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 4, 2011

Serial No. 112–44

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
70–740 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chair
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
MICHAEL F. DOYLE, Pennsylvania
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chairman
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Mary Bono Mack, a Representative in Congress from the State of California, opening statement	1
Prepared statement	4
Hon. Henry A. Waxman, a Representative in Congress from the State of California, opening statement	6
Hon. G.K. Butterfield, a Representative in Congress from the State of North Carolina, opening statement	7
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	7
Prepared statement	9

WITNESSES

David Vladeck, Director, Bureau of Consumer Protection, Federal Trade Commission	10
Prepared statement	13
Answers to submitted questions	114
Pablo Martinez, Deputy Special Agent in Charge, Criminal Investigation Division, U.S. Secret Service	26
Prepared statement	28
Answers to submitted questions	119
Eugene H. Spafford, Professor and Executive Director, Purdue University Center for Education and Research in Information Assurance and Security	37
Prepared statement	39
Answers to submitted questions	120
Justin Brookman, Director, Consumer Privacy Project, Center for Democracy and Technology	59
Prepared statement	61
Answers to submitted questions	124

SUBMITTED MATERIAL

Letter, dated April 6, 2011, from subcommittee leadership to Ed Hefferman, President and Chief Executive Officer, Alliance Data Systems, Inc., submitted by Mrs. Bono Mack	96
Letter, dated April 18, 2011, from Jeanette Fitzgerald, General Counsel, Epsilon Data Management, LLC, to subcommittee leadership, submitted by Mrs. Bono Mack	98
Letter, dated April 29, 2011, from subcommittee leadership to Kazuo Hirai, Chairman, Sony Computer Entertainment America LLC, submitted by Mrs. Bono Mack	103
Letter, dated May 3, 2011, from Kazuo Hirai, Chairman, Sony Computer Entertainment America LLC, to subcommittee leadership, submitted by Mrs. Bono Mack	105

THE THREAT OF DATA THEFT TO AMERICAN CONSUMERS

WEDNESDAY, MAY 4, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2322, Rayburn House Office Building, Hon. Mary Bono Mack (chairwoman of the subcommittee) presiding.

Present: Representatives Bono Mack, Blackburn, Stearns, Harper, Lance, Cassidy, Guthrie, McKinley, Kinzinger, Butterfield, Dingell, Schakowsky and Waxman (ex officio).

Staff Present: Paul Cancienne, Policy Coordinator, CMT; Brian McCullough, Senior Professional Staff Member, CMT; Carly McWilliams, Legislative Clerk; Gib Mullan, Chief Counsel, CMT; Andrew Powaleny, Press Assistant; Shannon Weinberg, Counsel, CMT; Michelle Ash, Democratic Chief Counsel; Felipe Mendoza, Democratic Counsel; and Will Wallace, Democratic Policy Analyst.

Mrs. BONO MACK. Good morning. The subcommittee is now in order. And I would like to start by saying that a wise person once said great challenges create great opportunities. As we begin looking into the pervasive problems of cyber attacks and data breaches, this is our subcommittee's great opportunity to come up with new safeguards against identity theft.

The chair now recognizes herself for an opening statement.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Today American consumers are under constant assault. As quickly and quietly as a wallet can be stolen by a skilled pick pocket, your personal identity can be highjacked without you knowing it by online hackers. The Federal Trade Commission estimates that nearly 9 million Americans fall victims to identity theft every year, costing consumers and businesses billions of dollars annually. And those numbers are growing steadily and alarmingly. In recent years, sophisticated and carefully orchestrated cyber attacks designed to obtain personal information about consumers, especially when it comes to their credit cards, have become one of the fastest growing criminal enterprises here in the U.S. and across the world.

The boldness of these attacks and the threat that they present to unsuspecting Americans was underscored recently by massive

data breaches at Epsilon and Sony. With 77 million accounts stolen, including some 10 million credit card numbers, the data breach involving Sony's PlayStation network has the potential to become the Great Brinks Robbery of cyber attacks, and the take just keeps going up.

While the FBI and Secret Service, along with other law enforcement agencies, work around the clock to try and crack the sensational case, we now learn that a second Sony online service was also compromised during the same time period.

Computer hackers obtained access to personal information relating to an additional 25 million customer accounts. That is more than 100 million accounts now in jeopardy. Like their customers, both Sony and Epsilon are victims, too. But they also must shoulder some of the responsibility for the stunning thefts, which shake the confidence of everyone who types in a credit card number and simply hits enter. E-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it, and that starts with robust cybersecurity.

As chairman of this subcommittee, I am deeply troubled by these latest data breaches and the decision by both Epsilon and Sony not to testify today. This is unacceptable. According to Epsilon, the company did not have time to prepare for our hearing, even though its data breach occurred more than a month ago. Sony meanwhile says it was too busy with its ongoing investigation to appear.

Well, what about the millions of American consumers who are still twisting in the wind because of the breaches? They deserve some straight answers, and I am determined to get them.

For instance, how did the breaches occur? What steps are being taken to prevent future breaches? And what is being done to mitigate the affects of these breaches on American consumers? Yet for me the single most important question is simply this: Why weren't Sony's customers notified sooner of the cyber attack? I fundamentally believe that all consumers have a right to know when their personal information has been compromised, and Sony as well as all other companies have an overriding responsibility to promptly alert them.

In Sony's case, company officials first revealed information about the data breach on their blog. That is right, a blog. I hate to pile on, but in essence, Sony put the burden on consumers to search for information instead of accepting the burden of notifying them. If I have anything to do with it, that kind of halfhearted, half-baked response is not going to not fly in the future. This ongoing mess only reinforces my long-held belief that much more needs to be done to protect sensitive consumer information. Americans need additional safeguards to prevent identity theft. And I will soon enter legislation designed to accomplish this goal. My legislation will be crafted around the guiding principle consumers should be promptly informed when their personal information has been jeopardized.

Clearly, as I have said, cyber attacks on the rise. According to the Privacy Rights Clearinghouse, over 2,500 data breaches, involving some 600 million records, have been made public since 2005. In fact, last month alone, some 30 data breaches at hospitals, insurance companies, universities, banks, airlines and governmental

agencies impacted nearly 100 million records. And that is in addition to the massive breaches at Epsilon and Sony.

The time has come for Congress to take decisive action. We need a universal national standard for data security and data breach notification, and we need it now.

While I remain hopeful that law enforcement officials will quickly determine the extent of these latest cyber attacks, they serve as a reminder as well as a wake up call that all companies have a responsibility to protect personal information and to promptly notify customers when their information has been put at risk. We have the responsibility as lawmakers to make certain that this happens.

[The prepared statement of Mrs. Bono Mack follows:]

Statement of the Honorable Mary Bono Mack
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
May 4, 2011
Hearing on "The Threat of Data Theft to American Consumers."
(As Prepared for Delivery)

Today, American consumers are under constant assault. As quickly and quietly as a wallet can be stolen by a skilled pickpocket, your personal identity can be hijacked without you knowing it by online hackers. The Federal Trade Commission estimates that nearly nine million Americans fall victim to identity theft every year, costing consumers and businesses billions of dollars annually – and those numbers are growing steadily and alarmingly.

In recent years, sophisticated and carefully orchestrated cyber attacks – designed to obtain personal information about consumers, especially when it comes to their credit cards – have become one of the fastest growing criminal enterprises here in the United States and across the world. The boldness of these attacks and the threat they present to unsuspecting Americans was underscored recently by massive data breaches at Epsilon and Sony.

With 77 million accounts stolen – including some 10 million credit card numbers – the data breach involving Sony's PlayStation Network has the potential to become the "Great Brink's Robbery" of cyber attacks. And the "take" keeps going up.

While the FBI and Secret Service, along with other law enforcement agencies, work around the clock to try and crack this sensational case, we now learn that a second Sony online service was also compromised during the same time period. Computer hackers obtained access to personal information relating to an additional 25 million customer accounts. That's more than 100 million accounts now in jeopardy.

Like their customers, both Sony and Epsilon are victims, too. But they also must shoulder some of the blame for these stunning thefts, which shake the confidence of everyone who types in a credit card number and hits "enter." E-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it – and that starts with robust cyber security.

As Chairman of this Subcommittee, I am deeply troubled by these latest data breaches, and the decision by both Epsilon and Sony not to testify today. This is unacceptable.

According to Epsilon, the company did not have time to prepare for our hearing – even though its data breach occurred more than a month ago. Sony, meanwhile, says it's too busy with its ongoing investigation to appear. Well, what about the millions of American consumers who are still twisting in the wind because of these breaches? They deserve some straight answers, and I am determined to get them.

For instance: How did these breaches occur? What steps are being taken to prevent future breaches? And what's being done to mitigate the effects of these breaches on American consumers?

Yet for me, the single most important question is simply this: Why weren't Sony's customers notified sooner of the cyber attack? I fundamentally believe that all consumers have a right to know when their personal information has been compromised, and Sony – as well as all other companies – have an overriding responsibility to alert them…immediately.

In Sony's case, company officials first revealed information about the data breach on their blog. That's right. A blog. I hate to pile on, but – in essence – Sony put the burden on consumers to "search" for information, instead of accepting the burden of notifying them. If I have anything to do with it, that kind of half-hearted, half-baked response is not going to fly in the future.

This ongoing mess only reinforces my long-held belief that much more needs to be done to protect sensitive consumer information. Americans need additional safeguards to prevent identity theft, and I will soon introduce legislation designed to accomplish this goal. My legislation will be crafted around a guiding principle: Consumers should be promptly informed when their personal information has been jeopardized.

Clearly, cyber attacks are on the rise. According to the Privacy Rights Clearinghouse, over twenty-five hundred data breaches – involving some 600 million records have been made public since 2005. In fact, last month alone, some 30 data breaches at hospitals, insurance companies, universities, banks, airlines and governmental agencies impacted nearly 100 million records. And that's in addition to the massive breaches at Epsilon and Sony.

The time has come for Congress to take decisive action. We need a uniform national standard for data security and data breach notification, and we need it now.

While I remain hopeful that law enforcement officials will quickly determine the extent of these latest cyber attacks, they serves as a reminder – as well as a wake-up call – that all companies have a responsibility to protect personal information and to promptly notify consumers when that information has been put at risk. And we have a responsibility, as lawmakers, to make certain this happens.

Mrs. BONO MACK. And now I would like to recognize the gentleman from North Carolina, the ranking member of the subcommittee, Mr. Butterfield, for 5 minutes for an opening statement.

Mr. BUTTERFIELD. Let me thank the chairman for convening this important hearing today and particularly thank the witnesses for coming forward with your testimony. Before giving my opening statements, I would yield such time as he may consume to the former chairman of this committee, of the full committee and now the ranking member, the gentleman from California.

Mr. WAXMAN. Thank you very much, Mr. Butterfield. I appreciate your courtesy in allowing me to go ahead of you in an opening statement. I must go to another committee that is meeting at the same time.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

I would like to thank Chairman Bono Mack for holding this timely and important hearing. In the last month, we have seen some serious private-sector data breaches that have affected millions of Americans. Just last week, Sony revealed that information connected to 77 million customer accounts had been compromised. And then, on Monday, Sony announced that even more consumer information was breached. Data breaches threaten the financial well-being of individuals whose personal information is exploited to commit identify theft or fraud. There is no one solution to these threats. Criminal hackers are targeting us every minute.

Today we will hear from Federal law enforcement and how they are attacking this problem. However, the private sector also must step up to the plate. The private sector can and must do a better job of safeguarding sensitive personal information.

Information is the currency of the digital economy, and it must be secured. Just as a bank would not leave its vault unlocked and open to thieves, companies must secure information and keep it out of the hands of identify thieves and other criminals. And when personal information is compromised, companies have an obligation to inform those individuals whose information was lost or stolen so that they can take steps to detect and prevent identity theft or other harm.

I am hopeful this committee can again in a bipartisan fashion pass the Data Accountability and Trust Act, and work as a team to get the Senate to follow suit. The DATA bill that was passed by last Congress creates two major security requirements: One, an entity holding data containing personal information must adopt reasonable and appropriate security measures to protect such data; and two, that same entity must notify affected consumers in the event of breach, unless the entity determines there is no reasonable risk of identity theft, fraud or other unlawful conduct.

I look forward to today's hearings and working together to quickly repass the Data Accountability and Trust Act.

I yield back the balance of my time.

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Mr. BUTTERFIELD. Let me thank you, Mr. Waxman, for your leadership on this issue and your leadership on this committee.

In preparing for this hearing today, I was told by my staff that well over 100 million consumer records have been compromised as a result of breaches at Epsilon Data Management, an e-mail marketer, and at Sony's PlayStation and online entertainment networks. If that is indeed a fact, this is very, very alarming. And so this hearing today is certainly very important.

I want to you know, Madam Chairman, that I stand ready to work with you and our colleagues to pass strong bipartisan data security legislation like the DATA bill that will prevent this from reoccurring.

I ask unanimous consent that my full statement be included in the record.

I yield back.

Mrs. BONO MACK. I thank the gentleman.

The chair recognizes Mr. Stearns from Florida for 3 minutes.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Thank you, Madam Chair. And let me also compliment you on having this hearing.

I share your disappointment that Epsilon and Sony have not shown up. Obviously, they could provide us a lot of information that perhaps some of our witnesses could not, and I think it ultimately is their responsibility to explain it.

Madam Chair, as the chairman of the Oversight and Investigation Committee I certainly would want to work with you to find out perhaps what really happened and perhaps to extend a hearing on this on my subcommittee.

Let me also say to you, this is an issue that, in the 109th Congress, when I was chair of this subcommittee, I had a bill, a data security bill, and this bill was H.R. 4127. It passed out of the subcommittee, bipartisan support. It passed out of the full committee, bipartisan support. It did not pass the House, unfortunately, and so with your leadership, perhaps we can get this through the House.

So I am very anxious to support you and help you in your endeavors to actually get a bill through the House and to the Senate. This is so important. If the data security bill that I had in the 109th Congress had actually passed, which required entities which hold personal information to establish and maintain appropriate security policies to prevent unauthorized acquisition of that data, so companies would have a data security officer, and that officer would have the mandate and the requirement to protect the information.

It was interesting that the issue is so important that bipartisan support in the 109th Congress was available. So surely, I would think we could get bipartisan support again. I know Mr. Rush, when he was chairman, he took the bill that we had, and he offered it again. And I cosponsored that bill with him. And now with a new

majority and you, Madam Chair, the chairwoman, I think this is really a very important issue for you and this subcommittee to make a stand, get the bill through the subcommittee, through the full committee and try and get it through the House.

I think a lot of people are just staggered by what has happened. And we should not delay. I think this hearing is important. I look forward to participating and also hearing their comments, but in the end, I think both parties agree that this is something that should be answered with a bill that is substantive and bring in the jurisdiction of the Federal Trade Commission and others to help us out.

So, thank you, I yield back.

[The prepared statement of Mr. Stearns follows:]

CMT Subcommittee Hearing Data Theft
By Rep. Cliff Stearns
Wednesday, May 3, 2011
156 words

Thank you, Mr. Chairman.

I am pleased this committee is having this hearing today to discuss data security, an issue I have supported and even addressed when chairing this very subcommittee. As Chairman, I introduced H.R. 4127 the DATA Act, which passed committee with bipartisan support.

Last month, I along with Rep. Matheson, introduced a privacy bill that requires covered entities to notify consumers in clear and easy to understand language that their personal identifiable information may be used for a purpose unrelated to the transaction. Covered entities must establish a privacy policy and notify consumers to any changes in this policy. Entities must also provide consumers with the opportunity to preclude the disclosure of their information to other organizations.

I understand the importance of transparency with consumers' information. Data theft needs to be addressed, and this subcommittee is taking the right steps to do so. I look forward to hearing the testimonies of our witnesses, and I yield back.

Mrs. BONO MACK. I thank the gentleman. And we would like to say that we have one panel of witnesses joining us today. Each of our witnesses has prepared an opening statement that will be placed into the record. Each of you will be given 5 minutes to summarize the statement with your remarks.

On our panel, we have David Vladeck, director of the Bureau of Consumer Protection at the Federal Trade Commission. Also testifying, we have Pablo Martinez, deputy special agent in charge of the Criminal Investigative Unit for the U.S. Secret Service. We have Dr. Gene Spafford, professor and executive director from Purdue University, Center for Education and Research and Information Assurance and Security. And last but not least, we have Justin Brookman, director of the Consumer Privacy Project at Center for Democracy and Technology.

Good morning to each of you, and we welcome you. We are very grateful that you are here with us this morning. If you can keep track of the time by the time clocks that are on the table, I am assuming.

Staff?

Oh, that is a new improvement, technology. OK, well, green, yellow and red, much like a stoplight. If you could keep your eye on it, we would appreciate it.

STATEMENTS OF DAVID VLADECK, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; PABLO MARTINEZ, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE; JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY PROJECT, CENTER FOR DEMOCRACY AND TECHNOLOGY; AND EUGENE H. SPAFFORD, PROFESSOR AND EXECUTIVE DIRECTOR, PURDUE UNIVERSITY CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY

Mrs. BONO MACK. Mr. Vladeck, we recognize you for 5 minutes.

STATEMENT OF DAVID VLADECK

Mr. VLADECK. Good morning, Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee. I am David Vladeck, director of the Federal Trade Commission's Bureau of Consumer Protection.

We appreciate the opportunity to present testimony here this morning. The written statement is submitted on behalf of the commission. This statement and my responses to questions represent my views.

As the Nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. We all know that data security is critically important to consumers. If companies do not safeguard the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm to consumers. And as more and more breaches take place, there is a risk that consumers could lose confidence in the marketplace.

As the commission's testimony makes clear, the commission unanimously supports legislation that would require companies to

implement reasonable security policies and procedures. The commission also supports legislation that would require companies to notify consumers in appropriate circumstances when there is a security breach so that consumers can take steps to protect themselves.

By enacting legislation, Congress would also send a clear message that all companies that hold consumer information, including common carriers and nonprofit organizations, must take responsible and appropriate measures to safeguard that information and must notify consumers if their information has been exposed in a breach.

A data security statute would establish the standards that companies must adhere to and, by empowering the Federal Trade Commission to seek civil penalties for violations, would deter poor security practices. These statutory provisions would reduce the incidence of identity theft and other financial harms, saving consumers from the hardships that ensue when there is a breach.

The commission's testimony also describes our efforts to promote data security, which focuses on three activities: Enforcement cases against companies that fail to provide adequate security; education for consumers and businesses; and policy initiatives to promote better data security.

Enforcement: We have brought more than 30 law enforcement actions against businesses that fail to protect consumers' personal information, including two actions we announced just yesterday. In the first case, Ceridian, a large payroll processing company that maintains highly sensitive payroll information, failed to take reasonable measures to prevent an intruder from hacking into Ceridian's payroll processing system. The hacker compromised personal information, including Social Security numbers and financial account information of approximately 28,000 employees of Ceridian's small business customers.

In the second case, Lookout Services a company offering a Web-based application to assist employers in verifying their employees' eligibility to work in the United States had weak practices in Web application vulnerabilities. As a result, an employee of a Lookout customer was able to gain unauthorized access to Lookout's entire customer database, which includes highly sensitive information, including Social Security numbers, dates of birth, passport numbers, alien registration numbers, drivers licenses, military identification numbers and so forth.

The orders entered in both cases require the companies to implement comprehensive data security programs and obtain independent audits for 20 years. Orders of this kind are standard in our data breach cases, and I underscore, we are not authorized to seek civil penalties in these cases, so we rely on injunctive relief.

The commission also promotes data security practices through extensive use of consumer and business education. For example, our Web sites designed to educate consumers about basic security, computer security, have recorded more than 14 million unique visits. And our business education touches on a wide range of issues, from P2P file sharing, which I know is of particular interest to the chair and to copier data security.

We also engage in policy actions. We published a staff report in December proposing a new framework for privacy which calls on companies to build privacy and data security into the design of goods and services, to maintain reasonable safeguards for consumer data, to limit the data they collect, to retain data for only so long as they have a legitimate business need to do so.

In closing, we thank the chair for holding this important hearing, and we look forward to working with you and your colleagues on data security. Of course, we would be happy to answer any questions, thank you.

[The prepared statement of Mr. Vladeck follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Security

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

May 4, 2011

I. INTRODUCTION

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am David C. Vladeck, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on data security.[1]

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has brought more than 30 law enforcement actions against businesses that allegedly failed to protect consumers' personal information appropriately, including two new cases yesterday. Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives. And in July, the Commission will be hosting a forum to explore the issue of identity theft targeting children. This testimony provides an overview of the Commission's efforts and reiterates the Commission's unanimous, bipartisan support for legislation that would require companies to implement reasonable security policies and procedures and, in the appropriate circumstances, provide notification to consumers when there is a security breach.

---

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several laws and rules that impose obligations upon businesses that possess consumer data. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for financial institutions.[2] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[3] and imposes safe disposal obligations on entities that maintain consumer report information.[4] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[5]

Since 2001, the Commission has used its authority under these laws to bring 34 cases against businesses that allegedly failed to protect consumers' personal information

---

[2] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[3] 15 U.S.C. § 1681e.

[4] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[5] 15 U.S.C. § 45(a).

appropriately.[6] Just yesterday, the Commission announced two new data security cases. The first involves Ceridian Corporation, a large payroll processing company that maintains highly-sensitive payroll information.[7] In December 2009, as a result of Ceridian's alleged failures to adequately protect its data, an intruder was able to hack into Ceridian's payroll processing

---

[6] *See Lookout Servs., Inc.*, FTC File No. 1023076 (May 3, 2011) (consent order approved for public comment); *Ceridian Corp.*, FTC File No. 1023160 (May 3, 2011) (consent order approved for public comment); *SettlementOne Credit Corp.*, FTC File No. 082 3208, *ACRAnet, Inc.*, FTC File No. 092 3088, and *Fajilan & Assocs., Inc.*, FTC File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment); *In re Rite Aid Corp.*, FTC File No. 072-3121 (July 27, 2010) (consent order); *In re Twitter, Inc.*, FTC File No. 092-3093 (June 24, 2010) (consent order); *Dave & Buster's, Inc.*, FTC Docket No. C-4291 (May 20, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15. 2010) (stipulated order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009) (stipulated order); *In re James B. Nutter & Co.*, FTC Docket No. C-4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008) (stipulated order); *United States v. American United Mortg.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order); *In re CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order); *In re Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *In re Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *In re The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *In re Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order); *In re Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In re Goal Fin'l., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *In re Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In re Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *In re DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *In re Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *In re Nationwide Mortg. Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *In re Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In re Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *In re MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In re Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In re Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[7] *Ceridian Corp.*, File No. 1023160 (May 3, 2011) (consent order approved for public comment).

system and compromise the personal information – including Social Security numbers and financial account numbers – of approximately 28,000 employees of Ceridian's small business customers.

The second case the Commission announced today involves Lookout Services, a company that offers a web-application to assist employers in meeting federal requirements to verify their employees' eligibility to work in the United States.[8] Within this application, Lookout maintains highly-sensitive information provided by employees, including Social Security numbers, dates of birth, passport numbers, alien registration numbers, driver's license numbers, and military identification numbers. In October and December of 2009, due to the company's alleged weak authentication practices and web application vulnerabilities, an employee of a Lookout customer obtained unauthorized access to the entire Lookout customer database.

In both cases, the Commission alleged that the companies did not maintain reasonable safeguards for the highly-sensitive information they maintained. Specifically, the Commission alleged that, among other things, both companies failed to adequately assess the vulnerability of their web applications and networks to commonly known or reasonably foreseeable attacks, such as – in the case of Ceridian – "Structured Query Language" ("SQL") injection attacks and – in the case of Lookout – "predictable resource location," which enables users to easily predict patterns and manipulate the uniform resource locators ("URL") to gain access to secure web pages. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

---

[8] *Lookout Servs., Inc.*, File No. 1023076 (May 3, 2011) (consent order approved for public comment).

Similarly, earlier this year, the Commission brought actions against three credit report resellers, alleging violations of the FCRA, FTC Act, and the Safeguards Rule.[9] Due to their lack of information security policies and procedures, the respondents in these cases allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access sensitive consumer reports through an online portal. This failure enabled hackers to access more than 1,800 credit reports without authorization. As with *Ceridian* and *Lookout*, the settlements require each company, among other things, to have comprehensive information security programs in place to protect the security, confidentiality, and integrity of consumers' personal information.

B. Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[10] OnGuard Online was developed in partnership with other government agencies and the technology sector. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have recorded more than 14 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected.

---

[9] *SettlementOne Credit Corp.*, File No. 082 3208; *ACRAnet, Inc.*, File No. 092 3088; *Fajilan and Associates, Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment).

[10] *See* www.onguardonline.gov.

For example, the FTC's identity theft primer[11] and victim recovery guide[12] are widely available in print and online. Since 2000, the Commission has distributed more than 10 million copies of the two publications and recorded over 5 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service – in cooperation with the FTC – sent copies of the Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States. Moreover, the Commission maintains a telephone hotline and dedicated website to assist identity theft victims and collect their complaints, through which approximately 20,000 consumers contact the FTC every week.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. The Commission has developed a second consumer education toolkit with everything an organization needs to host a "Protect Your Identity Day." Since the campaign launch in 2006, the FTC has distributed nearly 110,000 consumer education kits and over 100,000 Protect Your Identity Day kits.

The Commission directs its outreach to businesses as well. The FTC widely disseminates

---

[11] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[12] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

its business guide on data security, along with an online tutorial based on the guide.[13] These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. The Commission also has released articles directed towards a non-legal audience regarding basic data security issues for businesses,[14] which have been reprinted in newsletters of local Chambers of Commerce and other business organizations.

The FTC also creates business educational materials on specific topics, often to address emerging issues. For example, last year, the Commission sent letters notifying several dozen public and private entities – including businesses, schools, and local governments – that customer information from their computers had been made available on peer-to-peer ("P2P") file-sharing networks.[15] The purpose of this campaign was to educate businesses and other entities about the risks associated with P2P file-sharing programs and their obligations to protect consumer and employee information from these risks. As part of this initiative, the Commission developed a new business education brochure – *Peer-to-Peer File Sharing: A Guide for Business*.[16] More recently, we issued a guide to businesses about how to properly secure and dispose of information on digital copiers, after news reports called attention to the vast amounts of consumer data remaining on such copiers being prepared for re-sale.[17]

---

[13] *See* www.ftc.gov/infosecurity.

[14] *See* http://business.ftc.gov/privacy-and-security.

[15] *See* FTC Press Release, *Widespread Data Breaches Uncovered by FTC Probe* (Feb. 22. 2010), *available at* www.ftc.gov/opa/2010/02/p2palert.shtm.

[16] *See* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[17] *See* http://www.cbsnews.com/video/watch/?id=6412572n.

C. Policy

The Commission's efforts to promote data security also include policy initiatives. This testimony describes two such initiatives – the recent Privacy Roundtables and the accompanying preliminary staff report as well as the upcoming forum on child identity theft.

1. Privacy Roundtables and Preliminary Staff Report

In December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore issues surrounding consumer privacy.[18] Panelists at the roundtables repeatedly noted the importance of data security as an important component of protecting consumers' privacy. Many participants stated that companies should incorporate data security into their everyday business practices, particularly in today's technological age. For example, participants noted the increasing importance of data security in a world where cloud computing enables companies to collect and store vast amounts of data at little cost.[19]

Based on these roundtable discussions, staff issued a preliminary privacy report in December 2010,[20] which proposed and solicited comment on a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy

---

[18] *See generally* FTC Exploring Privacy web page, www.ftc.gov/bcp/workshops/privacyroundtables.

[19] *See, e.g.*, Privacy Roundtable, Transcript of January 28, 2010, at 182, Remarks of Harriet Pearson, IBM (noting the importance of data security as an issue for new computing models, including cloud computing).

[20] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively.

protection. The proposed framework incorporates the principles of privacy by design, simplifying the presentation of privacy choices for consumers, and improving transparency of privacy practices for consumers. In the context of data security, the principle of "privacy by design" is especially important. Indeed, consumers should not be expected to understand and evaluate the technical details of a company's data security plan; rather, reasonable security should be incorporated into the company's business practices.

As the staff report notes, privacy by design includes several substantive components related to data security. First, companies that maintain information about consumers should employ reasonable safeguards – including physical, technical, and administrative safeguards – to protect that information. The level of security required depends on the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces. Second, companies should collect information only if they have a legitimate business need for it. Because the collection and maintenance of large amounts of data increases the risk of unauthorized access to the data and the potential harm that could result, reasonable data collection practices help support sound data security practices. Third, businesses should retain data only as long as necessary to fulfill the business purposes for which it was collected and should promptly and securely dispose of data for which they no longer have a business need.[21]

---

[21] *See, e.g.,* Privacy Roundtable, Transcript of January 28, 2010, at 310, Remarks of Lee Tien, Electronic Frontier Foundation ("And having the opposite of data retention, data deletion as a policy, as a practice is something that, you know, really doesn't require any fancy new tools. It is just something that people could do, would be very cheap, and would mitigate a lot of privacy problems."); Privacy Roundtable, Transcript of March 17, 2010, at 216, Remarks of Pam Dixon (supporting clear and specific data retention and use guidelines). The Commission has long supported this principle in its data security cases. Indeed, at least three of the Commission's data security cases – against DSW Shoe Warehouse, BJ's Wholesale Club, and Card Systems – involved allegations that companies violated data security laws by retaining magnetic stripe information from customer credit cards much longer than they had a business

While old data may not be valuable to a particular company, it can be highly valuable to an identity thief.

In addition to these substantive principles, the staff report recommends that companies implement and enforce privacy procedures – including appropriate data security – throughout their organizations. This includes assigning personnel to oversee such issues, training employees, and assessing and addressing risks to privacy and security.

2. Child Identity Theft Forum

Along with periodically conducting policy reviews of privacy and security issues generally, the Commission also hosts workshops to study and publicize more specific issues. One such issue that has been in the news recently is identity theft targeting children.[22] For a variety of reasons – including poor safeguards for protecting children's data – identity thieves can get access to children's Social Security numbers. These criminals may deliberately use a child's Social Security number, or fabricate a Social Security number that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans, or even mortgages. Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks

---

need to do so. Moreover, in disposing of certain sensitive information, such as credit reports, companies must do so securely. *See* FTC Disposal of Consumer Report Information and Records Rule, 16 C.F.R. § 682 (2005).

[22] *See e.g.,* Richard Power, Carnegie Mellon Cylab, Child Identity Theft, New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers (2011), *available at* http://www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html; Children's Advocacy Institute, The Fleecing of Foster Children: How We Confiscate Their Assets and Undermine Their Financial Security (2011), *available at* http://www.caichildlaw.org/Misc/Fleecing_Report_Final_HR.pdf.

employment, or applies for student and car loans.

To address the challenges raised by child identity theft, Commission staff, along with the Department of Justice's Office of Victims of Crime, will host a forum on July 12, 2011. Participants will include educators, child advocates, representatives of various governmental agencies, and the private sector. The forum will include a discussion on how to improve the security of children's data in various contexts, including within the education system as well as the foster care system, where children may be particularly susceptible to identity theft. The goal of the forum is to develop ways to effectively advise parents on how to avoid child identity theft, how to protect children's personal data, and how to help parents and young adults who were victimized as children recover from the crime.

III. DATA SECURITY LEGISLATION

Finally, the Commission reiterates its support for federal legislation that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[23] Companies' implementation of reasonable security is important for protecting consumers' data from identity theft and other harm. And if a breach occurs, prompt notification to consumers in appropriate circumstances can mitigate any such harm. For example, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit

---

[23] *See e.g.*, Prepared Statement of the Federal Trade Commission, "Protecting Social Security Numbers From Identity Theft," Before the Subcommittee on Social Security of the House Committee on Ways and Means, 112th Cong., April 13, 2011, *available at* http://ftc.gov/os/testimony/110411ssn-idtheft.pdf (citing the Commission's support for data security and breach notification standards); FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on the topic of data security. We remain committed to promoting data security and look forward to continuing to work with you on this important issue.

Mrs. BONO MACK. Thank you very much, Mr. Vladeck.

Mr. Martinez, you are recognized for 5 minutes.

STATEMENT OF PABLO MARTINEZ

Mr. MARTINEZ. Good morning.

Mrs. BONO MACK. And would you please, excuse me, turn on your microphone?

Mr. MARTINEZ. Good morning, Madam Chair.

Good morning, Madam Chair, Ranking Member Butterfield and distinguished members of the subcommittee. Thank you for the opportunity to testify on the role of the Secret Service in cyber investigations.

In February 2010, the Department of Homeland Security delivered a Quadrennial Homeland Security Review which established a framework for Homeland Security missions and goals and underscored the need for safe and secure cyberspace.

As a vital component of DHS, we work to support the department's mission to safeguard cyberspace. Through a greater understanding of how the criminal world operates, the Secret Service has developed strategies that have a tremendous impact in terms of disrupting and dismantling underground networks. We use this knowledge of criminal networks to adapt our response to the challenges posed by financial crimes in the 21st century.

Breaking up criminal networks requires a highly coordinated law enforcement approach focused on constant innovation and tactics to meet these emerging threats. The Secret Service continually develops the technical expertise to track down and successfully infiltrate, investigate and prosecute with our partners cyber criminals who pride themselves on their knowledge and technical prowess. In many cases, law enforcement has learned the tricks and techniques that cyber criminals use to hide their identities and their crimes and in turn develop countermeasures that allow the perpetrators to be apprehended and prosecuted.

A central component of our approach is the training provided through our Electronic Crimes Special Agent Program, which gives our special agents the tools they need to conduct computer forensic examinations on electronic evidence obtained from computers, personal data assistance and other electronic devices.

To date, more than 1,400 special agents are ECSAP trained. In fact, the Secret Service values this training so highly that the basic level is now incorporated as a part of the curriculum that all special agent trainees receive at our James J. Riley training center.

The training we provide, however, extends past our agents to others in the public sector. To further address cyber crime, we continue to train State and local law enforcement through our National Computer Forensic Institute initiative.

Since 2008 the, Secret Service has provided training to 932 State and local law enforcement officials, prosecutors and judges. The Secret Service's commitment to sharing information and best practices is perhaps best reflected through the work of our 31 electronic crime task forces, two of which are located overseas in Rome, Italy, and London, England.

Our domestic and foreign partners benefit from the resources, information, expertise and advance research provided by our inter-

national network of members. The Secret Service continues to undertake complex cases that require a large investment of time and actively targets individuals who take part in criminal activities regardless of where they are physically located. To coordinate these investigations at the headquarters level, the Secret Service has enhanced our cyber intelligence section to identify transnational cyber criminals involved in network intrusions, identity theft, credit card fraud, bank fraud and our computer-related crimes.

In the past 2 years, CIS has directly contributed to the arrest of 41 transnational cyber criminals who were responsible for the largest network intrusion cases ever prosecuted in the United States. These intrusions resulted in the theft of hundreds of millions of credit card numbers and the financial loss of approximately $600 million to financial and retail institutions. These cases are complicated and directly impact the lives of millions of American citizens.

At all levels, law enforcement is also having some success in getting the legal system to recognize the seriousness of losses stemming from online financial crime. And this fact is reflected in the lengths of some of the prison sentences levied against these defendants. As a result of Secret Service's successful investigation into the network intrusion of Heartland Payment Systems, which I describe in more detail in my written remarks, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment plead guilty and was sentenced to 20 years in Federal prison.

There is little doubt that the possibility of serving 20 years in prison will provide a much greater deterrent than sentences typically seen in such cases a decade ago.

Madam Chair, Ranking Member Butterfield, and distinguished members of the subcommittee, the Secret Service is committed to our mission of safeguarding the Nation's cyber infrastructure and will continue to aggressively investigate cyber- and computer-related crimes to protect American consumers and institutions from harm.

This concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service.

[The prepared statement of Mr. Martinez follows:]

Statement of Mr. Pablo A. Martinez
Deputy Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service

Before the Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives

May 3, 2011

Good morning, Madam Chair, Ranking Member Butterfield and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the role of the U.S. Secret Service (Secret Service) in investigating and dismantling criminal organizations involved in cyber crime.

On February 1, 2010, the Department of Homeland Security (DHS) delivered the Quadrennial Homeland Security Review (QHSR), which established a unified, strategic framework for homeland security missions and goals. The QHSR underscores the need for a safe and secure cyberspace:

> "Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services and resources. We know this interconnected world as cyberspace, and without it, we cannot communicate, travel, power our homes, run the economy, or obtain government services.
>
> Yet as we migrate more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. We face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services. For this reason, safeguarding and securing cyberspace has become one of the Department of Homeland Security's most important missions." (p. 29)[1]

[1] Department of Homeland Security. (2010). *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.*

In order to maintain a safe and secure cyberspace, we have to disrupt the criminal organizations and other malicious actors engaged in high consequence or wide-scale cyber crime.

As the original guardian of the nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

Due to our extensive experience investigating financial crimes, the Secret Service participated in the President's Comprehensive National Cyber Security Initiative to raise our overall capabilities in combating cyber crime and all forms of illegal computer activity. The Secret Service developed a multifaceted approach to combating cyber crime by: expanding our Electronic Crimes Special Agent Program; expanding our network of Electronic Crimes Task Forces; creating a Cyber Intelligence Section; expanding our presence overseas; forming partnerships with academic institutions focusing on cybersecurity; and working with DHS to establish the National Computer Forensic Institute to train our state and local law enforcement partners in the area of cyber crime. These initiatives led to the opening of 957 criminal cases and the arrest of 1,217 suspects in fiscal year 2010 for cyber crime related violations with a fraud loss of $507.7 million. The arrest of these individuals prevented an additional loss estimated at $7 billion dollars and involved the examination of 867 terabytes of data, which is roughly the equivalent of 867,000 copies of the Encyclopedia Britannica. As a result of these efforts, the Secret Service is recognized worldwide for our investigative and innovative approaches to detecting, investigating and preventing cyber crimes.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software and account takeovers leading to significant data breaches affecting every sector of the world economy.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting membership of approximately 80,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell and trade malicious software, spamming services, credit, debit and ATM card data, personal identification data, bank account information,

brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

Over the years, the Secret Service has infiltrated many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraudulent proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

In both of these cases, the effects of the criminal acts extended well beyond the companies compromised, affecting millions of individual card holders in one of the incidents. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Further, business costs associated with the need for enhanced security measures, reputational damage and direct financial losses are ultimately passed on to consumers.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems. An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The Secret Service investigation – the largest and most complex data breach investigation ever prosecuted in the United States – revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server

operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working with our law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[2] The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, resulting in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, TJX and Heartland investigations, as well as the recent apprehension of Vladislav Horohorin, were possible as a result of this valued partnership. The Secret Service looks forward to continuing our excellent work together.

The Secret Service also maintains an excellent relationship with the Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force where the FBI leads federal law enforcement efforts surrounding cyber matters of national security. In the last several years, the Secret Service has partnered with the FBI on various high-profile cyber investigations.

For example, in August 2010, a joint operation involving the Secret Service, FBI and the Security Service of Ukraine (SBU), yielded the seizure of 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of 85 terabytes of data, which was eventually transferred to law enforcement authorities in the United States. The data was seized from a criminal Internet service provider located in Odessa, Ukraine, also referred to as a "Bullet Proof Hoster." Thus far, the forensic analysis of these systems has already identified a significant amount of criminal information on numerous investigations currently underway by both agencies, including malware, criminal chat communications, and personally identifiable information of U.S. citizens.

---

[2] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

The case of Vladislav Horohorin is another example of successful cooperation between the Secret Service and its law enforcement partners around the world. Mr. Horohorin, one of the world's most notorious traffickers of stolen financial information, was arrested in Nice, France on August 25, 2010, pursuant to a U.S. arrest warrant issued by the Secret Service. Mr. Horohorin created the first fully-automated online store which was responsible for selling stolen credit card data. Working with our international law enforcement partners, the Secret Service identified and apprehended Mr. Horohorin as he was boarding a flight from France back to Russia. Both the CCIPS and the Office of International Affairs of the Department of Justice played critical roles in this apprehension. Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. We are presently awaiting Mr. Horohorin's extradition to the United States to face charges levied upon him in different districts by both the Secret Service and the FBI. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

One of the main obstacles that agents investigating transnational crimes encounter is the jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our international law enforcement counterparts. Currently, the Secret Service operates 23 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

The Secret Service also commends the efforts of both the Department of Justice and the FBI in working to address the "Going Dark" problem – the widening gap between the legal authority to intercept electronic communications pursuant to court order and providers' practical ability to actually intercept those communications. The Secret Service supports the written statements made by FBI Chief Counsel Valerie Caproni before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on February 17, 2011. As stated in her recent testimony, there are significant law enforcement challenges in light of the pace of technological advancements. Cyber criminals are at the forefront of exploiting these latest technological gaps to commit crimes.

Within DHS, the Secret Service has strengthened our relationship with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with US-CERT. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

The Secret Service is committed to ensuring that all its information sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Secret Service Framework

To protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- providing computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program**, and to our state and local law enforcement partners through the **National Computer Forensics Institute**;
- collaborating with our partners in law enforcement, the private sector and academia through our 31 **Electronic Crimes Task Forces**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Cyber Intelligence Section**;
- maximizing partnerships with international law enforcement counterparts through our **international field offices**; and
- maximizing technical support, research and development, and public outreach through the **Software Engineering Institute/CERT Liaison Program** at Carnegie Mellon University.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have

received extensive training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces

In 1995, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress further directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD of DHS, the State of Alabama and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Computer Emergency Response Team/Software Engineering Institute (CERT-SEI)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program to provide technical support, opportunities for research and development and public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; to provide an opportunity to work closely with CERT-SEI and Carnegie Mellon University; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI to publish the first ever "Insider Threat Study" examining the illicit cyber activity in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS S&T, are working to update the study. An updated study, expected to be released in late 2011, will analyze actual incidents of insider crimes from inception to prosecution. The research team will share its findings with federal, state, and local law enforcement, private industry, academia and other government agencies.

Conclusion

As more information is stored in cyber space, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted.

The Secret Service is committed to safeguarding the nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Subcommittee recognizes the magnitude of these issues and the evolving nature of these crimes.

Madam Chair, Ranking Member Butterfield, and distinguished members of the Subcommittee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mrs. BONO MACK. Thank you, Mr. Martinez.

Dr. Spafford, you are recognized for 5 minutes.

STATEMENT OF EUGENE H. SPAFFORD

Mr. SPAFFORD. Madam Chair, Ranking Member Butterfield, Members of the Committee, I have been working in the field of information security for about 30 years, and I am speaking with that background and also as chairman of USACM, which is the Public Policy Council of the ACM, which is the world's largest educational and scientific computing society. And we have a number of members who work in security, privacy, and electronic data. So we have a great deal of expertise in this arena.

And our knowledge of this is that this is a very significant problem. We have seen this as a growing area of concern over a number of decades, and certainly the data that has been presented, what you have heard, what you have seen, indicates that the problem is getting worse. It is not only a national problem but, as Mr. Martinez just said, an international problem.

We would like to point out that it is a problem not only for private firms but also for government agencies. There is data that is held by government agencies and databases, and some of it is privileged information because government is in a position to collect particularly sensitive data, and that is often compromised and released.

The Privacy Rights Clearinghouse maintains a database where they track various forms of data breaches and releases. And according to their figures, it is averaged approximately 100 million records per year for the last 6 years running have been released. Interestingly, the Sony breaches this year have totaled 100 million all on their own. So we are well ahead of that record just based on those releases by themselves.

If we combine that with a study that was done by the Ponemon Institute, it indicates that for companies having these breaches, they cost approximately $214 per record to clean up after the breaches. We come up with a figure of $21 billion per year in costs to clean up after the breaches on average. And those costs are being passed on to the consumers.

Along with that, we then have all of the costs for the various fraud, law enforcement investigation, other kinds of losses piled onto that and all of the losses for unreported breaches and other losses that are unreported.

So it is possible that the losses to the American public and the American economy could be as high as $100 billion per year from these breaches.

I will note that there was a story in the New York Times today that some of the credit card fraud underground bulletin board groups are worried that the massive loss of credit cards from the Sony breach may be depressing the price, the underground price, for credit cards by a factor of 5 or 10 because it will reduce the cost on the black market trading price of credit card numbers. So perhaps there is some good to be had from the Sony breach.

Looking at the problem realistically, disclosure notification laws help at some level after the fact because it does help victims take some action to protect their identity and to protect against some of

their information being used illegally. However, it does not solve all of the problem.

Law enforcement has made some gains, but they are not adequately resourced. We certainly do not have enough in the way of forensic tools. There is more need for research there, and there certainly is a need for more law enforcement agents and resources for prosecution.

But more importantly, there are the preventative aspects. We don't have enough in the way of requirements on companies to take the preventative measures to prevent the kinds of disclosures that are occurring. In large part, that is because security is not viewed as something that returns a value. It is not something that adds to the bottom line. It takes away from the bottom line. Companies don't like to invest in security. They don't understand the risk involved by not investing in security. And those that do understand some of the risk in tight economic times are willing to play the risk. They believe they may not be hit by the problem. So when they are and they have to pay the cost, they pass that along to their customers and to the rest of society. That is where all of this large expense comes from.

So among the recommendations we have are, first of all, minimize the amount of data that is kept by these companies. Second, age the data. They shouldn't keep the data any longer than they absolutely need to. Many companies keep a great deal of data simply because they think it might be useful some day. They should have sound security practices in place, and there are a number that are known that companies don't apply. We urge you to make sure that government databases are covered equally, the same as private databases, in any regulations, so that all are covered by any appropriate regulations.

And there are a number of others that are in my written testimony. I would be happy to answer any questions, and USACM and our experts would be happy to help you in any way.

[The prepared statement of Mr. Spafford follows:]

Testimony before the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade

Hearing on *"The Threat of Data Theft to American Consumers"*
May 5, 2011

Statement of Eugene H. Spafford

Professor and Executive Director
Purdue University Center For Education and Research
in Information Assurance and Security (CERIAS)

Chair of the U.S. Public Policy Council
of the Association For Computing Machinery (USACM)

Summary of Recommendations

- A Federal mandatory notification law that includes a requirement for informing consumers about redress should be considered..
- Any regulation or statute should incorporate at least the 24 privacy recommendations listed in Appendix A (the USACM Privacy Principles).
- Any regulation or statute should apply equally to government as well as the private sector to maximize the benefit of development of software, training, and requirements, as well as protection of data.
- Our nation needs to invest in cyber forensic technologies to combat cyber crime, to support law enforcement investigation of data breaches, and to bring criminals to trial.
- Entities holding PII data should be required to meet minimum standards of good security, including staying current with software patches. No particular technology use (e.g., encryption) should be held out as a "safe harbor"; some form of appropriate third-party standards and audit should be used.
- There should be considerably more support for both fundamental and applied research in privacy and security technologies by both government and the private sector.
- As a nation, we must strengthen the cybersecurity workforce--federal programs should devote resources to improve computer science and computing education programs in K-12 as well as in higher education.

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

Introduction

By way of self-introduction, I am a professor at Purdue University. I also have courtesy appointments in the departments of Electrical and Computer Engineering, Philosophy, and Communication. At Purdue, I am also the Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we have been ranked as the #1 such program in the country. CERIAS also has close working relationships with many of other universities, major commercial firms and government agencies.

Along with my role as an academic faculty member, I have served as an advisor to several Federal agencies, including the FBI, the Air Force, the GAO, and the NSA. I have been working in information security for almost 30 years.

I am also the chair of USACM, the U.S. public policy council of the ACM. With over 100,000 members, ACM is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. USACM acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. USACM tracks U.S. public policy initiatives that may affect the membership of ACM and the public at large,

and provides expert advice to policy-makers. This advice is in the form of nonpartisan scientific data, educational materials, and technical analyses that enable policy-makers to reach better decisions. Members of USACM come from a wide-variety of backgrounds, including industry, academia, government, and end users.

My testimony is as an expert in the field. My testimony does not reflect any official position of Purdue University. My recommendations have been endorsed by USACM.

General Problem

Citizen concerns about disclosures of personally identifiable information (PII) held in computer databases is not surprising given the significant — and growing — number of reported breaches each year. Organizations are increasingly collecting data about various groups of people and storing that data in computing systems for their use in various business processes — or simply to warehouse for possible future use. However, those systems are often not adequately protected, and portions of the data are exposed by accident or stolen with criminal intent.

Data may be disclosed in a number of ways. Some disclosures are accidental, as a result of carelessness or flaws in the operation of underlying software (or rarely, hardware). Usually, the disclosures are a result of malicious behavior coupled with inadequate protections and policies. Malicious disclosure may come about from authorized employees (insiders) or customers who are taking or disclosing information, usually for financial gain. These disclosures may occur over a long time. These disclosures are often to confederates who commit the crimes using the information, thus making it more difficult to identify the

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

source of the disclosure. The resulting problems may be further complicated by delayed response, and inadequate law enforcement follow-up.

A second form of disclosure occurs when an attacker discovers some flaw or misconfiguration in the system, and uses this to gain access to the desired information. One common current method is via *spear phishing*, which occurs when a targeted piece of attack software is sent in email to a victim inside the target company, masquerading as some harmless document or application from a friend or coworker. When the attack code is run, it acts similar to a virus, installing itself on the local machine, and provides remote access for the criminal to access the system.[1] Similar types of attack code also exist that run from web pages that may be visited by employees of the company.

Attacks can also occur by exploitation of flaws in installed software. For instance, the software that drives a web commerce transaction using the SQL database language may improperly check user input given in response to a question about shipping address. A malicious user may be able to take advantage of this by inserting a semicolon followed by SQL instructions to send the entire customer database over the network to a remote site.

Theft of information is not limited to online copying of data — data exists in physical form as well as online. Thus, the fixed, physical copy can be lost or stolen as well as the online version. There are many documented cases of theft or loss of backup media (disks, tapes,

---

[1] There have been some very high-profile cases of spear phishing in the news recently. Oak Ridge National Labs had to shut down their Internet connection in April when over 500 employees were attacked like this, RSA had some of their security software compromised this spring via spear phishing, and the highly publicized breakins of Google and over 30 other large companies were accomplished with spear phishing from China.

thumb drives, CD-ROMs), theft or loss of laptop computers, and even theft of whole server machines and disks. The theft or loss of paper records may also lead to some of the same forms of disclosure mentioned here — high speed scanners can quickly convert paper documents into database files again; my university has been forced to limit what is printed in our campus phone directory, for instance, because some commercial firms were obtaining copies, digitizing them, and using the results for marketing.

Growth of the Problem

One of the more notable incidents occurred in 2005, when the data broker ChoicePoint revealed that fraudulent access to over 140,000 customer records had occurred over the previous two year period, leading to multiple instances of identity theft and fraud.[2] That incident led to investigations by the FTC and SEC, as well as multiple lawsuits.

Despite the publicity of the ChoicePoint case, and the potential for lessons-learned, the instances of disclosure and loss of PII data have only increased in the years since, with hundreds of cases per year in the United States reported — and undoubtedly many more unreported. This year, before this hearing, two very large and troubling exposures of such data were reported by Sony and Epsilon, with potentially over 100 million consumers affected by the combination of incidents.

These two cases are particularly illustrative of the complexities of such incidents. The individuals affected by the Epsilon case had no idea they had records stored with Epsilon, and

---

[2] See "The ChoicePoint Dilemma", by Paul N. Otto, Annie I. Antón, and David L. Baumer, *IEEE Security & Privacy*, Sep/Oct 2007, pp. 15-23.

likely still have no idea what the extent of their relationship is with that company.[3] In the Sony case, the majority of the victims are likely young people whose sense of risk, privacy and consequence are not yet fully developed, and thus they may also not understand the full ramifications of what has happened. Presumably, both companies are large enough that they could have afforded to spend an appropriate amount on security and privacy protections of their data; I have no information about what protections they had in place, although some news reports indicate that Sony was running software that was badly out of date, and had been warned about that risk.

To put those incidents in a different perspective, the Privacy Rights Clearinghouse keeps a database[4] of *exposed*[5] breaches from 2005 that includes both accidental disclosures and fraudulent accesses. As of the 1st of May 2011, they documented almost 600 million records have been disclosed in 2,459 separate incidents in the United States. That is an average of approximately 100 million records per year. The Sony breaches disclosed in April and May of 2011 alone equal approximately 100 million records. Other firms listed in their database for those months included Blockbuster, several hospitals, the IEEE (Institute of Electrical and Electronics Engineers) and , a restaurant in southwest Indiana, Albright College

---

[3] This is similar to the ChoicePoint breach in that the individuals affected in that incident also did not realize the relationship they had with the company.

[4] Available at http://www.privacyrights.org/data-breach#CP

[5] I emphasize *exposed* because there are undoubtedly many more that are undisclosed, and many that are also simply not discovered. There may be more that are undiscovered than disclosed and undisclosed combined.

in Reading, PA, the Hartford Insurance Company, many doctors offices, US Airways, and Apple iTunes.

Sometimes, a company is involved even though their computers are not the ones breached. Among the more than 50 companies whose customer lists were stolen in the Epsilon data breach were Chase Bank, Hilton, Best Buy, and Target. Customers of those companies should expect to receive emails suggesting that as loyal customers, they can click to receive a valuable coupon. Ironically, some possible fraud may even be in the form of warnings about fraud —customers will receive messages telling them that their email address was stolen and to protect themselves they should click on a link to enter their credit card information, or apologizing for the inconvenience and offering a discount by clicking on a link and signing in, thus disclosing their password to criminals.

It is important to note that data breaches occur in all forms of organizations: retail establishments, financial services, nonprofit entities, health care providers, public utilities, and even computer security firms themselves. Federal and state government agencies are also affected, and are sometimes responsible for disclosure of particularly sensitive material because of their privileged access status under law. A review of the aforementioned list for the last few months reveals disclosures by the IRS, a U.S. District Court, the Social Security Administration, Veterans Affairs, the Oklahoma Department of Health, the Texas Comptroller's Office, the Maine State Prison, and the town of Barton, Vermont (to name a few). Clearly, the problem of properly safeguarding personal information is not limited to the private sector.

Disclosure and theft of PII records has not abated since the ChoicePoint incident in 2005 first prompted Congressional scrutiny. More data is being collected and stored, often for less well-defined purposes. More firms have access to large-scale storage and computing, and thus are now able to store and aggregate data online. Additionally, there are more entities interested in committing fraud online, and their sophistication and reach has grown considerably faster than has that of law enforcement and security personnel in the same time. Their ability to distribute what they take has also increased with the speed and reach of networks.

Nonetheless, the increase in sophistication of attackers, and the growth in data do not totally explain all the incidents. My personal conclusion from reviews of reports in the press and discussions at professional meetings is that operators of these systems — both in government and the private sector — continue to run outmoded, flawed software, fail to follow some basic good practices of security and privacy, and often have insufficient training or support. The most commonly cited reason for these failings is cost. The cost of providing better security and privacy protection is viewed as overhead that is not recovered in increased revenue, and it is usually one of the first things trimmed in budget cuts. Running outdated software and unpatched operating systems exposes citizens to risks and consequences whose cost a company does not bear. Therefore a company does not have an immediate economic incentive to make the investment needed to prevent breaches. There is a risk of real loss if a

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

breach occurs, however: the cost to a company per record averages $214, and has increased every year since 2005.[6]

As a cautionary note for the future: many companies are eager to move their operations "into the cloud." This will mean that the PII databases may be stored on servers located outside the United States. If those servers are compromised or the media is stolen, it is unclear what legal rights and protections the victims may have.

Types of Abuse

It may not be immediately obvious why disclosure of some of this information might be of concern. In some cases, the disclosure might only be of an account name and some password hint, or directory information that might be otherwise easily found in a public directory. However, such information in context or in combination with other information can be quite damaging. The presence of a record in a database is informative — that someone is a customer, patient, or subscriber, for instance. Combining information from several different sources may allow someone to infer much more than from any single source alone (and given the availability of information on social media sites and from other breaches, this is not difficult to do).

It is then how these bits of information are used that are of concern. Certainly, any disclosure poses a privacy concern to some users, but there are additional concerns related more specifically to criminal activities.

---

[6] According to an annual study by the Ponemon Institute: http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

Identity theft. If sufficient information is obtained about someone, it is often possible to perform identity theft, thus gaining false identification for employment, obtaining credit, or evading law enforcement.

Harassment and stalking. Information about individuals may be used to harass public officials or celebrities, or stalk victims. Obtaining address information may be used to stalk spouses who have fled abuse, for instance.

Spear phishing. Phishing, the attempt to get someone to click through to a false web site through email or divulge their account information, can be made more effective if the email is tailored somewhat to the victim. This is known as spear phishing. Details from large data bases, such as account names, length of service, addresses, and account options can be used to tailor a phishing message to make it appear legitimate and thus trick someone into divulging their account information.

Tracking for physical crime. It is possible to use data from a database to identify victims for physical crime, although I am unaware of any cases of this yet occurring. This would be instances where the database would indicate something about income level or perhaps that indicated people were away on vacation, and this would be useful to criminals seeking to commit burglaries in an area.

Extortion. The presence of information in a database could be used for extortion. This has occurred in cases of medical information, particularly regarding HIV status. There are many other items of information that might be used, including past criminal violations, past marriages, or even items as simple as what videos and on-line books someone likes to

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

download. In an extreme case, some individuals open to extortion might be in sensitive positions, and this could then lead to espionage.

Inference. People tend to use the same passwords, and use the same hints for passwords when visiting multiple sites. The trend at sites to use prompts for password recovery such as "Name your first pet" elicit the same (honest) response from most people or they would otherwise not be able to remember all the answers. Thus, gaining the passwords or hint answers for users from one site might be combined with the same user name at other, more valuable sites such as a bank, to provide access for direct fraud.[7]

Direct fraud. Clearly, information containing credit card numbers, ACH numbers, or other financial information may be used directly — and usually is.

USACM Recommendations

1. **A Federal mandatory notification law that includes a requirement for informing consumers about redress should be considered.** Mandatory notification of consumers after a breach (possibly) involving their PII, along with information about steps to take to safeguard their identity appears to have some positive value. A study[8] by Romanosky, et al. suggests that state mandatory notification laws provide a small decrease (about 6 percent) in identity theft. Not all states have a mandatory notification law.

---

[7] See, for example, http://www.pcworld.com/article/188763/too_many_people_reuse_logins_study_finds.html or http://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/

[8] Romanosky, Sasha, Telang, Rahul and Acquisti, Alessandro, Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated) (September 16, 2008). Forthcoming in the Journal of Policy Analysis and Management, 2011. Available at SSRN: http://ssrn.com/abstract=1268926

2. **Any regulation or statute should incorporate at least the 24 privacy recommendations listed in Appendix A.** USACM has developed a set of 24 basic privacy recommendations for use with databases. Those are enclosed as Appendix A to this testimony. We strongly recommend that they be followed for all data sets containing PII, whether government or private, commercial or nonprofit. All of them are important to limit exposure and damage.

3. **Any regulation or statute should apply equally to government as well as the private sector to maximize the benefit of development of software, training, and requirements, as well as protection of data.** We encourage the committee to ensure that any legislation or regulation apply equally to all government data collections as well as private sector data. The dangers and risks apply no matter who collects and holds collections of PII.

4. **Our nation needs to invest in cyber forensic technologies to combat cyber crime, to support law enforcement investigation of data breaches, and to bring criminals to trial.** Law enforcement also appears to be insufficiently supported with resources for forensic investigation of computing incidents. This is another area where resources for research into better tools and technologies would be helpful. So long as the criminals do not fear apprehension, they will continue to attack our systems. There also appear to be too few agents to investigate breaches, and too few resources to ensure prosecutions.

5. **Entities holding PII data should be required to meet minimum standards of good security, including staying current with software patches. No particular technology use**

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

(e.g., encryption) should be held out as a "safe harbor"; some form of appropriate third-party standards and audit should be used.

6. **There should be considerably more support for both fundamental and applied research in privacy and security technologies by both government and the private sector.** There needs to be additional research into privacy-enhancing and privacy-preservation technologies for large data sets. This is a nascent area of research, as is much of security, and the area is under-resourced. Many of the problems being faced might be solved with better tools, software, and understanding of fundamental processes.

7. **As a nation, we must strengthen the cybersecurity workforce—federal programs should devote resources to improve computer science and computing education programs in K-12 as well as in higher education.** As companies increasingly store data in digital formats, a well-prepared cybersecurity workforce is needed. Strengthening computer science and computing education will help address security challenges in the long-run, ensuring that students have adequate knowledge of the field. The education pipeline feeding our current workforce too often focuses on training rather than education and is frequently absent in K-12 education. Expanding this workforce via education is critical and should start at K-12 and extend through our higher education system.

Acknowledgements

I wish to acknowledge comments and assistance provided to me in preparing this testimony from David Bruggeman, Cameron Wilson, Annie Antón, Sarah Granger, Emil Volcheck, Travis Breaux, Andy Grosso, Ollie Smoot, Jim Horning, Jeremy Epstein, Aaron

Massey, Paul Otto, and other members of USACM. Despite listing their names here, none of those individuals necessarily agrees with, nor endorses any of my comments or opinions.

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

Appendix A

USACM Policy Recommendations on Privacy

Background

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data — including copies of video, audio, and other surveillance — needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Council of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These

recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

Recommendations

Minimization

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.
5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

Consent

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (*opt-in*); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

information, including when appropriate, the deletion of that information (*opt-out*). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)

7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

Openness

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

Access

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.

15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.
16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

Accuracy

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

Security

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

Accountability

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

23. Maintain *provenance* — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de-identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in identifying experts and applicable technologies.

(June 2006)

1828 L Street, NW Suite 800
Washington, DC 20036

www.acm.org/usacm

202 659 9711 *tel*
202 667 1066 *fax*

Mrs. BONO MACK. Thank you, Dr. Spafford.

Mr. Brookman, you are recognized for 5 minutes.

STATEMENT OF JUSTIN BROOKMAN

Mr. BROOKMAN. Thank you, Madam Chair, in today's hearing. The Center for Democracy and Technology is extremely pleased——

Mrs. BONO MACK. Is your microphone on?

Mr. BROOKMAN. Is it on now?

Mrs. BONO MACK. Very good, thank you. A little closer, it helps.

Mr. BROOKMAN. CDT is extremely pleased to see the subcommittee is placing such a high priority on protecting consumers' personal information in an increasingly complex data economy. We very much appreciate the chair's leadership in this area.

Data security breaches are, sadly, nothing new for most consumers, but as more and more industry players get access to more and more consumer data and storage costs continue to get lower and lower, consumers, it is clear, are increasingly at risk for loss of their personal data.

Now, fortunately or unfortunately, depending on how you look at it, strong law already does exist to require companies to put into place reasonable security measures and to notify consumers in the event of a breach.

The FTC, as Director Vladeck, explained has applied its unfairness authority to require companies to adopt reasonable security measures, not just for financial information but for nonfinancial information as well. And a considerable majority of States require notification to consumers in the event of a breach that could result in a monetary loss.

I understand the subcommittee is considering legislative solutions in order to address the issues of data security and data breach. From our perspective and from a consumer perspective, we believe that Federal legislation should not merely replicate the existing protections that are out there for consumers but should be significantly strengthened to offer greater protections.

For example, the FTC's authority to get—for enforcing in poor data security practices could be put specifically into law to be more clear, but they would be stronger if the FTC were given greater resources to bring more cases and the ability to get civil penalties for persons who violate section 5 of the FTC Act.

Similarly, we believe that data breach notification laws would be improved if they were to enact the full range of full, fair information practice principles, not merely security and notification after the fact.

As an initial matter considering legislative solutions, our first advice would be do no harm. While it is clear that the existing legal framework is insufficient to protecting consumers, they do offer strong protections, without which we think consumers would be worse off. CDT has testified previously positively about the DATA act referenced by Representative Stearns. We did so because we believed it was a strong bill and, with some minor revisions, could be as strong as the best State laws, but it also offered consumers something they didn't already have, which is the rights of access to data stored by data brokers, so we thought it would be a net positive for consumers.

We believe also that whatever law is passed should allow States to continue to innovate and to bring—to pass new consumer protections for consumers. It is important to remember that it was in the laboratories of the States that the idea of data breach notification came up, because the relatively narrow precise preemption language in Gramm-Leach-Bliley, and CDT would be skeptical of any law that prohibited similar State innovations for consumer protection.

But fundamentally, we believe the most effective way to safeguard consumer data would be to enact the comprehensive privacy protection legislation that implements the full range of fair information practice principles. These do not necessarily prevent data breaches from occurring, but they would, I believe, significantly mitigate their effects. And one idea—one of these principles is the idea of data minimization. Companies should only collect the data they need to accomplish a specific purpose, and they should get rid of it when it is no longer valuable. And I think it is fair to say, as Dr. Spafford pointed out, this is really honored in the breach today. Companies request and retain data without notice to the consumers on the chance it may become valuable to them one day.

One example from the recent data breaches is I think indicative. Walgreens was hit by a data breach in 2010, in December. They had to send notices not just to current customers but also folks who have had previously unsubscribed from receiving their e-mails, and they didn't explain why they retained those e-mail addresses in the first place.

And then, just last month, as part of the Epsilon data breach, Walgreens was again hit by a data breach incident. Again, previous customers who had previously unsubscribed had their information exposed to the hackers.

Similarly, it was reported just last night that as part of the Sony online data breach incident, 10,000 credit card numbers were accessed from "an outdated database going back to 2007." I guess the good news from that is that only 900 of those credit cards numbers were still active, but it remains a legitimate question why those numbers were being stored in the first place.

And I know as a result of Epsilon data breach, I got notice from at least one company who I had not done business with in almost 6 years and who I had unsubscribed from as well.

We believe that a comprehensive privacy law that requires reasonable data minimization, that requires companies to actually tell consumers what they are doing with their data, and gives consumers meaningful choice about how that data is shared and transferred would be the most effective policy means to limit the consequences of data security breaches.

We look forward to continuing to engage with the members of the subcommittee on appropriate legislative solutions, and I look forward to your questions.

[The prepared statement of Mr. Brookman follows:]

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Before the House Committee of Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
"The Threat of Data Theft to American Consumers"

May 4, 2011

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to participate in this hearing on data breach. Members of the Subcommittee on Commerce, Manufacturing and Trade deserve praise for focusing on privacy and security issues at a time when incredible growth in the volume of consumer data is matched only by the risks that that data will be breached or misused. I would especially like to thank Chairman Bono Mack for showing leadership and commitment on the issue of consumer privacy.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. After a note regarding the scope of the data breach problem, this testimony will briefly describe the existing framework of federal and state data breach and security laws, as well as potential legislative proposals. CDT generally believes that any federal rules on data breach would best be enacted as part of comprehensive baseline privacy legislation that in no way weakens stronger state laws. Finally, this testimony will place the need for data breach rules in the broader context of long overdue baseline consumer privacy legislation.

I. Data Breach – A Longstanding Problem

At the time of this hearing, news reports are still circulating about two large recent data breaches. In late April, Sony Corp. announced that its Playstation Network had been hacked earlier that month, compromising an estimated 77 million accounts containing unencrypted personal information such as names, addresses, birth dates, login credentials in addition to potentially tens of thousands or even millions of credit card numbers.[1] On Monday night, Sony

[1] Alex Pham, Sony apologizes, says 10 million credit card accounts may have been exposed in network attack, *LA Times*, May 1, 2011, http://latimesblogs.latimes.com/technology/2011/05/sony-apologizes-says-10-million-credit-card-accounts-may-have-been-exposed-in-network-attack.html.

revealed that the breach had extended to its Sony Online network as well, taking the total number of affected accounts to over 100 million.[2] In early April, Epsilon – a major email marketing firm whose 2,500 clients include Best Buy, Capital One Financial, Citigroup, US Bank, JP Morgan Chase, Kroger, Target, Verizon and Walgreens – suffered a cyber attack that breached information on an estimated five million people.[3] The information lost in the Epsilon breach was evidently limited to the names and email addresses of Epsilon clients' customers. A recent report conservatively estimated the total number of email addresses compromised in the Epsilon breach to be 60 million.[4]

Although these two data breaches have grabbed headlines lately because of their recency, data breach is a major longstanding problem for consumers, businesses and government. According to Privacy Rights Clearinghouse, a staggering 600 million records have been breached due to the roughly 2,460 data breaches made public since 2005.[5] According to a 2010 Ponemon benchmark study, the cost of data breaches to businesses – in terms of preventing, detecting, and notifying individuals of breach, as well as legal defense and lost business opportunities – have risen considerably over the past several years.[6] Consumers whose personal information is lost or stolen in data breaches face increased risks of identity theft, spam and phishing attacks, reduced trust toward services on which they depend, and sometimes humiliating loss of privacy over sensitive medical conditions.

Given its growing scale and persistence, it is appropriate to question whether enough is being done to solve the data breach problem. Although some state and federal regulations require companies to notify affected consumers of a data breach, the financial and reputational cost of notification may not provide many companies with adequate incentive to properly protect consumers' data in the first place. Any federal action on data breach should be a mix of requirements and incentives for both companies and government bodies to install sufficient front-end data security measures, to minimize their holdings of consumer data that is no longer necessary for a specific, legitimate purpose, and to develop structures that monitor and control where consumer data resides. Finally, although data breach is an important problem, new rules on data breach would be best addressed as one part of comprehensive baseline consumer privacy legislation.

---

[2] Ian Sherr, Hackers Breach Second Sony Service, *Wall Street Journal*, May 2, 2011, http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw.

[3] Matthew J. Schwartz, Epsilon Fell To Spear-Phishing Attack, *InformationWeek*, April 11, 2011, http://www.informationweek.com/news/security/attacks/229401372

[4] Les Luchter, Epsilon Confronts Possible $225M In Data Breach, *MediaPost News*, April 29, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149603.

[5] Privacy Rights Clearinghouse, "Chronology of Data Breaches," last updated May 2, 2011, http://www.privacyrights.org/data-breach#CP.

[6] Ponemon Institute, "2010 Annual Study: U.S. Cost of a Data Breach," March 2011, http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf.

II. Existing Legal Framework for Data Breach

As of late 2010, 46 states and the District of Columbia have enacted legislation on the breach of personal information.[7] There are also several federal laws requiring notification to consumers in the event of a data breach. Although the state standards vary and the federal laws are incomplete in their coverage, most companies already do notify affected individuals in the event of a data breach as a practical matter. The great majority of data breach law focuses on notifying consumers after a data breach, without providing incentives and requirements regarding data collection and retention that could help prevent data breach from occurring in the first place.

Each of the state laws provides a general time frame in which the compromised entity must notify consumers of a breach (often simply the in the most expedient time possible and without unreasonable delay). Some states – such as New York[8] and Texas[9] – levy civil or criminal penalties on compromised entities for failing to promptly notify consumers of a breach, while other states – such as California[10] – do not. Some states – such as California,[11] but not New York or Texas – allow individuals to bring a private right of action for injuries suffered as a result of violations of the breach notification law. Most states – including California,[12] New York[13] and Texas[14] – provide for some exemption from breach notification requirements when breached private information is encrypted.

At the federal level, there are several laws and regulations requiring reasonable security and, sometimes, notification to the victims of data breach, typically containing the same basic elements of the state laws. The federal laws are something of a patchwork insofar as they cover some data in certain contexts, but not others, reflecting the sector-by-sector approach Congress has thus far taken with regard to privacy rules. For example, the Federal Information Security Management Act (FISMA),[15] the Privacy Act[16] and the Veterans Affairs Information Security Act[17] apply to the federal sector, but not the private sector. The Fair Credit Reporting Act (FCRA) applies to consumer reporting agencies,[18] the Gramm-Leach Bliley Act (GLBA) applies to covered financial institutions,[19] and the Health Insurance Portability and Accountability Act

---

[7] National Conference of State Legislatures, "State Security Breach Notification Laws," last updated October 12, 2010, http://www.ncsl.org/Default.aspx?TabId=13489.

[8] N.Y. Gen. Bus. Law 899-aa(d)(6).

[9] Tex. Bus. & Com. Code 521.151.

[10] Cal. Civ. Code 56.06, 1785.11.2, 1798.29, 1798.82.

[11] Cal. Civ. Code 1798.84(b).

[12] Cal. Civ. Code 1798.82(e).

[13] N.Y. Gen. Bus. Law 899-aa(b).

[14] Tex. Bus. & Com. Code 521.053(a).

[15] 44 U.S.C. 3541 *et seq.*

[16] 5 U.S.C. 552a *et seq.*

[17] 38 U.S.C. 5722 *et seq.*

[18] 15 U.S.C. 1681 *et seq.*

[19] 15 U.S.C. 6801 *et seq.*

(HIPAA) applies to covered health care entities.[20] Consumer data that is not covered under these laws are generally protected under the Federal Trade Commission (FTC) Act.[21]

Section 5 of the FTC Act prohibits deceptive and unfair practices in interstate commerce.[22] Although the FTC Act does not provide for notification to consumers in the event of a data breach, the FTC has at times used its authority to bring suits against for failing to adopt reasonable security procedures. In 2006, the FTC filed a complaint against CardSystems Solutions (CSS) after a hacker gained access to the credit card processing company and stole tens of millions of credit and debit card numbers.[23] The FTC complaint alleged that CSS engaged in a number of "practices that, taken together, failed provide reasonable and appropriate security for personal information stored on its computer network."[24] The FTC claimed these circumstances qualified as an unfair or deceptive practice under §5 of the FTC Act, but CSS settled quickly so the question never reached adjudication.

The FTC has recently extended its interpretation of §5 of the FTC Act to non-financial information. In 2010, the FTC filed a complaint against Twitter after security lapses gave hackers administrative control over its users' accounts.[25] Like the CSS complaint, the Twitter complaint charged that the social networking site engaged in several "practices that, taken together, failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users in designating certain tweets as nonpublic."[26] The FTC alleged that these practices qualified as unfair or deceptive under §5 of the FTC Act, though Twitter also settled with the FTC before the matter reached a court of law. CDT hopes FTC will continue to be clear that reasonable security standards apply to non-financial information, such as email addresses and accounts.

III. Elements of Future Data Breach and Security Proposals

CDT has previously testified in favor of federal data breach and security legislation. We think such legislation could be a step forward to the extent that it goes beyond just breach notification and reasonable security, which are already required under the law, to include useful new

---

[20] 42 U.S.C. 1320d *et seq.*

[21] 15 U.S.C. 45(a) *et seq.*

[22] Id.

[23] Federal Trade Commission Complaint, *In the Matter of CardSystems Solutions, Inc.*, Docket No. C-4168, September 5, 2006, http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf.

[24] The CSS practices the FTC complaint identified included creating "unnecessary risks to the information by storing it in a vulnerable format for up to 30 days," failing to asses the vulnerability of its computer network to common and foreseeable attacks, failing to use strong passwords and other readily available defenses to such attacks, and failing to employ sufficient means to detect unauthorized access to personal information. *See* FTC Complaint, *In the Matter of CardSystems Solutions, Inc.*, Pg. 2., Para. 6.

[25] Federal Trade Commission Complaint, *In the Matter of Twitter, Inc.*, Docket No. C-, June 24, 2010, www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.

[26] FTC complaint alleged that, among other things, Twitter failed to make administrative passwords difficult to guess, failed to suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts, and failed to restrict employee access to user accounts according to the needs of the employees' jobs. *See* FTC Complaint, *In the Matter of Twitter, Inc.*, Pg. 4., Para. 11.

safeguards.[27] For example, the Data Accountability and Trust Act that was introduced last Congress by Representatives Rush, Barton, Stearns, Radanovich, and Schakowsky contained provisions on consumer access to data broker files in addition to security and breach notification requirements.[28] That bill would have created a nationwide data breach notification standard, which CDT supports so long as that standard is at least as effective as the laws already in place at the state level. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. However, it is true that the current patchwork of notification standards can prove a challenge from an industry compliance perspective. In the interest of removing unnecessary compliance barriers, CDT supports the concept of a nationwide data breach notification standard. CDT believes that for a federal law to be as effective as the strongest state laws, the following elements would be necessary:

- **Appropriately-scoped preemption:** CDT has reservations about preempting state data security laws covering topics other than notification. The information security provisions of the Gramm-Leach-Bliley Act (GLB) preempted inconsistent state laws, but otherwise allowed for state-level experimentation on the difficult question of how to ensure sufficient attention and precautions with respect to data security. Any federal data breach notification regime should preserve a state's ability to come up with an idea that is truly a fresh approach. California's breach notification law, the first in the nation, was a classic example of this. Had GLB broadly preempted state privacy and data security laws, this very important legislation would not have been possible.

- **A "notify unless" notification trigger:** A notification trigger should permit notification to be avoided only when there is an affirmative determination that there exists no serious risk that personal information could be misused. In other works, the standard should be that, in the event of a breach, a company must notify unless such an affirmative determination can be made. A finding that appropriate technical safeguards prevent unauthorized access to the data should qualify as an affirmative determination that there is no significant risk is misuse.

  A "notify unless" trigger creates strong incentives for a company suffering a breach to get to the bottom of what happened –because if it can determine there is no real risk, it will not have to notify its customers.[29] A trigger that requires notification only in the event of an affirmative finding of risk would create the opposite incentive — a company might not want to investigate too closely, because finding evidence of risk would trigger the obligation to notify.

  A "safe harbor" provision that exempts companies that appropriately safeguard the data they hold through reasonable encryption will both incentivize companies to adopt better data security practices and help prevent needless consumer notification. It is important to note, however, that safeguards should not excuse notification when the circumstances of the

[27] Statement of David Sohn, Senior Policy Counsel of the Center for Democracy & Technology, before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, "Legisaltvie Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act," May 5, 2009, http://www.cdt.org/files/pdfs/20090505_data_p2p.pdf.

[28] H.R. 2221, 111th Cong. (1st Sess. 2009). Introduced by Rep. Rush, co-sponsored by Reps. Barton, Radanovich, Schakowsky and Stearns. The House of Representatives passed DATA in the 111th Congress.

[29] DATA had a "notify unless" formulation. See H.R. 2221 Sec. 3(f).

breach suggest that those safeguards are unlikely to be effective. For example, a breach involving encrypted data should generally be exempt from notification, but not when it appears that the encryption keys may have been breached as well.

- **Outside scrutiny:** Adopting a "notify unless" notification trigger is crucial. However, in the absence of any outside scrutiny of risk determinations, a company could have an incentive to err consistently on the side of finding little or no risk. Even if the affected individuals were eventually to become victims of identity theft, it would be difficult ever to trace those crimes back to the specific breach, since nobody other than the company and the identity thieves would be aware that the breach even occurred. In short, with nobody in a position to question dubious risk assessments, there could be a temptation to under-notify.

  CDT believes this problem could be greatly mitigated by requiring a company, when it determines a breach poses insufficient risk to warrant notification, to notify the FTC or other appropriate regulator and provide some explanation as to why the company believes there is no significant risk. No formal process for FTC review or approval of a company's determination would necessarily be required. Simply knowing that a brief explanation would need to be filed with the FTC, and that the FTC might respond if it spotted a pattern of behavior or otherwise became suspicious, may be all it would take to ensure that companies remain diligent in their risk determinations and weigh the inevitable judgment calls in an even-handed manner. CDT therefore recommends that any data breach law require that breaches judged to be non-risky still necessitate a submission of a brief written explanation to a regulatory body such as the FTC.

- **Strong enforcement:** A national data breach standard should allow for enforcement by the FTC and state attorneys general. The most important enforcement lever would be to provide the FTC and states the authority to levy penalties for existing data security and breach notification requirements.

- **No harm standard:** Debates about security breach notification requirements often center around whether or not notification should be required in the absence of a determined "harm" to the consumer, such as identity theft. CDT cautions against a federal framework that would limit notification to cases where particular harms or risks of particular harms can be identified. The "notify unless" formulation that CDT suggests excuses notification when there is no real risk of misuse, but does not require any showing that harm has occurred or is likely to occur. Nor does it require any analysis of what specific harms could occur; it would not say, for example, that notification depends on whether there is a risk of a particular harm such as identity theft or of a type of harm such as financial cost.

  Some companies may claim that a more narrowly focused harm standard ensures that consumers are not overwhelmed by unnecessary notices. However this argument incorrectly presupposes that the only purpose of breach notification is informing individuals of the steps they can take to protect themselves from specific threats such as identity theft. While this is in fact one purpose behind breach notification standards, it ignores the larger goal of the policy: reducing the number of data breaches by incentivizing companies to improve their data security practices. Indeed, a 2007 study of the impact of state-implemented breach laws conducted by the Samuelson Law, Technology, & Public Policy Clinic at the University of California, Berkeley found that "regardless of the risk of identity theft and alleged

individual apathy towards notices, the simple fact of having to publicly notify causes organizations to implement stronger security standards that protect personal information."[30]

As for federal security legislation, CDT believes that the numerous settlements achieved by the FTC demonstrate that Section 5 of the FTC Act already requires companies to implement reasonable security protocols to protect consumer data. We encourage the FTC to continue to aggressively bring data security enforcement actions, including cases around the treatment of non-financial consumer information, as in the Twitter settlement.[31] In order to make the FTC's actions more effective, CDT has long recommended equipping the FTC with stronger tools to protect consumers, such as greater resources and the ability to recover civil penalties.[32] We believe legislation granting the FTC such additional capacity could be potentially the most effective measure to incentivize companies to adequately safeguard consumer information. CDT would be skeptical of legislation that mandated specific technological data security solutions; such mandates would quickly become outdated as technologies change, and would not encourage (and may deter) companies from innovating new responses to evolving security threats. However, CDT is supportive of general reasonable security requirements as part of a comprehensive privacy law, in order to put to rest any doubts about the FTC's authority to require as much under its §5 unfairness authority.

IV. Future Data Breach and Security Proposals Should Be Part of Baseline Privacy Legislation

CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and off-line. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. The Subcommittee should recognize that, from a consumer perspective, even a good federal breach notification requirement does not by itself offer much tangible progress over the status quo, since notification is already effectively the law of the land. To be of real benefit to consumers, data privacy and security legislation must include some additional protections. What is needed more than security and notification requirements is a data privacy law that incentivizes and requires companies to collect only as much personal information as necessary, be clear about with whom they're sharing information, and expunge information after it is no longer needed.

Fair Information Practices (FIPPs) must be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The most recent formulation of the FIPPs by the Department of

---

[30] Samuelson Law, Technology, & Public Policy Clinic, "Security Breach Notification Laws: Views from Chief Security Officers," University of California-Berkeley School of Law, December 2007, http://www.law.berkeley.edu/files/cso_study.pdf.

[31] *See* FTC Complaint, *In the Matter of Twitter, Inc.*

[32] Statement of Ari Schwartz, Deputy Director of the Center for Democracy & Technology, before the Senate Committee on Commerce, Science, Trade and Tourism, "Reauthorization of the Federal Trade Commission," September 12, 2007, http://old.cdt.org/privacy/20070912schwartz-testimony.pdf.

Homeland Security offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation.[33] Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

Although data security, individual access to personal information, and notification of breaches are important safeguards under the FIPPs, it is crucial that baseline consumer privacy legislation not give short thrift to the other FIPPs, such as data minimization. Companies should collect only that data which are directly relevant and necessary to accomplish a specified purpose, and data should only be retained for as long as is necessary to fulfill a specified purpose. Unlike breach notification, data minimization is a pre-breach remedy and should be an obligation of all companies that collect personal information. Requiring companies to get rid of unneeded consumer data would reduce the impact of data breaches, and potentially result in fewer targets for identity thieves.

For example, in December of last year, the drug store chain Walgreens experienced a data breach incident, and sent notifications not just to current customers, but also to persons who had previously unsubscribed from Walgreens email lists.[34] Even though those persons had elected to terminate their relationship with Walgreens, the company retained those person's email addresses for undefined purposes. Four months later, Walgreens' customer data was again compromised as a result of the Epsilon security breach. Again, the company sent notifications to prior customers who had unsubscribed from Walgreens marketing lists.[35] While it is admirable that the company in both cases informed previous customers about the potential exposure of their data, it remains unresolved why the company retained that data in the first place. Our current legal framework has failed to require or even encourage companies to adopt data minimization procedures, and we therefore believe that requiring reasonable data minimization would result in less consumer information being exposed through data security breaches.

Comprehensive privacy legislation should also provide consumers with reasonable access to the information that companies possess about them. When companies collect, maintain, and transfer personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy

---

[33] U.S. Department of Homeland Security, "Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[34] Bob Sullivan, Hackers steal Walgreens e-mail list, attack consumers, *MSNBC Technolog*, December 10, 2010, http://technolog.msnbc.msn.com/_news/2010/12/10/5624759-hackers-steal-walgreens-e-mail-list-attack-consumers.

[35] Dissent, "Why unsubscribing might not have protected you from the Epsilon breach," PogoWasRight.org, April 5, 2011, http://www.pogowasright.org/?p=22239.

and misuse, and also provide needed transparency to consumers about the wide range of entities that possess and use information about them.

As data flows have grown more complex, companies must have safeguards in place to monitor them. The fact that major data breaches continue to occur demonstrate that current practices for collecting and storing consumer data have outstripped the practices for keeping it safe. The most effective solution will not lie in an isolated effort to apply encryption to data or to quickly notify consumers of a data breach. Rather, the law should provide companies with a range of incentives and requirements that encourage them to establish internal privacy policies that seamlessly protect data throughout the data's lifecycle.[36] A comprehensive data protection framework coupled with strong enforcement is that solution, and for this reason CDT is has previously testified before this Committee in support of the flexible, forward-looking BEST PRACTICES Act[37] introduced by Representative Rush. CDT looks forward to working with both chambers to improve the bills and enact strong privacy protections for American consumers.

V. CONCLUSION

CDT would like to thank Chairman Bono Mack for calling this hearing on such an important topic, and for the opportunity to testify today.

For more information, contact Justin Brookman, justin@cdt.org at (202) 637-9800.

[36] Center for Democracy & Technology, "The Role of Privacy by Design in Protecting Consumer Privacy," January 28, 2010, http://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy.

[37] H.R. 611, 112th Cong. (1st Sess. 2011).

Mrs. BONO MACK. Thank you very much, Mr. Brookman.

The chair now recognizes herself for 5 minutes for the first round of questions.

I would like to start with Mr. Vladeck. According to reports, Sony took nearly a week before notifying consumers—customers about the cyber attack. How long does a typical company that has been subjected to a data breach need before it notifies its customers? And what is the average time that is necessary to make a determination and to inform consumers that their information may have been breached?

Mr. VLADECK. We share the concern I think of everyone in this room; the consumers need to be notified as promptly as possible. There are two practical exigencies that sometimes delay notification. One, there is a need that the company patch whatever hole there is in their system before the breach is made public. And second, it sometimes takes the company some time to understand what information has been accessed and who needs to be notified of the breach. We think this should happen as soon as practical, and in the prior legislation, for example, there was an outer limit set at 60 days. I don't know whether that is the right date or not.

I can't answer your question about common practices. Data breaches vary so much that it is hard to extract a general rule. The smaller the breach, typically the quicker the notification can go out. But in a massive breach where the company may still be trying to patch up its system if it is still operating—and Sony, one of the systems was not—you do worry about notification before the company has had an opportunity to plug the hole. But I think that we all would agree that consumers need to be notified as swiftly as possible so that they can take action to protect themselves.

Mrs. BONO MACK. Thank you.

Mr. Martinez, a couple of questions, can you briefly explain to me the difference from why the FBI might be involved as opposed to your agency?

Mr. MARTINEZ. Yes. The statute most used to prosecute cyber criminals is 18 U.S.C. 1030, which is a computer fraud statute. The Secret Service shares concurrent jurisdiction with the FBI on those types of investigations.

However, with investigations that deal with national security or terrorism that are cyber-related, the FBI is the lead agency in those efforts. And for the NCIJTF, they lead the government or law enforcement's efforts in state-sponsored or national security type investigations. We have a representative there.

When it comes to criminal matters, we have concurrent jurisdiction, so it is—a lot of times it depends on the relationship that either the specific company might have with either law enforcement agency, whether it is through some type of working group or task force or cyber task force where that company might reside. So, for example, the Secret Service has 29 domestic electronic crime task forces, and one of the things we ask our people to do is develop those relationships with these private-sector companies so that that relationship is there prior to the incident happening. The last thing we want is for that sort of when the fire goes off, that is the first time you meet the firemen. We want there to be a relationship, and there are a lot of things that we both, us and the FBI,

do with private-sector companies to try to develop those points of contacts prior to an intrusion happening.

Mrs. BONO MACK. As I understand it, though, you are involved with Epsilon but not with Sony. Can you explain that to us briefly?

Mr. MARTINEZ. Yes. Unfortunately, we can't comment on ongoing investigations. I can't comment on the Sony investigation because that is being lead by the FBI.

All I can say with regard to the Epsilon investigation, because it is still ongoing, is that they did notify us early on in the investigation and have cooperated so far with the Secret Service in that investigation.

Mrs. BONO MACK. Thank you, Mr. Spafford—excuse me, Doctor. Can you speak a little bit to Mr. Vladeck's answer about notification for consumers within—I think we are puzzled with the 60-day time line. To me it seems reasonable that the consumer should know immediately, that there is no greater protector of one's own identity than the person himself. Can you speak a little bit to the 60-day time line?

Mr. SPAFFORD. Well, after an intrusion or breach has occurred, it is necessary to find out—after an incident has occurred, it is necessary to determine what records have been accessed to determine who needs to be contacted and what information was possibly taken to be able to inform the individuals what information might be at risk and perhaps give them information as to how to protect that.

Unfortunately, not every organization keeps the kinds of records that would allow them to determine that. It is also often the case that when evidence has been found that some kind of incident has occurred, that doesn't necessarily tell them how long that incident has been ongoing. They just detect that it has happened, but they don't know how far back it goes. So they have to very often pull records, do so forensic investigation. It may take a while to determine how many people, how far back the records go, how much data it takes, and that is not something that can occur instantaneously.

Mrs. BONO MACK. Excuse me, Doctor, I am sorry to cut you off, but I have run out of time, so we will come back to a second round of question.

The chair recognizes Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. I thank the chairman.

In the last Congress, the House passed H.R. 2221, the Data Accountability and Trust Act. We all know that. This bipartisan bill has built up widespread support across Congress for its goal of reducing the number of data breaches and providing new rights to individuals whose personal information is compromised when a breach occurs.

First question to Mr. Vladeck: Sir, if H.R. 2221, if it is passed into law and it gives the FTC new authority and responsibility, can you talk for a minute about the limitations you are under now with regard to information security and how such a law, if enacted, could strengthen FTC's hand with regard to breaches?

Mr. VLADECK. Thank you, yes.

It would strengthen our hand in at least three ways. First, I think the key insight in the proposed legislation is that it would

for the first time erect a national standard requiring businesses that hold sensitive personal information to take reasonable and rigorous safeguards to protect it. And so, for one thing, there would be a congressionally dictated standard by which we could judge the performance of companies that hold onto personal information.

Second, there would be a national breach notification standard, which would encompass a broad range of companies who may not be subject to all State and other laws. It would cover a broader range of activities.

And third, we would have civil penalty authority. At the moment, we can place companies that have failed to protect consumer information under order to ensure that they don't violate consumer privacy again. But that doesn't involve general deterrence. It doesn't send a signal to other companies that they have to step up to the plate and protect consumer information.

Mr. BUTTERFIELD. Thank you.

Let me direct it to Mr. Brookman.

Mr. Brookman, I agree with you that we need more front-end data security measures, so that the need for breach notification actually diminishes. Your written testimony discusses support for 2221 for that model and the need for proper incentives for industry to take data security seriously. Can you elaborate more for me? Are you suggesting that the incentive be fear of enforcement?

Mr. BROOKMAN. Yes, I think that is a very important incentive. I think in Dr. Spafford's testimony, he talks about how companies just don't——

Mrs. BONO MACK. Excuse me, Mr. Brookman. Would you please——

Mr. BROOKMAN. I apologize. Companies don't think about this very seriously in advance. The FTC has somewhat on an ad hoc basis said that their prohibition on unfair practices means that it is the case that companies must exercise reasonable security. I am not entirely sure how well that has sunk into corporate America. Even more recently, they have expanded their concept of data security, not just to financial information but to things like e-mail addresses instead. And that was in their what I think was a very strong and important settlement with the Twitter case.

I would like to see H.R. 2221 or whatever it looks like in the next iteration to expand their concept of personal information, not just to financial information but to other potentially personal information as well, such as e-mail addresses or else things like the Epsilon breach actually wouldn't be affected by it. Companies should have to have reasonable security measures in place to do that. I think the FTC is getting there. I think with sporadic enforcement just merely because of limited resources is not entirely clear to the rest of the world that is in fact the law. Putting it into law I think would be an important thing, especially with the threat of civil penalties behind it to give it a punch.

Mr. BUTTERFIELD. Well, let me ask you this, how do we ensure that a company is holding on to personal data as long as necessary? Each company has different needs; how can we measure that?

Mr. BROOKMAN. Yes, it is a very tricky issue. This is one of the criticisms of the Boucher-Stearns privacy bill—draft privacy bill

that came out last year. It prescribed a hard 180-day or maybe an 18-month cap on holding all personal data. And some companies were like, that makes sense for us; maybe in behavorial advertising, that is a good idea. Data brokers, maybe not; maybe they should have to maintain the data for longer. So we have supported a safe harbor model for legislation such that companies who have similar business interests can get together and propose for our industry, hey, let's all agree to hold onto data for 180 days, 6 months, couple weeks, depending on the scenario, so they don't feel at a competitive disadvantage to hold onto data just because their competitors might be doing the same thing.

Mr. BUTTERFIELD. All right. Let me go back to the other end. What about Hill Newspaper CQ Today reported earlier this week that the White House proposal on cyber security will be circulated later this month. The article explains that it calls for a Federal standard for notification about data breaches and a stronger role for the Department of Homeland Security. Special Agent Martinez, what role would the Secret Service have, if you know, and what other agencies at DHS would have a role?

Mr. MARTINEZ. Sir, the Secret Service, along with other executive agencies, has been working with the administration on a comprehensive cybersecurity legislation. And specifically in the area of data breach, I think a couple of things that that legislation needs to have is notice to consumers but also notice to the government, so that we can take appropriate actions. And also some type of safe harbor provision for companies that are adhering to the right practices.

In addition to the enforcement part, which would be handled by the Secret Service as part of the Department of Homeland Security, the National Protection and Programs Directorate of DHS where US–CERT and the NCSD and some of the other cyber entities sit, like the national cyber security division, they would also be involved in cyber intrusions in part with respect to the——

Mr. BUTTERFIELD. Five seconds left.

Mr. Vladeck, what role would FTC have, if you know?

Mr. VLADECK. Well, we would hope we would have authority to enforce data breaches as we currently do, to enforce failures to inform consumers promptly of data breaches, and we would hope we would get civil penalty authority——

Mr. BUTTERFIELD. Thank you.

I yield back.

Mrs. BONO MACK. I thank the gentleman.

And the chair recognizes the vice chair of the subcommittee, Ms. Blackburn, for 5 minutes.

Mrs. BLACKBURN. Thank you.

And thank you all for being here I appreciate that we are having this hearing today. I think one of the things we can all agree on is that giving consumers the tools that are necessary to protect their virtual you, if you will, their virtual online presence, is going to be an imperative.

Mr. Brookman, you just spoke to this in your brief comments.

I want to go to Dr. Spafford, if I could. I appreciate that you start with recommendations to us and basically summarize things. I think that the thing that is of concern to me is when it comes to

notification, it basically looks as if what is happening is a culture of damage control by not doing these expediently. And I think we all realize that the technology is there for almost instant notification and allowing individuals to know.

Now I am one of those that would prefer to see the industry move forward with some best practices and some standards on how to deal with not only the data security issue but also the privacy issue. And whether you are looking at the Epsilon case or the Sony case or the Android aps, the Skype case this week, what we see is an intrusion and an invasion into an individual's privacy because of a breach that has taken place in a relationship that they have.

Dr. Spafford, moving to your recommendations on page 16 of your presentation, basically what you are saying is minimize the data, age the data, provide anonymity to the consumer, and then you get down to talking about consent. Let's move to that and talk about that for just a second. When you have consumer consent, should you also allow a consumer an eraser switch so that if the company does not eliminate the data, then the consumer has the ability to go in and say, you know, whether it is 90 days or 180 days, that they can remove their data? Where—is that a recommendation that you all would consider workable or plausible?

Mr. SPAFFORD. It depends upon the organization. There are some circumstances where the information may need to be kept and the user may not be able to remove it because of—there may be other reasons, for health reasons for instance, or there may be contractual reasons that it really needs to be kept, but that certainly could be something that—for commercial reasons, marketing reasons, the user may have that right or should have that right to have that removed.

Mrs. BLACKBURN. OK, all right.

Mr. Martinez, we have—we continue to talk about companies being breached. And I find it so interesting that we don't talk as much about penalties for the hackers and those that are actually the cyber snoops in committing these crimes. And it seems like that is what gets moved to the bottom of the conversation. And I would like to—for you just to talk a little bit about that. You mentioned the computer fraud statute, but it seems as if the perpetrators of the crimes, the hackers themselves, is where we should put more of our emphasis.

Mr. MARTINEZ. Thank you. In recent years, we have really seen an increase in the amount of sentencing that these hackers are getting. For example, in the TJ or the Heartland Payment Systems case, TJX, we saw a sentence of 20 years for that individual. Recently, in another case that we recently did, an individual was sentenced to 25 years.

We believe these actions are having a deterrent factor, and one of the reasons we believe so, for the last 2 years, we have collaborated with Verizon business on the data breach investigative report that talks about not only data breaches investigated by the Secret Service but also those that Verizon businesses responded to. One of the things we have seen and it is mentioned in the study is that we are now seeing these criminals—in the past, they had always attacked financial services type companies because of the large volume of financial information they had, like processors and financial

institutions. What we see now as the main targets are the hospitality and the retail industry. And we believe the reason for that is because of the deterrent factor that some of the sentences are having.

So, for example, instead of trying to breach into a system that has 150 million financial accounts, they are going now after 10 or 12 smaller ones that have smaller amounts because of the fact that they might face a higher sentence were they to be apprehended for the larger breach. So we believe that these sentences have increased and are having some form of a deterrence.

Mrs. BLACKBURN. I know I am out of time. I will look forward to a second round.

Mrs. BONO MACK. I thank the gentlelady.

And the chair recognizes Ms. Schakowsky for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Madam Chairman.

Dr. Vladeck, you mentioned the need for a civil penalty authority to protect consumers. I am wondering if you have seen a draft of a civil penalty authority. There was discussion earlier I think about the White House proposal on cybersecurity that is going to be circulated this month. Do you know if there is a draft of a civil penalty authority?

Mr. VLADECK. I know there is a draft. I don't know how far along the drafting is. I know that at least in that draft there is authority for us to assess civil penalties of the appropriate cases, yes.

Ms. SCHAKOWSKY. Have you any expectation on when you might see that draft?

Mr. VLADECK. None.

Ms. SCHAKOWSKY. OK. So you have just heard that that includes——

Mr. VLADECK. We have been shown a draft, and that draft did contain a civil penalty provision.

Ms. SCHAKOWSKY. So you have seen a draft.

Mr. VLADECK. Yes, a draft, but the process is ongoing.

Ms. SCHAKOWSKY. That was my question. OK.

Let me also ask any of you this, I am a cochair of a House Democratic task force on seniors, senior citizens, and I am particularly concerned about cyber criminal attempts to prey on older Americans. And I wonder if any of you could speak to that threat and to any efforts that are being made to protect, particularly vulnerable people, like seniors.

Mr. VLADECK. If I may, we have seen a spike in prize and sweepstake scams aimed at senior citizens. I was in Chicago on Monday. One of your staff members was at our hearing, and it is quite clear that scammers are targeting the elderly, defined as people over 60, which worries me a little.

Ms. SCHAKOWSKY. Are you taking it personally?

Mr. VLADECK. I am taking it very personally. Targeting people of that age group for particularly prize and sweepstake scams. This is all on the Internet, and increasingly there is a phishing element. There is a spear phishing element. They know something about that person that makes the scam particularly appealing. We are working with our colleague organizations to do both public information and to do enforcement work in this area.

Ms. SCHAKOWSKY. Is it the scam itself that they are after, or are they looking for information about the individual? I mean, are they trying to get people to pay money to participate in a sweepstakes or both?

Mr. VLADECK. Both. And what they often do is say you have won a million dollars; you just need to pay a penalty—you just need the taxes or a customs fee, and they will often send a fake check. It is cashed, and then the person who has been scammed sends, typically wires, money abroad. They never see obviously their winnings, but they are out whatever the value of the check was.

Ms. SCHAKOWSKY. Thank you.

Let me finally ask a bit about Sony and the security breach, the information breach there was.

Professor Spafford, I know you don't have any specific knowledge about what Sony did or did not do to protect the personal information that it collected from consumers, but in your testimony, you say, "Some news reports indicate that Sony was running software that was badly out of date and had been warned about that risk." And I have seen some news reports about the Sony breach, and truthfully, it seems like a lot of them come from blogs and press releases from Sony. So this is the first time I am really hearing about the potentially outdated software and ignored warnings.

Sony was actually invited today but declined to appear, and Epsilon declined the subcommittee's invitation to testify as well. So I am just wondering if you can discuss the problems with that software and any of the information that lead to you make that statement?

Mr. SPAFFORD. On a few of the security mailing lists that I read, there were discussions that individuals who work in security and participate in the Sony network had discovered several months ago while they were examining the protocols on the Sony network to examine how the games worked, they had discovered that the network servers were hosted on Apache Web servers. That is a form of software. But they were running on very old versions of Apache software that were unpatched and had no firewall installed, and so these were potentially vulnerable, and that they reported these in an open forum that was monitored by Sony employees but had seen no response and no change or update to the software.

Ms. SCHAKOWSKY. How long ago was that?

Mr. SPAFFORD. That was 2 or 3 months prior to the incident when the break-ins occurred.

Ms. SCHAKOWSKY. Thank you. I yield back.

Mrs. BONO MACK. The Chair recognizes Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Madam Chair, and I certainly appreciate you holding this very timely hearing on this topic. And I certainly appreciate the witnesses being here to give their insight.

And Dr. Vladeck, the first question I would have for you is, you know when you look at the expense that many companies go through to try to put in a system that is secure and works—and let's say that it is—how long can we say that it will remain secure as technology improves and changes? And with that, is there a set time period that it would need to be updated, or is it just an as-needed. And what do you recommend in that situation?

Mr. VLADECK. We provide a lot of advice to businesses on our Web site. And businesses use that, those resources, constantly. But our basic advice is inventory what you have, assess risks, don't collect information you don't need. For the information you do have—and this going to Sony— protect against viruses, spyware, constantly be vigilant to make sure the patches you need to put in place are installed promptly, discard information when you are done, and put someone in charge. This is an ongoing, dynamic process.

And one of the things I think, the key insights of the first piece of legislation, Mr. Stearns' legislation, was the need to start building an infrastructure to protect data. And that is an ongoing process. You can't check it every 6 months, like you might do the oil in your car. It is something you need to be vigilant about.

Mr. HARPER. As you look at what you are working on, how do you coordinate and keep in synch with all of the State attorneys general on what they are trying to do and what you are trying to do? How do you coordinate that?

Mr. VLADECK. I think when there are data breaches, we generally take the lead on investigations. Many States have requirements that consumers be notified. But they don't investigate and then take action when the breach was the result of, in our view, truly substandard data security measures.

But we do keep the States informed. We recently settled a case against Lifelock for data security violations, as well as others, and in that case we coordinated with 35 State attorneys general. But in terms of the hardcore investigation, I think the key is that we take the lead on those.

Mr. HARPER. Mr. Martinez, on both the Epsilon and Sony matters, I know you are limited on what you can tell us, but can you tell us how long it took from the time the breach was detected until the time consumers were notified? Is that something you can share?

Mr. MARTINEZ. I am not sure. Again, we didn't investigate the Sony intrusion or are not investing it. And on the Epsilon, I am not sure what that information is. I can get back to you.

Mr. HARPER. And when we are looking at all of the breaches, we certainly—the first thought we have is that it is going to be somebody who is there for financial gain, to access the account info, the personal info, or perhaps sell that data to someone. How much of it would you say is directly attributable to terrorist activity as opposed to what we consider the basic criminal?

Mr. MARTINEZ. Unfortunately, sir, all of those matters are handled by the FBI. So I think that would be a question better answered to by them.

Mr. HARPER. And certainly I know that it goes to the FBI, but you know there is the whole of all of the breaches, so what percentage do you think comes to you and what percentage goes to the FBI? I mean, that would be my question.

Mr. MARTINEZ. With regards to criminal?

Mr. HARPER. How much of it would you say of the overall pie is related to terrorist activity?

Mr. MARTINEZ. Again, I couldn't speak to what percentage is related to terrorist activities. I believe there are a lot of the intru-

sions and a lot of the ones that this committee has been talking about today are criminal in nature.

Mr. HARPER. Mr. Brookman, I know we are about out of my time here, but we talk about—we certainly hear in the news what has been detected. We know what we learn, what goes out in the press. What would you imagine—I know it is just speculation, but what would you imagine goes undetected?

Mr. BROOKMAN. I mean, most of the State data breach laws really only require notification in the event of a chance of financial breach. And the States vary. Some of them say notify, unless you can pretty much prove that nothing went wrong. Some of them require some thought that there might be harm. And if I lost my credit card, if I was a business and lost my credit card numbers, I really have no reason to know those were used. So I think those go undetected.

I think a lot of the things like what happened with Epsilon, because it is personal information, it is not financial information, there is no requirement for those companies to come out and say, Hey, we lost your e-mail address; and, to the contrary, are intended not to do that. So I think a lot goes on under the radar that we don't know about.

Mr. HARPER. I yield back.

Mrs. BONO MACK. The Chair recognizes Mr. Stearns for 5 minutes.

Mr. STEARNS. Thank you, Madam Chair.

Mr. Vladeck, when I did the bill in the 109th Congress, I think there were probably less than 30 States that had passed data security legislation and now there are 46, I am told. What I am curious, it would seem to me with almost the entire United States adopting—each State adopting legislation—wouldn't that be incentive enough for companies like Sony and Epsilon worrying about their reputation and the civil litigation—I mean, why would this occur, based upon 46 States already having legislation?

Mr. VLADECK. Well, I think there are two reasons. One is the State laws do not do what you propose, which is to require good, underlying security. And to me, one of the key insights of your legislation was that we need to do that on a national basis. Congress needs to step in and say to people, holding companies, holding on to sensitive consumer legislation, Look, you need to take reasonable security measures.

The second is, and as the statistics today have sort of driven home, there are an awful lot of data breaches that have been made public. I am not sure the reputational hit these companies take necessarily is strong enough general incentive to make them step up to the plate.

Time and again, we investigate substantial companies and we find very outdated, outmoded, and insecure practices. And so I think the proof is in the marketplace. There are still, by my measure, way too many breaches, and breaches caused by the kind of failures that Dr. Spafford is talking about, failure to patch known vulnerabilities. In the Ceridian case, the vulnerability there was well known to the company, there were free patches available, and the company quickly acknowledged that it had been asleep at the switch.

Mr. STEARNS. We had in our legislation, Federal preemption. We worked out the language. Jan Schakowsky was the ranking member so it was bipartisan.

How would you change that bill from the 109th Congress, coming out of this subcommittee? Would you have Federal preemption again in the bill and would you also change it in any dramatic way?

Mr. VLADECK. Well, let me say two things. One is the Commission is generally supportive for preemption. That is, the Federal standard should be the floor, States should be free if they saw fit to provide——

Mr. STEARNS. Because right now in these 46 States, a company like Sony could be sued in 46 States.

Mr. VLADECK. That would be true. I think regardless, but I would also point out that the civil cases involving security breaches have not fared particularly well.

But in terms of the bill that emerged last year, we were generally supportive, but we would prefer, as Mr. Brookman has suggested, to expand the definition of "harm." One concern was the definition of harm referred to financial loss or other unlawful acts. It would not have covered geolocation data, information about health status, or, for example, information about children. And we think that the concept of harm needs to be broadened to reflect the kinds of breaches that we have seen and the kinds of concerns that we think are broadly shared.

Mr. STEARNS. One of the things that I was struggling with is: So a corporation sets up a data security officer to do that. How do you make sure that that data security officer is complying, and is there a frequent way that you could do it? And I thought through the free market, you could have something like accounting firms that would just on their own, develop to say we will come in and do private audits.

But the question is how much should the government get involved to make sure that that data security officer is actually complying with Federal Trade Commission requirements; because everybody will say—the janitor could be the national security officer, the elevator operator. Bingo, we are all done. But how do we as legislators and you as the jurisdiction ensure that that is actually happening?

Mr. VLADECK. I mean your auditing illustration is a good one. When we put companies under order, we require them to develop a very detailed privacy policy to appoint a responsible official which we hope has the credentials of a Dr. Spafford and not a janitor. And we have outside firms that are qualified to do this audit every 2 years to make sure the company is living up to its promise.

And as an enforcement tool, if there is a chief privacy officer who is required to ensure the plan is being implemented, if there is another breach, I suspect that not only would we sue the company but we might sue the responsible official. In that case, it would be the chief privacy officer.

So there are ways of holding people accountable. One of the insights of the bill is you need somebody responsible within the company. And we think that is very important.

Mr. STEARNS. My time has expired but, Madam Chair, if there is somebody else on the panel that would like to comment on my questions. Is that possible? Mr. Martinez, Dr. Spafford, Mr. Brookman.

Mrs. BONO MACK. We are going to have a second round to be more fair to the more junior members to allow that in the second round.

So the Chair recognizes Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you very much. Thank you for being here today on this important hearing and thank you, Madam Chairwoman, for holding this.

This is really to both Mr. Vladeck and Mr. Martinez. The core of the problem, is it typically improperly secured information from people who are holding the data, or is it the criminal networks that are just a step ahead? They figure it out. Somebody could be vigilant in what they are doing and somebody just figures out a way around their system.

What are you seeing? Is it just sloppy corporate side, or data holders, or is it the other? I know it is probably a combination of both. What do you see the most?

Mr. MARTINEZ. Yes, sir. It is a combination of both. I will just real quickly go through some of the statistics on this recent study that we just did with Verizon business. Ninety-two percent of the attacks were not highly difficult, and 96 percent of their breaches were avoidable through simple or intermediate controls. I think our panel members here have told you—have brought up a lot of recommendations. So a lot of times it is that some of these security measures that should be in place just aren't fully implemented.

And although we do have criminals that are highly sophisticated—and we have seen the amount of attacks due to hacking increase—a lot of these attacks, though, could have been avoidable had just best practices been applied.

Mr. GUTHRIE. So you are saying that 96 percent I know essentially could have been avoided if it had been reasonable and rigorous?

Mr. MARTINEZ. Correct.

Mr. GUTHRIE. Is that the same?

Mr. VLADECK. I don't know that I would quantify it that way, but many of the breaches that we see are due to laxity or just foolishness. For example, we have sued both Rite Aid and CVS for taking patient employee records and throwing them into unsecured dumpsters. You don't need to be a smart criminal to go dumpster diving.

But we have seen also sophisticated hacks of the kind Mr. Martinez is talking about. And in those cases, we do an investigation, but we don't pursue civil enforcement because, you know, we don't want to be playing "gotcha." This is not a strict liability regime.

Mr. GUTHRIE. I guess the question is, if you have a standard of reasonable and rigorous, and there is somebody always getting a step ahead through technology, then you always have to update your reasonable rigorous.

But it sounds like you could eliminate over 90 percent of the problems we have had just by having a reasonable policy in place.

I guess you are saying it is being stored. Obviously throwing stuff in a dumpster is not reasonable. But you are seeing clear differences.

Mr. VLADECK. But also not applying the patches that the company is sending you to fix a known vulnerability, in our view that is not any different than leaving the door of the vault right open.

Mr. GUTHRIE. FTC—and you are doing consumer education, I know, as a part of this. But this is a little outside of this, but it is a little bit within the realm of what we are talking about. The other day I got a phone call: "This is your bank. We have had a problem with your account. Give us your account number" and whatever. Of course, I hung up. But a lot of people don't. And this is what Ms. Schakowsky is talking about. And particularly I guess he is somebody that I know elderly that would—oh, I have got to fix my bank account, and all of a sudden there is something.

Are you focusing on that area? Is that your area? What are you doing?

Mr. VLADECK. Yes and yes.

You know, we are principally the antifraud agency and that is the kind of classic fraud that we are fighting every day. And there are an awful lot of people who have taken advantage of the economic downturn. People are more vulnerable to fraud when they are in financial jeopardy. And there are fraudsters that are out in force taking advantage of the most vulnerable. And that is what we spend a lot of our time on.

Mr. GUTHRIE. If I have a few seconds left, I will go back to Mr. Stearns.

Dr. Spafford, in your testimony you are talking about the cost of the breach. I guess my question is, as a business, if the cost is going to be so expensive, why wouldn't I invest up front? Is the problem that the costs on the business are up front, but the cost of the breach is spread out like societal? Is that the issue? When you said $214 per breach, that is not borne by the company. Is that societal? I think you said $214. I didn't write it down.

Mr. SPAFFORD. The cost was a result of the study that was done. And that cost was per record, $214 per record.

Mr. GUTHRIE. Cost in the company that allowed the breach to happen?

Mr. SPAFFORD. Yes. To the company. That cost was cost of notification, cost of cleanup, cost of outside auditors, legal costs.

Mr. GUTHRIE. So businesses are not aware of these costs? Seems like if I was a business and that was my liability—I mean, I am wondering why they are not going in that direction.

Mr. SPAFFORD. That is correct. The businesses don't realize what it is going to cost them.

Mr. GUTHRIE. Or they have a known cost here and hopefully not another cost there.

Mr. SPAFFORD. That is correct.

Mr. GUTHRIE. Mr. Stearns, I don't know if you got time.

Mr. STEARNS. I thank the gentleman for his courtesy. I will wait for the second time around.

Mrs. BONO MACK. I appreciate that, gentlemen.

And the chair recognizes Mr. McKinley for 5 minutes.

Mr. MCKINLEY. Thank you, Madam Chairman.

I am curious about this whole issue, because I have not been a victim that I know of. Have any of you four been victims of a breach?

Mr. VLADECK. Yes.

Mr. BROOKMAN. Yes

Mr. SPAFFORD. Yes.

Mr. MARTINEZ. Yes.

Mr. MCKINLEY. All four of you.

How does a company know that it has been breached? Do the lights go on?

I mean, I had a real life before I came to Washington, and we had a firm with a hundred employees. Would our IT person have seen a breach? Would he have seen something flashing? How do we know we were breached? You all keep talking about these larger companies. What about the real America, the small businesses?

Mr. BROOKMAN. Before I joined CDT, I worked for the New York Attorney General's Office and I worked in the Internet Bureau. And in conjunction with the Consumer Fraud Bureau, we would get these notifications from smaller companies that said, oops, we lost a lot of data. In our experience, a lot of it was we lost a computer. Maybe even a half was like someone put their computer in their car, and this is not just small companies too, this is how the Veterans Affairs famous breach happened. Someone put a lot of data in the laptop, left it in the back seat of their car with the window open, and someone took it. And they don't know. There is a very strong chance in that scenario the person wouldn't look for the file and know what to do. But the fact of the matter is you have a large number of consumer records that are gone now to someone who does have access to it, and you don't know how they are being used.

Mr. MCKINLEY. Yes.

Mr. SPAFFORD. Another possibility is that someone comes in in the morning and they discover in the record on their system that it has been accessed from an account in Eastern Europe or China or South Africa. And that person has downloaded megabytes' worth of information off the system, including the entire customer database, and that is certainly not someone who has legitimate access to the system.

Mr. MCKINLEY. How do you know they have access?

Mr. SPAFFORD. Because there is a record of it. There is an audit trail of that information.

Mr. MCKINLEY. Every small company would have that?

Mr. SPAFFORD. Not every company, but some would. So there is a record, and the company, if they turned on that record— or it is possible that a business partner or someone else would say we found a copy of your entire customer record on our machine, and how did it get here? Somebody must have left it here. And so you often discover this because it got out and somebody found a copy of it.

Mr. MCKINLEY. I am still not clear on that. I am going to have to live with this a little longer and maybe ask more questions every time. I still think what I have heard were a lot of larger firms, a lot more records; but smaller firms are—I am trying to understand what their point is, because I have never—not that I know of,

knock on wood—have been breached, so I don't know what they are looking for and I don't know with our former firm what type of security we have for that.

But I think it was at the end you said something about if you have been breached, and the notification that the consumers take appropriate action. What is appropriate action? It has happened. Are they supposed to get a new credit card or what are—what is appropriate action for the 70-year old lady on Main Street if somebody notifies her; what action is she supposed to take? Do they tell her.

Mr. VLADECK. Generally the breach notifications do tell her what action to take. And our Web site and others provide that basic information.

Mr. MCKINLEY. They are not going to go to your Web site.

Mr. VLADECK. The breach notification should tell her what action to take. So if someone has hacked e-mail addresses, she will be alerted that she may get these e-mails from her bank asking her to provide account information. These are phishing attacks. I don't think they would be described in those technical terms. But I think she would be warned if there was credit card information—she may be told to look at her account information, to engage in credit monitoring where they may be—or the company might provide credit monitoring for her.

There are steps people can take to minimize the risk of loss. And one point of data notification or breach notification is to provide individual notice to every consumer about what the appropriate steps that consumers should take to protect his or her interest.

Mr. MCKINLEY. Thank you. Whatever this bill comes out, I hope there are some ways to get down to the grassroots level how we can deal with this.

Mrs. BONO MACK. Thank the gentleman.

Round two, I recognize myself for 5 minutes.

Dr. Spafford, your testimony supports legislation that would apply to all entities that collect personal information, including the government. Do you think the government is ahead, equal, or behind the private sector in data security practices, and what about universities and nonprofits also in that regard?

Mr. SPAFFORD. I think the government and many nonprofits have good security in some places and very poor security in others. I have testified at hearings in previous years for losses of information at the Veterans Affairs. There was an occasion there where it was just mentioned, laptops being lost. There have been occasions where databases have been breached, even in the military, and information taken. There have also been a number of cases where the systems are very well protected.

At universities, some are very well protected, some are wide open, and student records are regularly disclosed. Charities, businesses, it is across the board. Some are very good; some, unfortunately, are not.

Mrs. BONO MACK. Thank you.

Mr. Brookman, as the subcommittee knows, we submitted a letter to Sony, and we have the responses as of late last night. And I looked at them this morning to share something with you that they do have in their letter to us.

We asked them about new security measures. They responded they are implementing new security measures that include—they have added automated software monitoring and configuration management to help defend against new attacks; they have enhanced levels of data protection and encryption; they have enhanced ability to detect software intrusions in the network. And Mr. McKinley was asking, and they have also included in that, unauthorized access and unusual activity patterns. But if these are just a few of the new safety precautions, my question is, given how many consumer records were at risk, why weren't these measures in place before?

Mr. BROOKMAN. I think that is an excellent question. As I said in my testimony, it just boggles my mind that they are leaving open access to the 2007 database of credit card information that apparently they weren't even using. It just happened to be a legacy system. This is something the FTC said a lot of good things about. A lot of times, it is more expensive for a company to go in and erase data than leave it lying around.

We, in talking to the companies, have tried to get them to use privacy by design and security by design to build these concepts into products from the ground up. But sadly, in so many places it is not someone's job to go up and delete legacy data.

I was very interested in the suggestion of Vice Chair Blackburn about the idea of an eraser button. I think it is a very strong idea. If I have a direct relationship with a company and I want to end my relationship, I should be able to delete that data. I think it is a very strong idea, recognizing Ranking Member Butterfield's idea that it is hard for Congress to, say, keep data for so long because it really varies across industries. Giving consumers the power to say, Hey, go ahead and delete that now I think it is a very good idea.

Mrs. BONO MACK. Dr. Spafford, you were speaking of the vulnerability that was known to many, I guess, via the blogosphere somewhere. I am assuming you are speaking about the San Diego facility, that some speculate there was a breach, or they are saying it was an AT&T service center in San Diego where there is a known vulnerability. But if there are known vulnerabilities, what do we do with the policy that minimizes these sort of physical locations and vulnerabilities?

And I think my question would be better directed to Mr. Martinez or Mr. Vladeck about known vulnerabilities in a system and our ability to protect those physical locations that have—again, known to the bad guys, but it seems we are always sort of behind the bad guys in our limits to stop them from what they are doing.

Mr. MARTINEZ. Like I stated earlier, a lot of times what we see when we do investigations. And again, this collaborative study that we have conducted, what it shows is that 96 percent could have been avoidable through simple intermediate controls meeting. If there were a hundred servers that the company owned, they possibly patched 99 of them but forgot to patch that last one. So an instance like that one could create the havoc that we see.

Mrs. BONO MACK. So you are saying it is all corporate responsibility at that point, correct?

Mr. MARTINEZ. What I am saying is no matter the size of the company or who it is, you really have to be diligent in your systems. It is not about being compliant for that moment. You have to maintain that diligence and maintain and monitor your system on that constant basis.

Mrs. BONO MACK. Mr. Vladeck, with my remaining 25 seconds, I think it is important you spoke to the concept of harm. And I think it is critical, and I think people don't understand what it means to have been hacked or have your personal information stolen until it has happened.

You mentioned geolocation, your kids and health records. Can you speak a little bit more about the vulnerabilities beyond somebody might just buy something on my credit card? I think people need to understand what the crimes could be.

Mr. VLADECK. I don't know whether these would be crimes, and that is why we are concerned about the definition that was in 221. One harm was other unlawful action. But, for example, Eli Lilly, in one of the first cases we did, sent out an e-mail blast which associated particular patients with Prozac. Now, that is a reputational harm that I think most people would like to avoid. They don't know whether Eli Lilly committed a crime. But people ought to be notified in those kinds of circumstances. It just struck us in CVS and Rite-Aid, they were dumping prescription records in dumpsters. People ought to know when that happens, even if the act of dumping them is not a crime.

Geolocation data could be used for stalking. It could be used for other purposes.

And so when the committee reexamines this legislation, we urge them to take a somewhat broader view of what constitutes harm in this area.

Mrs. BONO MACK. Thank you.

The chair recognizes Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you.

Technology evolves rapidly, and what is cutting-edge technology today is obsolete tomorrow. The Sony press releases have stated that consumers' credit card information was encrypted. In addition, Sony stated yesterday in The Hill newspaper that passwords were protected using a hash function, and described as a shortened version of full encryption.

The data breach provision in the bill that we passed last year established a presumption that no reasonable risk of harm exists following a breach if the data is encrypted.

Dr. Spafford, do you agree or disagree with that?

Mr. SPAFFORD. Sir, I disagree, because it is possible that disclosure could also include the password necessary to decrypt those passwords, and that would mean that they could then be decrypted and read as well.

Encryption all by itself is not a solution. It has to be such that encrypted material can also not be read.

Mr. BUTTERFIELD. Are there any technologies that you believe can be given such a presumption?

Mr. SPAFFORD. Certainly there are. There are some forms of encryption that could be appropriately used if the key material is kept separate, for instance. But one has to look at the overall risk

of whether or not the protected material would be disclosed if that material were breached.

Mr. BUTTERFIELD. Of course, encryption has its downside, but do you still believe it is the gold standard?

Mr. SPAFFORD. Some kinds are. Some forms of encryption can be broken fairly trivially. Some forms of encryption are fairly good and some are not. And some previous versions—in some previous versions of legislation that were introduced in this committee, we have sent letters about problems with encryption. And I would be happy to provide copies of those to you later.

Mr. BUTTERFIELD. Special Agent Martinez, in your testimony you describe a strong working relationship with the FBI which, you state, works through the National Cyber Investigative Joint Task Force to lead the Federal Government's response to online national security threats. Now, I imagine that there is some fuzziness around cyberthreats to businesses, and that some of these could also be threats to national security. That is probably part of the reason why there is a task force and why your agency is involved. I understand that businesses, not the government, own most of the network computer infrastructure. It is the private sector that controls and is responsible for vast swaths of the network, of the financial system, power generation, and our electricity grid.

Given your experience in dealing with intrusions into private sector computing assets, is the private sector doing enough to guard the security and integrity of networked computers?

Mr. MARTINEZ. I think there is always more that we can do, sir. I think from what you've seen today, from some of the testimony today, and from some of the intrusions that we are actually discussing, there is still a lot more that needs to be done. And I think what is important is that the public sector needs to collaborate with the private sector in making sure that we improve our security.

Mr. BUTTERFIELD. Would you extend that to the Federal Government?

Mr. MARTINEZ. Yes, and I believe there are already steps that have already been taken within the Federal Government to do that.

Mr. BUTTERFIELD. Special Agent, in your testimony you also described your relationship with the United States Computer Emergency Readiness Team. According to your testimony, that group defends against cyber intrusions on the dot.gov domain and shares information and collaborates with State and local governments and industry.

Insofar as you participate in partnerships and information sharing with businesses, can you please describe this relationship a bit more?

Mr. MARTINEZ. Yes. And I think it would be better explained by U.S. Serve. They have taken the role of remediation and mitigation, so when there is an incident that occurs, a lot of times what we will do is we will encourage the private sector partners to reach out to U.S. Serve so that they can come up with a mitigation plan or best practices and so forth.

I would say in the last year or so, we have really improved our efforts trying to do that, working with U.S. Serve and having them take the lead in remediation and mitigation efforts after intrusion.

Mr. BUTTERFIELD. All right. Thank you. I yield back.

Mrs. BONO MACK. The chair recognizes Mr. Stearns for 5 minutes.

Mr. STEARNS. The gentleman from North Carolina makes a good point. When you look across the Federal Government, it is almost a sector-by-sector approach in dealing with the government. I know serving on the Veterans Affairs, there were breaches of huge, in number of veterans, when a computer was taken home and the information was breached.

The staff has pointed out that there are examples for the Veterans Affairs, they had the Veterans Affairs Information Security Act, but that just applies to the Veterans Affairs. You had the Federal Information Security Management Act which, again, is sector by sector. So a thing that this committee would have to struggle with is also how to go about deciding what would apply to the Federal Government.

Mr. Vladeck, do you think there should be a small business exemption for this, because I heard from—a lot of small businesses say, I don't want the overlay of a data security officer; and how much is this going to cost me? It is more regulation.

So the question is, is there a possibility that a small business of, let's say, less than a hundred employees, less than 50 employees, there would be sort of a modified approach, or do you think the whole thing should apply to them, too.

Mr. VLADECK. I think we need to separate out the various requirements of the legislation. We did not support a small business exemption from the data security requirements. We thought that——

Mr. STEARNS. That was crucial.

Mr. VLADECK. That was crucial. What we did support was rulemaking for the Commission to determine when small businesses should be granted waiver from the provisions relating to the payment for monitoring credit reports following a breach. And I think that was the objection raised by small business at the time. And we favored some flexibility that would be determined after a public rulemaking, and perhaps exemptions would be authorized pursuant to that rulemaking.

Mr. STEARNS. Dr. Spafford, there is some some talk about cloud computing here in the House, and we no longer have our servers and hard disks and so forth. If a company moves toward cloud computing storage, is that more safe or less safe, in your opinion, keeping the servers proprietary and protected?

Mr. SPAFFORD. It depends on where the cloud storage is and how well it is protected, because you are putting your records on computing resources that are stored somewhere else and protected by someone else. If you have a private cloud, then that is within your corporate domain or within Congress here, protected here. But if you are using it outsourced, you may not even know where it is and how it is protected.

A concern that I mention in my testimony is that some cloud service providers may actually have their storage located outside

the country. And so if that storage is compromised, we have a whole new set of problems, because now that storage is now outside——

Mr. STEARNS. We don't really have reciprocity laws with countries outside, so it gets more difficult.

Mr. SPAFFORD. It gets considerably more difficult.

Mr. STEARNS. So if the information is breached, then where do people go to sue? I guess you would still go to the holding company of the major corporation.

Mr. SPAFFORD. That is beyond my area of expertise. Mr. Brookman or Mr. Martinez or anyone else want to comment on this cloud computing?

Mr. MARTINEZ. Yes, sir. Think of it this way. The crime scene now, like Dr. Spafford just said, the crime scene now does not become the server farm located at a building in a crime scene. Now, part of it could be in the Philippines, part of it could be in Mexico, and part of it could be in Los Angeles. So it makes it much more difficult for law enforcement to take action and obtain that information. Specifically when we have to go overseas, now there is a whole other trigger of requirements or things we need to do, such as Mitchell legal assistance treaties, and the question then becomes do we have treaties with countries where some of this information resides?

Mr. BROOKMAN. I would just say in response to that, I think in many cases it may well be the case that a cloud computing server will offer better privacy and security for you. Especially in the case maybe of the small business who doesn't have a technical know-how of how to protect this data or what the latest cutting edge in encryption techniques are. I think in that scenario, it may well make sense, maybe some marginal significant security benefits from using a third-party service provider. On the other hand, in the recent news, the Epsilon was a third-party provider whose job was knowing how to do mass marketing, and obviously it is not a fail-safe.

Mr. STEARNS. Yes.

Mr. VLADECK. I just wanted to say that we have encountered this issue already in our enforcement efforts. And our position is that U.S. companies, when they are storing data involving U.S. citizens or U.S. transactions, they are responsible to us even if the date is stored in a cloud computer offshore. And we have made that quite clear.

We haven't tested in the courts. But we are quite confident that we would be able to assert our authority in those kinds of instances. I think Mr. Martinez' concerns may be more complicated than ours.

Mr. STEARNS. Thank you, Madam Chair.

Mrs. BONO MACK. Thank you gentleman.

The chair recognizes Mr. Lance for 5 minutes.

Mr. LANCE. Thank you, Madam Chair. And good morning to the panel.

Dr. Spafford, in its letter to the subcommittee, Sony said that it acted with care and caution. And I am wondering if that is the case, why wouldn't Sony notify consumers as soon as it shut down its network.

Mr. SPAFFORD. Well, sir, I don't have full access to all of the details of what was required for them to gather the information as to what happened to determine what individuals were involved and what law enforcement needs were involved for them to gather evidence before notifying people.

Certainly they also were in a state where they had to be sure that they had closed all of the vulnerabilities before notifying individuals, I would assume. And so those factors probably introduced a lag into the notification.

Mr. LANCE. Is there anyone else on the panel who might be willing to comment on that? I know it is speculative. Is there anybody else who would be interested in commenting on that?

And another area. Agent Martinez, in its letter, Sony also says that it believes it has identified how the breach occurred. From your perspective and your expertise, why do law enforcement officials need a window of opportunity, so to speak, to investigate a data breach before consumers are notified?

Mr. MARTINEZ. Sir, I can't speak specifics to the Sony. I can tell you based on our experience in previous cases, there could be times where, through an operation that we are actually conducting an active investigation, we actually are the ones who find the breach and report it to the company. So in certain instances, we work with the company, and a lot of States have enacted the delay in notification for law enforcement purposes, because what we don't want to have happen is something the company does could impact the investigation and then possibly hurt the investigation and not allow us to apprehend the individual.

But what we always do is work with these companies. And in instances where we do need some form of delay in notification, we try to minimize that as much as possible so the company can make the notification it needs.

Mr. LANCE. I yield back the balance of my time to you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman. I will graciously take you up on your 2-minute and 30-second offer.

Mr. Dingell is on his way down here, and I would like to ask questions until he gets here, so he can participate.

But I want to say this has been a very insightful hearing. And each member has brought up I think different complexities in understanding how they see these problems.

Ms. Schakowsky, when she specifically brought up the threat to seniors, I hadn't thought about that. The Sony Play Station, we all thought about perhaps a little bit younger generation and the risks to them. And I want to reiterate, although she is not here, I will continue to work with her and explore the senior angle, and with the FTC as well.

And I want the thank and congratulate the members who have worked on this legislation previously, and certainly we have come a long way. 2005, I don't know many people were talking about cloud computing, and yet we are today.

So I think understanding briefly the cloud, the FTC will have the authority to go out at servers that are based offshore. But do we also risk over-legislating in sending more offshore if we are not careful?

I will go to either Mr. Martinez or Mr. Vladeck.

Mr. VLADECK. I don't think, frankly, this legislation is going to affect cloud computing. I think companies are migrating to the cloud. I think servers are networked to the point where the physical location of the server is much less important than the kind of security it provides. And the legal regimes I think will adapt.

So we have not gotten pushback from companies that we have investigated where there was an issue about whether the data was physically within the United States territory or not.

In Ciridian, Ciridian is a global company. And we ended up settling the case in a way that makes it crystal clear that its accounts for U.S. companies or for other companies that are employing people in the United States are covered, regardless of where physically the computer may be, where the server may be.

Mrs. BONO MACK. Thank you. Briefly. I just had a great question.

Dr. Cassidy, do you have a question immediately for the panel?

Mr. CASSIDY. I do.

Mrs. BONO MACK. The chair recognizes Dr. Cassidy for 5 minutes.

Mr. CASSIDY. I don't know quite who asked this. I was in another committee hearing, so I apologize if somebody has already answered this.

Let me start with Mr. Brookman. Mr. Brookman, I am driving to my in-laws. There is a wreck; pop open my cell phone, and it tells me the congestion on the freeway. It is pretty impressive. Then I read an article—to show how broad-minded I am—on MSNBC's Web site about how this location data is apparently stored forever. I am sitting there thinking, well, that is great, I can see where I am at any given time, and if there is a red zone up ahead and I need to get off on a side road. On the other hand, why should whomever, Google or Apple, keep this forever? What thoughts do you have?

Mr. BROOKMAN. There are definitely wonderful secondary uses of location data that Google and Apple all use this for. I think the map example is a great example. There are ways to do that that are not privacy-invasive. They have to remember that it is me for a little bit, so they have to see it is my car stopped on the Beltway, moving 5 miles per hour. But they can forget that after an hour, and there are things they can do to not have to remember that it is me, my entire life.

I think the recent Apple story about storing location information up to a year resident on your phone, for what seems to be a marginal performance improvement and to increase battery life, I think it is a great example of maybe not thinking through privacy by design. And the concept from the beginning, this engineer thought, Hey, it would be a great idea if you had all of the cell towers that are nearby you stored in the phone, so if—instead of checking back to Apple to say, Where am I, you can check back to your phone, not really thinking this is kind of a permanent log of everywhere I have been in the last year, that I might not want someone like a hacker or someone to get their hands on.

I think a lot of companies have taken the idea of location permission seriously, so I am glad that Android and Google and Microsoft

and RIM phones, they do ask, Hey, is it cool to use your location right now? I still think they are working through some of the secondary usage issues because you can create really detailed logs about people in ways they would not expect.

Mr. CASSIDY. OK. Now I am insensitive to it, and I am looking at my phone and I am logging onto a map, and there pops up that sort of, you know, "Click here after you have read 16,000 pages of legalese to proceed." But this time I actually read a little bit of it. And this is totally optional, and all I was doing was giving them permission to store my data. Sure, it gives them the patina, the fig leaf of being careful about my data, but in reality it was a trick. I was thinking that this is, you know— I am not going to, whatever, rip-off their copyright, but indeed it was, no, we can sacrifice your privacy.

So what kind of protections? Put it this way. I am just coming across this because I am driving in Mobile, Alabama. But I am assuming the people on the Commission have thought about this. What is the best way to address this?

Mr. VLADECK. There are two responses. One, for the purposes of data security, we have already discussed what we think would be an important amendment to the prior legislation, which is to talk about geolocation data, the disclosure of geolocation data as a result of a breach, as a harm that would trigger the notification requirements. Because if your geolocation data where you have been for the last 2 years——

Mr. CASSIDY. Which, by the way, I am not defensive of, just to be sure of that.

Mr. VLADECK. No implication at all. You ought to be notified of that.

Mr. CASSIDY. Do we need legislation that says, Thou shalt not keep this beyond X number days?

Mr. VLADECK. The Commission is very concerned about geolocation data. We are engaged in it—for example, the review of the Children's On-Line Privacy Protection Act. And one question that we have asked is how should we treat geolocation data? In our private report issued in December, we made clear that we viewed geolocation data as sensitive data that requires heightened protections.

Mr. CASSIDY. But my specific question is, should we have a rule or a law that says, Thou shalt not keep this beyond X-number of days?

Mr. VLADECK. The Commission has not taken a formal position on that, other than to underscore the sensitivity of that data, and I can't—

Mr. CASSIDY. What would be an argument against? I was only aware of it because I stumbled across a Web site I don't normally read.

Mr. VLADECK. Part of our concern of course is the notice and consent in "scare quotes" that is extracted in the kind of situation that you are talking about is not significant, is not substantial. We are worried about those.

Mr. CASSIDY. So, again, I guess, what is the argument against that? I am asking anybody.

Mr. VLADECK. I think there would be two arguments. One is functionality. The data is being retained really to enhance the functionality——

Mr. CASSIDY. Although Mr. Brookman suggests that that is a short-term functionality benefit.

Mr. VLADECK. That is correct. But I am making the arguments on the other side. Not my arguments.

So the argument is, one is functionality. The other is it helps their analytics. They help to protect the kind of services——

Mr. CASSIDY. Precisely my point.

Mr. VLADECK. I am not disagreeing with you. You asked that I at least rehearse the arguments that you will hear. And those are the two basic arguments that you will hear.

Mr. BROOKMAN. I think there are cases where it may be reasoned. I am always scared about proscribing a law, like you must delete after a certain period of time. But there are uses of data where it might be reasonable for it to be tied to me for a period of time. If I have a traffic program on my computer and I want my computer to—my phone to remember where I go, to give me the optimized directions, that could be a legitimate use of my data. People use these programs like foursquare and looped, and places to check into places to maybe overshare, but to create a very permanent log of all of the places they have been. Some people like that.

I think I have used a similar Trip Advisor feature that says, Hey, I have been to this place and that place and I have checked in through my phone.

I think it depends on the usage. If you really do want to create a Hey, this is where I have been, to tell the world, I don't necessarily want to get in the way of that and tell people they can't do it.

Mr. CASSIDY. So perhaps the solution is to be a little bit less tricky in terms of the do we have your permission, and so it is clear, to record your data for in perpetuity by clicking here.

Mr. BROOKMAN. I absolutely agree with that, that you should be very clear about the usage you are taking their data for. And before you share it to another person, you should be very clear in getting permission for that as well, and not just buried on paragraph 40, the terms of service, but up front in a clear way. FCC has done some great writing on what it means.

Mrs. BONO MACK. The chair recognizes Mr. Dingell for 5 minutes.

Mr. DINGELL. I thank you for your courtesy and commend you for holding this hearing. I particularly appreciate your keeping the hearing open for me.

To all witnesses this will be a "yes" or "no" answer, starting on your right and on my left.

First of all, sir, do you believe the current industry efforts with respect to ensuring data security are sufficient? Yes or no.

Mr. VLADECK. I would say no.

Mr. MARTINEZ. I would say no.

Mr. SPAFFORD. No.

Mr. BROOKMAN. No.

Mr. DINGELL. Members of the panel, again to all witnesses, can such efforts be improved or do you believe that the Congress should

pass comprehensive security legislation? First question is, can efforts be improved? And the second one is, should the Congress pass comprehensive security data, data security legislation?

Mr. VLADECK. Yes, as to both parts of the question.

Mr. DINGELL. Sir?

Mr. MARTINEZ. Yes to both.

Mr. DINGELL. Sir?

Mr. SPAFFORD. Yes to both

Mr. DINGELL. Sir.

Mr. BROOKMAN. Yes to both, if legislation is strong enough.

Mr. DINGELL. Gentlemen, you are being very patient. We have a lot to get across in very limited amount of time so your courtesy is very much appreciated.

Gentlemen, I understand that the comprehensive data security requirements do not at this time exist in the United States. Rather, there exists a patchwork of Federal and State law and regulations that impose varying requirements on different people. Should Federal data security requirements supersede State requirements; yes or no.

Mr. VLADECK. I can't use a yes or no. Yes, to the extent they are not as substantial as Federal requirements, they should be at least the floor.

Mr. DINGELL. Sir?

Mr. MARTINEZ. Sir, I believe there should be a national standard for data breach reporting.

Mr. DINGELL. Sir?

Mr. SPAFFORD. Without knowing what the standards are, I can't answer.

Mr. DINGELL. Sir?

Mr. BROOKMAN. If they are strong enough to allow for State innovation, yes.

Mr. DINGELL. Would I be fair in assuming, however, that the panel thinks that we need a lot of work to assure that we achieve the standards needed of a national character? Am I correct on that, sir?

Mr. VLADECK. Yes, sir.

Mr. DINGELL. Sir?

Mr. MARTINEZ. Sir, I think there has been a lot of work for several years on multiple different types of data breach on legislation introduced in all different types of committees, and I believe the administration is real close to presenting to Congress a package that was worked on by multiple executive agencies.

Mr. DINGELL. Thank you. I believe I have given you a little more friendly question this time, sir.

Mr. SPAFFORD. Yes.

Mr. DINGELL. Sir?

Mr. BROOKMAN. Yes.

Mr. DINGELL. Gentlemen, this is always a question we run into. Further, in the light of Federal fiscal constraints, should State attorneys general be allowed to enforce Federal data security requirements; yes or no?

Mr. VLADECK. Yes.

Mr. MARTINEZ. Can you repeat the question?

Mr. DINGELL. Should Federal fiscal restraints be able to be enforced by State attorneys general?

Mr. MARTINEZ. I am not sure about if I am qualified to answer that.

Mr. DINGELL. I will not press you on it.

Sir?

Mr. SPAFFORD. I am not sure if I am qualified to answer that, but I think so.

Mr. DINGELL. Sir?

Mr. BROOKMAN. Absolutely.

Mr. DINGELL. All again, gentlemen, do you believe that the Federal data security legislation should include the flexibility for the Federal Trade Commission to update requirements in order to keep pace with the advancements in threats to data security; yes or no?

Mr. VLADECK. Yes.

Mr. DINGELL. Sir?

Mr. MARTINEZ. Yes.

Mr. DINGELL. Sir?

Mr. SPAFFORD. Yes.

Mr. DINGELL. Sir?

Mr. BROOKMAN. Yes.

Mr. DINGELL. This one to Mr. Vladeck. Do you believe the FTC's Magnuson-Moss rulemaking procedures would stifle the Commission's ability to write rules that keep pace with technical advancements in threats to data security; yes or no?

Mr. VLADECK. Yes.

Mr. DINGELL. Again, Mr. Vladeck, do you want to give a comment? Do you believe that the FTC should be allowed to write data security regulations according to the Administrative Procedure Act? You will understand that there is quite a difference between the two standards for rule writing.

Mr. VLADECK. Yes, I do. And yes, to the extent we are given rulemaking authority, we would ask strongly that it be conferred under the Administrative Procedure Act.

Mr. DINGELL. Thank you. To all witnesses, does the Federal Trade Commission currently have the resources with which to implement and enforce comprehensive data security requirements; yes or no?

Mr. Vladeck, if you please.

Mr. VLADECK. We always need more resources.

Mr. DINGELL. If you please, sir.

Mr. MARTINEZ. I would defer to the FTC regarding the resources.

Mr. DINGELL. A wise move.

Mr. SPAFFORD. I do not, no.

Mr. DINGELL. If you please, sir.

Mr. BROOKMAN. They could do it, but they could use more.

Mr. DINGELL. To all witnesses who have demonstrated extraordinary patience here, if you felt no, in that case what additional authorization would the FTC require to enforce such data security requirements? It would be perfectly appropriate if you were to submit this for the record at a future and comfortable time.

Mr. VLADECK. We currently have a relatively small staff working on privacy issues relative to other agencies, but it is an important

part of our mission, and we are a small agency which would benefit greatly from having enhanced resources in this area.

Mr. DINGELL. Mr. Martinez?

Mr. MARTINEZ. Again, I would defer to the FTC.

Mr. DINGELL. Doctor?

Mr. SPAFFORD. I would defer to the FTC.

Mr. DINGELL. And the last witness?

Mr. BROOKMAN. Larger staff and penalty authority and definitely APA rulemaking would be tempered.

Mr. DINGELL. Gentlemen, you have been most patient. Madam Chairman, you have given me a minute and 34 seconds more than I am entitled to.

Mrs. BONO MACK. I thank the gentleman, and I am quite impressed with his ability to pack a wallop in 5 minutes with so many yeses and noes.

I ask unanimous consent to include the Sony and Epsilon correspondence in the record of this hearing. Without objection, so ordered.

[The information follows:]

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

April 6, 2011

Mr. Ed Heffernan
President and Chief Executive Officer
Alliance Data Systems, Inc.
7500 Dallas Parkway, Suite 700
Plano, TX 75024

Dear Mr. Heffernan:

We write today regarding the recent data breach experienced by the marketing firm Epsilon that falls under the umbrella of Alliance Data Systems, Inc. According to recent press reports, the Epsilon breach that occurred within the last week impacted costumers of some of the largest banks and retail companies in the United States. JPMorgan Chase, Best Buy, Home Shopping Network, Walgreens, Kroger, Verizon, Barclays Bank of Delaware, and Capitol One are among Epsilon's customers identified in those reports.

Those reports also describe this breach event as only relating to the release of customer email addresses and names; however, in this day and age, even this information can lead to an unfortunate attack on an individual's identity – especially if the consumer's information is paired with the correct retailer or bank. In the simplest fashion, a criminal can easily create a phishing email that could lead an unwitting consumer into financial disaster. With a reported 40 billion marketing emails sent a year, the Epsilon breach could potentially impact a historic number of consumers.

The Subcommittee on Commerce, Manufacturing and Trade has a longstanding history of interest in consumer privacy, in addressing identity theft, and in industry efforts to address the threats posed by data breach. Events such as this one directly inform our efforts in the data security arena. As a result, we request an answer to the following questions no later than April 18, 2011.

1. When did you, including your online marketing arm, Epsilon, become aware of the data breach?
2. How did you become aware of the breach?
3. When did you notify the appropriate authorities of the breach?

4. When did you notify your corporate customers of the breach?
5. When did you notify the consumers whose data was breached?
6. How many consumers were impacted by this breach, and how did you ascertain the number?
7. How many companies were impacted in the data breach? Please identify the companies involved in this event.
8. Have you identified how the breach occurred?
9. Have you identified the individual(s) responsible for the breach?
10. What information was obtained by the unauthorized individual(s) a result of this breach, and how did you ascertain this information?
11. What steps have you taken or do you plan to take to prevent future such breaches?
12. Do you currently have a privacy policy that addresses data retention practices? If not, why not? If so, what are those practices and do you plan any changes in your policies as a result of this breach?
13. Regarding the information obtained in the breach, how long had that personal data been retained?
14. What steps have you taken or do you plan to take to mitigate the effects of this breach? Do you plan to offer any credit monitoring or other services to consumers who suffer actual harm as a result of this breach?

Thank you for your attention to and assistance in this matter.

Sincerely,

Mary Bono Mack
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

G. K. Butterfield
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable Fred Upton, Chairman

The Honorable Henry A. Waxman, Ranking Member

epsilon.

April 18, 2011

Chairman Mary Bono Mack
Subcommittee on Commerce,
Manufacturing & Trade
House Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member G.K. Butterfield
Subcommittee on Commerce,
Manufacturing & Trade
House Committee on Energy & Commerce
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bono Mack and Ranking Member Butterfield:

I am writing on behalf of Epsilon Data Management LLC ("Epsilon") to respond to your recent inquiry regarding the March 30, 2011 security incident involving unauthorized access of Epsilon's e-mail services platform. The incident resulted in the theft of lists containing e-mail addresses and, in some cases, first and last names maintained by Epsilon on behalf of a small percentage of its customers.

Epsilon values strongly the trust its customers place in it and their expectation that Epsilon will secure their data. The company continually monitors and evaluates its systems in an attempt to ensure their integrity. For these reasons, Epsilon deeply regrets that the criminal activities of others have called into question this commitment. The company continues to investigate the incident thoroughly and is cooperating with law enforcement to try and apprehend those responsible. As data management services become more sophisticated, criminals likewise are enhancing their efforts to infiltrate even the most sophisticated systems. Companies like Epsilon must continue to work with law enforcement at the national and state levels to ensure strong protections for data management companies, our customers and, most importantly, the end consumers whose data is at issue.

We hope that the following information answers your questions. We remain available to provide further information.

Background

Epsilon, a subsidiary of Alliance Data Systems Corporation, is a leading provider of permission-based e-mail marketing services. The company's roots lie in the direct mail marketing industry, where for over 40 years Epsilon has provided valuable services to companies seeking to market to consumers directly through postal mail, for example, through catalog

AllianceData℠
Loyalty and Marketing Services
www.epsilon.com
7500 Dallas Parkway
Suite 700
Plano, TX 75024
214-494-3000

marketing. Today, in addition to those and other related services, Epsilon also provides its customers with an e-mail marketing platform that includes enabling management of consumer e-mail contact information and implementation of opt-out requests. Consumers opt-in to receive communications from companies/brands (Epsilon customers) for which they have an affinity, and those e-mail communications can be notifications, special incentives, rewards and educational information, among others. Epsilon provides the mechanism through which companies can help ensure that consumer e-mail lists are maintained and messages to them (and their subscription preferences) are managed in accordance with Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"). The platform enables customers and Epsilon employees, acting on their behalf as account managers, to manage this data.

As a provider of data management services to some major consumer brands and financial institutions, Epsilon is committed to responsible information governance and recognizes the importance of keeping client data secure. To enhance security across its databases, Epsilon has implemented and maintains an information-security program conforming to data security standards set forth by the International Organization for Standardization (ISO). The ISO 27001[1] management standards that implement ISO 27002[2] controls, established a checks and balances system. This system requires information-security management which systematically assesses an organization's information-security risks, designs and implements comprehensive safeguards to control unacceptable risks, and maintains that program to ensure continued improvement and ongoing assessments. The goal of the ISO 27002 standard is to facilitate best practices for controlling information-security risks of the type to which companies like Epsilon might be subject. For example, one of the controls employed by Epsilon that is particularly relevant to this incident is that the company segregates its systems hosting e-mail applications from its systems hosting other database solutions. Combined, the ISO 27001 standard and 27002 controls provide a process for comprehensive information security that is detailed, rigorous, and adaptable to changing circumstances.[3]

It is important to note that ISO certification is a thorough and demanding process. Epsilon began the process to implement and obtain ISO certification of its information-security program in 2005 and completed its certification in 2006. The certification process took nearly a year and involved coordination with Alliance Data Systems' internal audit group and required validation from third-party auditors. Since 2006, Epsilon has maintained its ISO 27001 certification, undergoing yearly reviews that demand continual improvements to the company's information-security program. By obtaining and maintaining this certification, Epsilon has demonstrated its commitment to ensuring its information-security program provides reasonable and appropriate safeguards for client and consumer data.

---

[1] International Organization for Standardization, ISO/IEC 27001:2005, http://www.iso.org/iso/catalogue_detail?csnumber=42103.
[2] International Organization for Standardization, ISO/IEC 27002:2005, http://www.iso.org/iso/catalogue_detail?csnumber=50297
[3] Ted Humphreys, *State-of-the-Art Information Security Management Systems with ISO/IEC 27001:2005*, ISO INSIDER, Jan.-Feb., 2006, *available at* http://www.iso.org/iso/info_security.pdf

Chronology

Like many other organizations, Epsilon's information-security program is designed to identify and respond to new attacks and threats. Here, Epsilon's security program identified unauthorized activity with respect to certain of the company's e-mail databases and invoked Epsilon's security incident-response program. This led to an immediate move to investigate and remediate the unauthorized entry and to put in place additional safeguards based on what the company has learned so far, as the following chronology illustrates.

On March 30th, an Epsilon employee reached out to the security hotline maintained by the company. The employee had detected unusual download activity which seemed suspicious. Epsilon responded immediately with an investigation into the incident. This effort revealed that the login credentials of the employee, an e-mail application administrator, had been compromised. As soon as Epsilon's investigators identified the compromised credentials, the security team disabled the credentials and began a forensic investigation of the relevant computer resources.

Among the immediate responses, the company undertook the following:

- Initiated additional virus scans of relevant systems.
- Revoked and re-issued Epsilon system-user credentials for admin-level users.
- Invested and committed additional resources to monitoring unusual or suspicious activity.
- Began a forensic investigation to identify root causes.

In addition to efforts to identify and contain the incident within the company, Epsilon also began promptly assisting its customers. These actions included:

- Contacting potentially affected customers and cooperating with them on an ongoing basis.
- Notifying law enforcement including the FBI and Secret Service to seek out their assistance.
- Communicating with its anti-virus support vendor to identify threat signatures and obtain additional support.

After the initial day, Epsilon continued to investigate the incident, cooperate with law enforcement, and monitor its systems.

On April 1st, the Secret Service began its investigation. Epsilon continued its investigation and engaged outside forensic consultants to assist. The following day, April 2nd, Epsilon met with its outside forensic consultants to review the evidence collected thus far and confirm that information was flowing to the Secret Service. Epsilon's outside forensic consultants also reviewed the company's containment measures implemented thus far and, as the investigation unfolds, will make recommendations regarding further measures.

To date, the investigation has confirmed preliminarily that only e-mail addresses and, in some cases first and last names have been affected, involving approximately two percent of the company's total client base. At this time the company has no evidence that any other services or information it maintains has been affected. The company is seeking information regarding whether or not there has been any increase in unsolicited commercial e-mail or fraudulent or deceptive e-mail, including "phishing" attacks. It also appears that the incident was isolated to Epsilon's e-mail services platform; other platforms, such as its hosted customer databases, were not affected, as they, again, are segregated from the e-mail services platform.

Public reports indicate that at least 50 of Epsilon customers were impacted; some of those customers chose to notify their customers of the incident, and in some cases those customers made public statements. Epsilon's relationships with its customers are confidential, and at their request, their identity was not disclosed publicly by Epsilon. For that reason, we are unable at this time to provide a complete list of the company's affected customers, as Epsilon is still reviewing its confidentiality and notice obligations with its customers.

Epsilon is also attempting to ascertain the total number of individual consumers affected. Determining this number, however, may be difficult for several reasons. First, because many consumers use multiple e-mail addresses and may appear on several or many of Epsilon's customers' lists, identifying the number of individually affected consumers with any precision may not be possible. Similarly, Epsilon cannot determine how many consumers may have been affected within a particular state because the information as maintained generally only included an e-mail address (or name in some cases). Epsilon has, however, provided public notice of the incident on its website via press releases on April 1st and April 6th, and has set up an incident-response center to answer questions from consumers and customers who contact the company. Epsilon has also added information to its website to provide educational materials for consumers on guarding against phishing attacks, available at http://www.epsilon.com/Privacy%20Policy/Consumer_Information_on_Phishing/p467-l2. This website provides information to consumers explaining phishing attacks, how they occur, and the steps a consumer can take to avoid being a victim.

We hope that the information above responds to the questions you posed and provides context for the attack that occurred on Epsilon's e-mail services platform. In addition, with regard to your question concerning how personal data is retained, Epsilon maintains its customers' e-mail address lists per the guidance of its customers upon whose behalf we maintain this data. The duration of the retention of that data likewise is done at our customers' direction. Finally, in reply to your query regarding whether Epsilon plans to offer any credit monitoring or other services to consumers, at this time, Epsilon is still investigating the potential implications of this attack on individual consumers. The company has not made an evaluation of whether it would be appropriate to provide credit monitoring or other services to consumers.

Moving Forward

Going forward, Epsilon will continue to adhere to and improve its security policies and procedures, especially in light of this criminal attack on its e-mail services platform. Further, Epsilon has engaged third-party services to review and recommend additional hardening processes to the company's existing controls.

We should also note that it remains Epsilon's first priority to respond to its customers and ensure they have the company's full cooperation so that their data and consumers are protected. The company anticipates identifying additional facts as part of its existing practice to remediate incidents and learn from them. As this effort is completed, Epsilon remains committed to cooperating fully.

* * * * *

We sincerely hope that this information answers your questions regarding this malicious attack on Epsilon's systems. The company continues to make significant efforts to remediate this situation and to work to prevent such breaches from occurring again. Epsilon will also continue to fully cooperate with law enforcement to identify the perpetrators involved. Please let us know if you have any additional questions or concerns.

Sincerely,
Epsilon Data Management, LLC

Jeanette Fitzgerald
General Counsel

cc: The Honorable Fred Upton, Chairman
The Honorable Henry A. Waxman, Ranking Member

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

April 29, 2011

Mr. Kazuo Hirai
Chairman
Sony Computer Entertainment America
919 East Hillsdale Blvd.
Foster City, CA 99404

Dear Mr. Hirai:

We write today regarding the recent data breach experienced by Sony Corporation's Playstation Network operated by Sony Computer Entertainment of America. According to Sony's statement, the breach occurred between April 17 and April 19, and impacted as many as 77 million account holders' personal information. A public acknowledgement of the breach was not made until April 26.

As we understand from Sony's statements, all facts regarding the breach are not yet known and an internal investigation continues. However, Sony's statement describes information illegally obtained to include account information as well as potentially profile information. Sony's public statements suggest there is no evidence credit card data was taken, but such a scenario cannot be ruled out. Given the amount and nature of the personal information known to have been taken, the potential harm that could be caused if credit card information was also taken would be quite significant.

The Subcommittee on Commerce, Manufacturing, and Trade has a longstanding interest in consumer privacy, identity theft, and industry efforts to address the threats posed by unauthorized access to consumers' personal information resulting from a data breach. Events such as this one directly inform our efforts in the data security arena. We expect to address Federal data security legislation in our Committee this year, and we have scheduled a hearing on May 4, 2011, regarding the threat of data theft to American consumers to explore these issues in greater detail. To inform our efforts to protect consumer information, we request answers to the following questions and requests no later than May 6, 2011.

1. When did you become aware of the illegal and unauthorized intrusion?
2. How did you become aware of the breach?

3. When did you notify the appropriate authorities of the breach?
4. Why did you wait to notify your customers of the breach?
5. Was the information obtained applicable to all accounts or a portion of the accounts? How many consumers or accounts were impacted by this breach, and how did you ascertain the number?
6. Have you identified how the breach occurred?
7. Have you identified the individual(s) responsible for the breach?
8. What information was obtained by the unauthorized individual(s) as a result of this breach, and how did you ascertain this information?
9. How many Playstation Network account holders provided credit card information to Sony Computer Entertainment?
10. Your statement indicated you have no evidence at this time that credit card information was obtained, yet you cannot rule out this possibility. Please explain why you do not believe credit card information was obtained and why you cannot determine if the data was in fact taken.
11. What steps have you taken or do you plan to take to prevent future such breaches?
12. Do you currently have a policy that addresses data security and retention practices? If not, why not? If so, what are those practices and do you plan any changes in your policies as a result of this breach?
13. What steps have you taken or do you plan to take to mitigate the effects of this breach? Do you plan to offer any credit monitoring or other services to consumers who suffer actual harm as a result of this breach?

Thank you for your attention to and assistance in this matter.

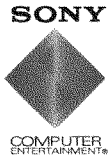
Sincerely,

Mary Bono Mack
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

G.K. Butterfield
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable Fred Upton, Chairman

The Honorable Henry A. Waxman, Ranking Member



Sony Computer Entertainment America
919 East Hillsdale Blvd.
Foster City, California 94404-2175
650 655 8000
650 655 8001 Fax

May 3, 2011

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable G. K. Butterfield
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bono Mack and Ranking Member Butterfield:

Thank you for giving me this opportunity to respond to questions from the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade.

Sony now faces a large-scale cyber-attack involving the theft of personal information. This cyber-attack came shortly after Sony Computer Entertainment America was the subject of denial of service attacks launched against several Sony companies and threats made against both Sony and its executives in retaliation for enforcing intellectual property rights in U.S. Federal Court. We are currently dealing with all aspects of this cyber-attack and have our personnel deployed and working around the clock to get the systems back up and to make sure all our customers are informed of the data breach and our responses to it. We expect to restore most services to our customers shortly. We have received so far no confirmed reports of illegal usage of the stolen information.

In dealing with this cyber-attack, the company has operated on the basis of several key principles:

1. Act with care and caution. This is why Sony Network Entertainment America Inc. ("Sony Network Entertainment America"), which operates the PlayStation Network and Qriocity services (collectively, "PlayStation Network"), has taken the almost unprecedented step of shutting down the affected systems as soon as threats were detected and is keeping them down, even at substantial cost to the company, until all changes to strengthen security are completed. We have tried to err on the side of safety and security in making these decisions and judgments.

2. Provide relevant information to the public when it has been verified. Sony Network Entertainment America immediately hired a highly regarded information technology security firm and supplemented that firm with additional expertise and resources over several days. Sony Network Entertainment America then released information to its consumers when we and those experts believed that information was sufficiently confirmed. The truth is that retracing the steps of experienced cyber-

attackers is a highly complex process that takes time to carry out effectively. At the same time that the experienced attackers were carrying out their attack, they also attempted to destroy the evidence that would reveal their steps.

3. Take responsibility for our obligations to our customers. We have apologized for the inconvenience caused by the illegal intrusion into our systems and offered a free month of service in addition to the number of days the systems are down as part of a "Welcome Back" program for our customers. We are also offering our customers in the U.S. complimentary identity theft protection services.

4. Work with law enforcement authorities to assist in the apprehension of those responsible and cooperate with all authorities on meeting our regulatory requirements. One of our first calls was to the FBI, and this is an active, on-going investigation.

I am of course aware of the criticism Sony has received for the time taken to disclose information to our customers. I hope you can appreciate the extraordinary nature of the events the company was facing - brought on by a criminal hacker whose activity was neither immediately nor easily ascertainable. I believe that after you review all the facts you will agree that the company has been acting in good faith to release reliable information in accordance with its legal and ethical responsibilities to its valued customers.

We have been investigating this intrusion around the clock since we discovered it, and that investigation continues today. Just this past Sunday, May 1st, we learned that a likely theft from another Sony company's online service had previously gone undetected, even after highly trained technical teams had examined the network infrastructure that had been attacked around the same time as the PlayStation Network. What is becoming more and more evident is that Sony has been the victim of a very carefully planned, very professional, highly sophisticated criminal cyber attack designed to steal personal and credit card information for illegal purposes. Sunday's discovery that data had been stolen from Sony Online Entertainment only highlights this point.

When Sony Online Entertainment discovered this past Sunday afternoon that data from its servers had been stolen, it also discovered that the intruders had planted a file on one of those servers named "Anonymous" with the words "We are Legion." Just weeks before, several Sony companies had been the target of a large-scale, coordinated denial of service attack by the group called Anonymous. The attacks were coordinated against Sony as a protest against Sony for exercising its rights in a civil action in the United States District Court in San Francisco against a hacker.

While protecting individuals' personal data is the highest priority, ensuring that the Internet can be made secure for commerce is also essential. Worldwide, countries and businesses will have to come together to ensure the safety of commerce over the Internet and also find ways to combat cybercrime and cyber terrorism.

Almost two weeks ago, one or more cyber criminals gained access to PlayStation Network servers at or around the same time that these servers were experiencing denial of service attacks. The Sony Network Entertainment America team did not immediately detect the criminal intrusion for several possible reasons. First, detection was difficult because of the sheer sophistication of the intrusion. Second, detection was difficult because the criminal hackers exploited a system software vulnerability. Finally, our security teams were working very hard to defend against denial of service attacks, and that may have made it more difficult to detect this intrusion quickly – all perhaps by design.

Whether those who participated in the denial of services attacks were conspirators or whether they were simply duped into providing cover for a very clever thief, we may never know. In any case, those who participated in the denial of service attacks should understand that - whether they knew it or not - they were aiding in a well planned, well executed, large-scale theft that left not only Sony a victim, but also Sony's many customers around the world.

Making the Internet safe for entertainment, commerce and education is a paramount government interest. The criminal cyber-attacks on Sony have been and will continue to be perpetrated on other companies as well. If not addressed, these types of attacks could become commonplace. Creating more stringent guidelines for maintaining and policing storage of personal information may be necessary in our current climate, but, make no mistake, without addressing the need for strong criminal laws and sanctions and, most importantly, enforcement of these laws, there will not be any meaningful security on the Internet.

Sony is grateful for the assistance it has received from law enforcement and appreciates this opportunity to raise these issues with this Committee as it considers how to build an environment where social networks and commerce on the Internet can develop uninhibited by security risks.

Turning to Sony's responses to the Committee's questions:

1. **When did you become aware of the illegal and unauthorized intrusion?**

On April 19, 2011 at 4:15 p.m. PDT, members of the Sony Network Entertainment America network team detected unauthorized activity in the network system, specifically, that certain systems were re-booting when they were not scheduled to do so. The network service team immediately began to evaluate this activity by reviewing running logs and analyzing information in order to determine if there was a problem with the system.

On April 20, 2011, in the early afternoon, the Sony Network Entertainment America team discovered evidence that indicated an unauthorized intrusion had occurred and that data of some kind had been transferred off the PlayStation Network servers without authorization. At the time, the network service team was unable to determine what type of data had been transferred, and they therefore shut the PlayStation Network system down.

2. **How did you become aware of the breach?**

Sony Network Entertainment America became aware of the PlayStation Network intrusion as described above. The Sony Network Entertainment America team became aware of a transfer of data out of the system also as described above. Sony Network Entertainment America then began the exhaustive and highly sophisticated process of identifying the means of access and the nature and scope of the theft. That investigation is on-going to this day.

3. **When did you notify the appropriate authorities of the breach?**

On April 22, 2011, Sony Computer Entertainment America's general counsel provided the FBI with information about the intrusion. (Sony Computer Entertainment America oversees the PlayStation brand in North America and has been involved with the PlayStation Network's operation since its inception). The forensic experts that Sony Network Entertainment America had retained had not determined the scope or effect of the intrusion at the time the FBI was contacted. A meeting was set up to provide details to law enforcement for Wednesday April 27, 2011.

Following an extensive investigation by a team of external forensic computer experts with the assistance of the internal network service team, Sony Network Entertainment America and Sony Computer Entertainment America coordinated to provide public notice of the intrusion on April 26, 2011. On the same day, Sony Network Entertainment America notified the applicable regulatory authorities in the states of New Jersey, Maryland, and New Hampshire. On April 27, 2011, Sony Network Entertainment America also notified regulatory authorities in the states of Hawaii, Louisiana, Maine, Massachusetts, Missouri, New York, North Carolina, South Carolina, Virginia and Puerto Rico of the criminal intrusion described above.

4. Why did you wait to notify your customers of the breach?

The PlayStation Network is a complex network, consisting of approximately 130 servers, 50 software programs and 77 million registered accounts. The basic facts of what occurred after the intrusion bear this out.

On April 19, 2011, the Sony Network Entertainment America network team discovered that several PlayStation Network servers unexpectedly rebooted themselves and that unplanned and unusual activity was taking place on the network. This activity triggered an investigation. The network team took four servers off line and an internal assessment began. The internal assessment of these four servers continued through the end of the business day and into the evening. The next day, April 20th, Sony Network Entertainment America mobilized a larger internal team to assist the investigation of the four suspect servers. This internal team discovered the first credible indications that an intruder had been in the PlayStation Network systems, and six more servers were identified as possibly being compromised. Sony Network Entertainment America immediately decided to shut down all of the PlayStation Network services.

In the afternoon of April 20th, Sony Network Entertainment America retained a recognized security and forensic consulting firm to mirror the servers to enable forensic analysis to begin. The type of mirroring required to provide meaningful information in this type of situation had to be meticulous. Many hours were needed simply to mirror servers before analysis could begin. Sony Network Entertainment America and its outside forensics team began to work on mirroring the servers.

The scope and complexity of the investigation grew substantially as additional evidence about the attack developed. On April 21, 2011, Sony retained a second recognized computer security and forensic consulting firm to assist in the investigation, to provide more manpower to image the servers and to conduct a forensic analysis of all aspects of the suspected security breach.

The team took until the afternoon of April 22, 2011 to complete the mirroring of nine of the 10 servers that were suspected of being compromised. By the evening of April 23, 2011, the forensic teams were able to confirm that intruders had used very sophisticated and aggressive techniques to obtain unauthorized access, hide their presence from system administrators, and escalate privileges inside the servers. Among other things, the intruders deleted log files in order to hide the extent of their work and activity within the network. Now Sony Network Entertainment America knew it was dealing with a sophisticated hacker and (on Easter Sunday) decided that it needed to retain yet another forensic team with highly specialized skills to assist with the investigation. Specifically, this firm was retained to provide even more manpower for forensic analysis in all aspects of the suspected security breach, and, in particular, to use their special skills to determine the scope of the data theft. By April 25, 2011, the forensic teams were able to confirm the scope of the personal data that they believed had been taken but could not rule out whether credit card information had been accessed.

Sony Network Entertainment America was of course aware of its affirmative obligations under various state statutes to conduct a reasonable and prompt investigation to determine the scope of breach and depth of the breach and to restore the integrity of our network system. Sony Network Entertainment America further understood its obligation to report its finding to consumers if certain, specific kinds of personal information could have been compromised. As this Committee knows, there are a variety of state statutes that apply and several that have conflicting or inconsistent requirements, but given the global nature of the network, Sony Network Entertainment America needed to be mindful of them all. Throughout the process, Sony Network Entertainment America was very concerned that announcing partial or tentative information to consumers could cause confusion and lead them to take unnecessary actions if the information was not fully corroborated by forensic evidence. For example, as of April 25, 2011, Sony had not and could not determine if credit card information had been accessed and, while no evidence existed at the time that this type of information had been taken, we ultimately could not rule out that possibility entirely based on the reports of the forensics teams. Given that situation, on April 26, 2011, Sony Network Entertainment America and Sony Computer Entertainment America notified consumers that their personal information had been taken and that the companies could not rule out the possibility that credit card data had been stolen as well.

5. Was the information obtained applicable to all accounts or a portion of the accounts? How many consumers or accounts were impacted by this breach, and how did you ascertain the number?

Information appears to have been stolen from all PlayStation Network user accounts, although not every piece of information in those accounts appears to have been stolen. The criminal intruders stole personal information from all of the approximately 77 million PlayStation Network and Qriocity service accounts.

6. Have you identified how the breach occurred?

Yes, we believe so. Sony Network Entertainment America is continuing its investigation into this criminal intrusion, and more detailed information could be discovered during this process. We are reluctant to make full details publicly available because the information is the subject of an on-going criminal investigation and also the information could be used to exploit vulnerabilities in systems other than Sony's that have similar architecture to the PlayStation Network.

7. Have you identified the individual(s) responsible for the breach?

No.

8. What information was obtained by the unauthorized individual(s) as a result of this breach, and how did you ascertain this information?

Based on the activity of the intruder, we know that queries were made in the PlayStation Network system database for user account information related to name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PlayStation Network online ID.

As of today, the major credit card companies have not reported that they have seen any increase in the number of fraudulent credit card transactions as a result of the attack, and they have not reported to us any fraudulent transactions that they believe are a direct result of the intrusions described above.

9. How many PlayStation Network account holders provided credit card information to Sony Computer Entertainment?

Globally, approximately 12.3 million account holders had credit card information on file on the PlayStation Network system. In the United States, approximately 5.6 million account holders had credit card information on file on the system. These numbers include active and expired credit cards.

10. Your statement indicated you have no evidence at this time that credit card information was obtained, yet you cannot rule out this possibility. Please explain why you do not believe credit card information was obtained and why you cannot determine if the data was in fact taken.

As stated above, Sony Network Entertainment America has not been able to conclude with certainty through the forensic analysis done to date that credit card information was not transferred from the PlayStation Network system. We know that for other personal information contained in the account database, the hacker made queries to the database, and the external forensics teams have seen large amounts of data transferred in response to those queries. Our forensics teams have not seen queries and corresponding data transfers of the credit card information.

11. What steps have you taken or do you plan to take to prevent future such breaches.

The new security measures being implemented include the following:

- Added automated software monitoring and configuration management to help defend against new attacks;
- Enhanced levels of data protection and encryption;
- Enhanced ability to detect software intrusions within the network, unauthorized access and unusual activity patterns;
- Implementation of additional firewalls; and
- The company also expedited a planned move of the system to a new data center in a different location with enhanced security.
- The naming of new Chief Information Security Officer (CISO) directly reporting to the Chief Information Officer, Sony Corporation.
-

12. Do you currently have a policy that addresses data security and retention practices? If not, why not? If so, what are those practices and do you plan any changes in your policies as a result of this breach?

Yes, we do have policies that address data security and retention practices.

Sony utilizes a global framework for providing policies to its group companies based on the international information security standard called "ISO/IEC 27001" to ensure consistent standard information security practices for each operating company. The Global Information Security Policy ("GISP") sets forth the company's information security management structure and administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of non-public information. The GISP also defines the overall direction and policy of Sony Group's information security program and the authorities and responsibilities for information security management. Additionally, Sony provides a set

of 14 standards, Global Information Security Standards ("GISS"), that specify the types of controls needed for the different categories of information security management (e.g., information classification, access controls and HR security).

Continued application of these policies and practices, in addition to, an expedited move to our new enhanced security data facility, are the changes being made as a result of this breach.

13. What steps have you taken or do you plan to take to mitigate the effects of this breach? Do you plan to offer any credit monitoring or other services to consumers who suffer actual harm as a result of this breach?

Sony Network Entertainment America is committed to helping its customers protect their personal data and will offer its U.S. account holders complimentary identity theft protection services. Because the breach affects customers worldwide, different programs may be offered in other territories.

Sony Network Entertainment America is also creating a "Welcome Back" program to be offered worldwide, which will be tailored to specific markets to provide our consumers with a selection of service options and premium content as an expression of the company's appreciation for their patience and support.

Central components of the "Welcome Back" program will include:

- Each territory will be offering selected PlayStation entertainment content for free download. Specific details of this content will be announced in each region soon.
- All consumers coming back to the PlayStation Network will be provided with 30 days of free membership in the PlayStation Plus premium subscription service. Current PlayStation Plus subscribers will have their subscriptions extended for the number of days PlayStation Network and Qriocity services were unavailable and, in addition, will receive 30 days of free service.
- Music Unlimited subscribers (in countries where the service is available) will have their subscriptions extended for the number of days PlayStation Network and Qriocity services were unavailable and, in addition, receive 30 days of free service.

* * * *

I want to thank this Committee for giving me this opportunity to respond to its questions. I hope I have been able to convey the extraordinary circumstances and challenges that have confronted the employees of Sony Network Entertainment America and Sony Computer Entertainment America over the past few days and weeks. My employees were facing and have endured an unprecedented large-scale criminal cyber-attack. They were faced with very difficult decisions and often-times conflicting concerns and objectives. Throughout this challenging period, they acted carefully and cautiously and strove to provide correct and accurate information while balancing concerns for our consumers' privacy and need for information.

This Committee is rightfully concerned to protect the information and privacy of individuals on the Internet and to ensure that companies have robust security and protection practices. We ask the Committee to consider as well the connection between data security and the cybercrimes and cyber terrorism that threaten to make the Internet unsafe for consumers and commerce. We very much appreciate the Committee's efforts to put in place laws to protect us from these very real threats.

Respectfully submitted,

RRR for Kazuo Hirai

Kazuo Hirai
Chairman of the Board of Directors
Sony Computer Entertainment America LLC

cc: The Honorable Fred Upton
Chairman
U.S. House of Representatives
Committee on Energy and Commerce

The Honorable Henry A. Waxman
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce

Mrs. BONO MACK. And I just want to sum up by saying that prior to 2005, we didn't spend a whole lot of time as a Nation talking about the dangers of data breaches. Things have sure changed in a hurry. We have gone from a stolen laptop containing 260,000 customers' records to a sophisticated criminal cyber attack on a worldwide network containing more than 100 million customer records. And this begs the important question, if we don't do something soon, what is next and where does it end?

So I would like to remind members that they have 10 business days to submit questions for the record and ask the witnesses to please respond promptly to any questions they receive.

Mrs. BONO MACK. Again, I thank our witnesses very much for your help today. And the hearing is now adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Federal Trade Commission

Responses to Questions for the Record to David Vladeck,

from Chairman Mary Bono Mack

Subcommittee on Commerce, Manufacturing and Trade Hearing Entitled "The Threat of Data Theft to American Consumers,"

May 4, 2011

1. Is there an industry standard for data minimization, retention, and protection?

With respect to the protection of data (i.e., data security), there are standards that are widely accepted by experts in the field of information security, and such standards should be adopted by industry. With respect to data minimization and retention limits, we are not aware of any similar industry-wide standards. For example, in the search engine industry, the major industry players adhere to differing anonymization and retention schedules. FTC staff have recommended that companies collect only the data needed for a specific business purpose and retain such data only as long as necessary to fulfill that purpose.

2. Without a data security law in place, what actions can the FTC take in response to a data breach?

Under the FTC Act, the Commission can challenge unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury not outweighed by other benefits. In such cases, the Commission issues orders containing strong injunctive relief, including requirements to maintain reasonable data security going forward and to conduct third-party audits of data security practices. The Commission cannot obtain a civil penalty for violations of Section 5, however, and the Commission's traditional equitable remedies – such as disgorgement and restitution – generally are not practicable in data security cases. So absent an independent statutory basis, in most data security cases the Commission's orders do not include monetary relief.

3. What are "principles of privacy by design"? Are businesses moving in that direction?

"Privacy by design" is the concept that privacy should be built into a company's everyday business practices and throughout the product life cycle from the very first stages of development. FTC staff has recommended that, under these principles, a company should provide reasonable security for consumer data, collect only the data needed for a specific business purpose, retain data only as long as necessary to fulfill that purpose, safely dispose of data no longer being used, and implement reasonable procedures to promote data accuracy. In addition, companies should assign personnel to oversee privacy issues, train employees on privacy issues, and conduct privacy reviews when developing new products and services. Many companies increasingly recognize the importance of privacy by design, but many others do not take adequate steps to manage the personal information they collect or to avoid collecting information they do not need.

4. In the data security bill that processed through the Committee on Energy and

Commerce and the House of Representatives in the 111th Congress, companies were required to notify consumers no later than 60 days. The timeframe of 60 days came in technical comments from the FTC.

a. Why did the FTC recommend 60 days? Is there harm in immediately informing consumers their information may have been breached so they can protect themselves, even if it later turns out their information was not breached?

FTC staff had proposed 60 days as an outer limit, with notice being provided as soon as practicable and without unreasonable delay. This is the standard used in our health breach notification rule, which applies to certain entities collecting health information. We are not wedded to that time frame, however, and would be happy to work with the Committee to discuss an appropriate time frame.

b. Is there harm in over-notification?

Certainly, over notification should be a consideration and consumers should not receive so many notices that they become confused or tune out the notices they receive. But when the trigger for notification is calibrated to the type of information breached and the degree of harm, notification is very beneficial and effective for consumers in allowing them to make informed decisions and mitigate potential harm.

c. If the timeframe for notice is shortened, is there a risk of many companies over-notifying consumers?

Although it is important for consumers to receive timely notice, companies need a reasonable amount of time to assess the extent of a breach and identify the consumers whose information was breached. In addition, there are times when a company may reasonably delay notification – for example, when the company is in the process of restoring the integrity of its systems. As mentioned above, the 60 day proposal was an outer limit, and notice should be provided as soon as practicable and without unreasonable delay. It is possible that this time frame could be shortened without a high risk of over-notification, and FTC staff would be happy to work with the Committee on what legislation should provide as an appropriate time frame.

d. What is the proper balance to consider between timely notice to consumer and effective notification to the affected consumers?

In order for notice to be most effective, a company must identify the consumers whose information was breached and the categories of information subject to the breach. Companies should be given a reasonable amount of time to assess these facts in order to provide effective notice, but notice should be provided as soon as practicable and without unreasonable delay.

5. Your testimony references your workshops on this issue and recommends that business mitigate risk by only holding data that is necessary.

a. Should consumers also be able to mitigate their risk by requesting a company no longer hold certain pieces of consumer's personal information after the business relationship is terminated?

In its preliminary staff report proposing a new privacy framework, FTC staff recommended that

companies retain consumer personal information for only as long as necessary to fulfill a specific business purpose. Staff solicited public comment on those proposals and is expecting to release a final report later this year. In its data security cases, the Commission has challenged companies' retention of data that was no longer necessary for a business purpose. *See, e.g., Ceridian Corp.*, FTC File No. 1023160 (May 3, 2011) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In re DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order). In the case where a business relationship is terminated, a company may no longer have a business purpose for retaining data unless it needs to maintain it to, for example, comply with statutory requirements. When information need no longer be maintained, the company should safely dispose of such data, whether at the request of the consumer or independently of any such request.

b. What information do you think should be outside the scope of retention for legitimate business needs?

The answer would vary depending on the nature of the business and the data retained, and other factors. Some businesses, such as banks, may need to maintain information such as name and address, along with detailed transaction information, for tax reporting purposes. Other businesses with the same type of information, such as online financial information aggregators, may be able to destroy the same type of information as soon as the customer terminates the relationship.

c. How would you recommend a business relationship be defined in this context? Is the definition of a business relationship in the context of telemarketing mail or calls instructive in this context?

Under the Telemarketing Sales Rule, the "established business relationship" exception allows a seller to contact a consumer for an 18 month period after the consumer's last financial transaction with the seller, or within three months of a consumer's inquiry regarding a seller's goods or services, regardless of whether the consumer is listed in the National Do Not Call Registry. In this context, the use of the information by the seller is limited to a very specific purpose: telemarketing. By contrast, with respect to a company's general data minimization and retention policies, the company may be retaining data for many different reasons. Thus, while the Telemarketing Sales Rule's definition of an "established business relationship" may provide a useful point of reference, there are broader issues that must be addressed in the context of general data minimization and retention policies. FTC staff would be happy to work with the Committee on these issues.

d. How long should a consumer's data be retained after the termination of a business relationship?

As mentioned above, FTC staff has recommended that companies retain consumer personal information for only as long as necessary to fulfill a specific business purpose. The answer would vary depending on the nature of the business and the information. A drug store, for example, might need to keep detailed records of a pharmacy transaction involving controlled substances for more than a year to comply with state or federal law, while other businesses would have no reason to retain customer data after the termination of the business relationship and should safely dispose of such data as soon as possible.

6. The FTC is already active on data security issues. Would a Federal data security law make the FTC's job easier? How would it affect what the Commission currently does?

Data security legislation would help consumers in several ways. First, the Commission has recommended legislation requiring all companies that hold sensitive consumer data -- not just companies within the FTC's jurisdiction -- to take reasonable measures to safeguard it and to notify consumers when the security of their information is breached. Under current federal law, many businesses outside FTC jurisdiction have no obligation to secure the consumer information they maintain, and the vast majority of businesses are not required to give notice of a breach. Legislation would also give the Commission authority to seek civil penalties in data security cases, which would increase the deterrent value of our orders, as equitable remedies such as disgorgement and redress are often inadequate in these cases. Moreover, Congressional legislation would send a clear signal that implementing reasonable protections for consumer information is part of doing business, while establishing clear standards for those companies to meet.

7. How would the FTC write rules that are flexible enough for a dynamic, technology-driven environment?

I agree that rules regarding data security must be flexible so that they can be adapted as technology and business practices evolve. The Commission has taken this flexible approach in its GLB Act Safeguards Rule, which provides a good roadmap for companies as to the procedures and basic elements necessary to develop a sound security program. Companies should perform a thorough risk assessment of their security practices for managing personal information and then design a security program to control and limit these risks. Although the Safeguards Rule applies only to financial companies, it provides helpful guidance to other companies as well.

8. How does the FTC keep enforcement by State Attorneys General in sync with Federal policy on these rapidly changing issues?

The FTC has a history of working well with state attorneys general on enforcement actions in many types of cases. Our privacy and data security staff coordinate with state enforcers on issues of shared interest – for example, in the LifeLock matter, 35 states joined the Commission in challenging deceptive conduct, together obtaining an $11 million settlement.

9. Some of the FTC's recent settlement agreements provide for 20 years of audits. Is that now the norm for post-breach audits? How does the FTC determine what is a reasonable length of time for post-breach audit?

FTC orders sunset in 20 years, so many FTC data security orders require that companies implement comprehensive security plans and obtain biennial audits over the life of the order. While the Commission invariably requires companies to implement comprehensive security plans for the full term of the order, in rare cases the Commission has varied the term of the audit provision based on the facts and circumstances of a particular case.

10. The Administration's proposal does not include a specific provision addressing data brokers. Do you believe it is no longer necessary to include provisions specific to data

brokers in Federal legislation?

In the past, the Commission has supported legislative provisions that would given consumers the ability to access certain information that data brokers have about them, and in appropriate cases, to correct or suppress such data. In addition, in December, the FTC Staff issued a preliminary report seeking comment on a new framework for privacy protection. In that report, Staff proposed providing consumers with reasonable access to the data that companies maintain about them, particularly for companies that do not interact with consumers directly, such as data brokers. Because of the significant costs associated with access, staff proposed that the extent of access should be proportional to both the sensitivity of the data and its intended use. Staff is reviewing the comments received and expects to prepare a final report by the end of this year.

Questions for the Record

DSAIC Pablo Martinez's Testimony before
House Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

"The Threat of Data Theft to American Consumers"

May 4, 2011

The Honorable Mary Bono Mack

1. **Is there an industry standard for data minimization, retention, and protection?**

As a law enforcement agency, the Secret Service does not participate in setting industry standards for data minimization, retention or protection. It is our understanding that one standard which is used frequently in the financial services sector is the Payment Card Industry Digital Security Standard (PCI DSS). PCI DSS provides recommendations for developing a strong payment card data security process, which includes prevention, detection and appropriate reaction to security incidents.

2. **There are 49 different State and territory data breach notification regimes in place. In your experience, has this complicated or delayed consumer notification? If so, how?**

Pursuant to many state breach notifications, the responsibility to notify consumers falls with the victim companies and not law enforcement. Therefore, the Secret Service is unable to comment on complications experienced by companies when notifying their consumers.

3. **The Committee on Energy and Commerce passed and the House of Representatives adopted a data security bill in the 111th Congress that provided no more than 60 days for a company to notice consumers of a data breach unless law enforcement requests an additional 30 days delay for their purposes.**

   a. **Should a consumer be notified immediately, or at least sooner than 60 days, of a breach involving their personal data?**

Immediate notification could potentially compromise an on-going investigation. As a law enforcement agency, the Secret Service believes that it is vital that victim companies be given an opportunity to provide as clear and concise a picture to law enforcement regarding what has occurred. A delay allows for victim companies to investigate internally and minimize damages, as well as work with law enforcement to further their local, state or federal investigation. In most cases, all of the above can be accomplished within the 60 day period.

   b. **If a criminal investigation prompts law enforcement to request a delay in notification, is 30 days enough additional time?**

Typically, state laws which provide for a 30 day delay notification for law enforcement purposes also allow for law enforcement to seek additional delays in 30 day increments. Based on our experience, the Secret Service has sought additional 30 day extensions, and therefore would not recommend limiting the extension to exclusively one 30 day period.

June 18, 2011

The Honorable Mary Bono Mack, Chairman
Subcommittee on Commerce, Manufacturing and Trade
House of Representatives
2125 Rayburn Office Building
Washington, DC 20515–6115

Dear Representative Mack:

Enclosed are my responses to your questions-for-record of June 6, 2011, following the May 4th hearing on "The Threat of Data Theft to American Consumers."

Thank you again for the opportunity to testify on this important topic. I would like to reiterate both my personal interest and willingness to provide further support on this issue, and that of the USACM Council. Should you have any questions or need additional information, please contact me or Cameron Wilson, our Director of Public Policy, at 202-659-9711 or at Cameron.wilson@acm.org.

Regards,

Eugene H. Spafford, Ph.D.
Chair, U.S. Public Policy Council
Association for Computing Machinery

cc: The Honorable G.K. Butterfield, Ranking Member
Subcommittee on Commerce, Manufacturing and Trade

Encl.

ABOUT ACM and USACM

With 100,000+ members, the Association for Computing Machinery (ACM) is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.

1828 L Street, NW Suite 800
Washington, DC 20036

USACM.acm.org

202 659 9711 *tel*
202 667 1066 *fax*

1) Is it possible that all companies could be the victim of a criminal breach regardless of security measures?

No set of security measures can guarantee that there will be no criminal breach. Even if an organization does not have its computers connected to the Internet it is possible for a corrupt insider to expose some of the data, or for a physical theft of storage media to occur. These kinds of exposures happen even in the most tightly controlled environments, such as the U.S. defense community and law enforcement (e.g., the Wikileaks exposures, and espionage by Aldrich Ames and Robert Hanssen).

Strong security measures can be instituted to protect against malicious insiders, against theft of media and equipment, against eavesdropping of communication, and other non-software threats. Security measures can also be put in place to provide extra protection for on-line storage of data. Policies, training and technology can also be deployed to minimize the risks of user errors that may result in a breach.

However, there is a significant cost associated with some of these methods, especially if multiple defenses are layered to provide greater assurance. The more safeguards that are deployed, the greater the cost to put them in place and maintain them, and (often) the greater the burden placed on legitimate operations. There are no good metrics for security or risk to know how many safeguards are "enough" and where the weakest points might be. Thus, most organizations have some residual risks and potential exposures.

Nearly all software in use today has flaws and design weaknesses that may be exploited to gain unauthorized access. Vendors have not been held accountable for poor-quality code or lack of security features, and clients are often at the mercy of whatever is provided to them because of the terms of sale and licenses. They are further restricted by Federal laws such as the DMCA (Digital Millennium Copyright Act, PL 105–304), that make it illegal to use reverse engineering to determine what may be in licensed code — Federal law thus protects poor design and dangerous (even malicious) practices by vendors. These factors help ensure that most existing systems have flaws — discovered and yet to be discovered — and new systems will also likely be flawed, and thus vulnerable.

Accidental breaches are not uncommon, and organizations may be subject to exposure in this way, too.

It is because of all these residual risks that I presented, in my original testimony on May 4, USACM's 24 Privacy Principles. All of these principles, if embraced, will reduce the exposure and damage caused by any breach that does happen, and many will help reduce the likelihood of a breach.

2) Is it safer or less safe for companies to move personal information to cloud computing storage versus storing it on proprietary servers?

This question has multiple answers. "Cloud" has many different forms: there are different modes of deployment (public, community, private, hybrid) and different models service (IaaS, PaaS, SaaS; respectively, infrastructure, platform and software "as a service). "Safe" can also be construed in different ways — is the permanent loss of data from a disaster more or less safe than exposure of some of the data from a criminal breach? Furthermore, many cloud providers use proprietary technologies (hardware and software) to host their storage offerings, so that aspect is not necessarily meaningful.

usacm ACM US Public Policy Council

Considering the answer to question #1, note that protection and safety are ongoing efforts that have a continual and often substantial cost and labor component. Maintenance of the physical system and its security, software patches, defensive measures, personnel screening, and other issues need to be continually monitored and upgraded. For many organizations of all sizes, there is neither the expertise nor budget available to do these things on an ongoing basis. In these cases, outsourcing some of the storage and operations to a cloud service could be an improvement over in-house operation. However, for organizations with greater resources, it may be more reasonable to maintain internal systems with local operation and supervision (which could include a private cloud).

Cloud systems also introduce some new vulnerabilities. A cloud is a huge, tempting target. Vendors use software (usually called hypervisors) to manage resources and give each customer the illusion of having private resources. This software is another point to be attacked; the fact that malicious actors can become customers of the same cloud makes it easier. The relative weight of cloud-caused advantages and vulnerabilities is difficult to assess, and no doubt situation specific. Neither approach can make a decisive argument for being more secure.

Whatever factors may be involved, it is also important to note that the security of any storage depends greatly on the provider. If a cloud provider does not have adequate physical and logical security, the data resident on that storage will be at risk. It is also necessary to properly secure the communications between the clients and servers to prevent eavesdropping, and to institute appropriate safeguards at the clients to prevent breaches. A recent study by the Ponemon Institute indicated that most cloud providers believe it is the responsibility of the client to provide data security, while clients believe it is the responsibility of the cloud provider. This mismatch suggests that neither side may currently be providing the level of protection that is really needed.

Using cloud storage requires caution and a careful examination of the risks. In-house data storage can be secured by a variety of known technical approaches, such as air gaps (not connecting systems to any networks), firewalls, and data diodes (systems that only allow one-way communications). These and similar measures can reliably prevent or control outside access, but they are not applicable to any remote storage. The need for remote data protection forces significant reliance on cryptography.

Modern cryptography provides some protection, but is not a panacea as it is widely abused and misunderstood, resulting in substantial vulnerabilities. First, the keys to the ciphers are high value targets. Clouds are accessed over networks (most often the Internet) and the keys are therefore network-accessible, and thus subject to both technical attacks and social engineering attacks against operators. Second, user accounts that have access to the data may be subverted, negating all storage-level protections. Third, applications and hardware may be subverted (including supply chain attacks) to provide access to unencrypted data at both the client and server.

There are other avenues of exposure and breach beyond the access to storage. For example, some business partners may create specialized data sharing portals to support B2B (business to business) activities. If one of those partners has poor security practices, the B2B portal may serve as an avenue of penetration to a much more secure partner. Storage of data in a cloud system may enhance security by allowing sharing while obviating the need for a portal. However, if there is a mix of portals and cloud storage, weaknesses in the portal may enable attacks against the cloud storage.

1828 L Street, NW Suite 800
Washington, DC 20036

USACM.acm.org

202 659 9711 *tel*
202 667 1066 *fax*

usacm ACM US Public Policy Council

Another factor to consider is the physical, legal locale of the storage. Data that is stored on systems may be discoverable (or deleted, altered or disclosed) based on legal proceedings local to that cloud provider. The client also needs to worry about bankruptcy or financial judgments against the cloud provider that may result in the storage being sold or confiscated. In cases such as this, it is possible that the information on the disks could be sold or revealed as a side effect. In these instances, having strong encryption of the data with the cloud provider having no access to the keys may provide some protection, but as noted above, encryption may not be sufficient. Large organizations already confront these issues when choosing data center sites, and cloud vendors may offer some control for those who demand it. The real problem is that in conventional systems these concerns are more visible; the very ease of setting up cloud-based systems makes this and many other real difficulties simple to overlook.

Last of all, security is something that must be managed in an ongoing fashion. Thus, movement of data to a cloud storage location may be safer now, but as time goes on might be degraded if the cloud provider fails to adequately invest in, and maintain, appropriate defenses.

3) You testified you support legislation that would apply to all entities that collect personal information, including government. Do you think the government is ahead, equal, or behind the private sector in data security practices? Is there a difference between the different levels of government? How do the data security practices of universities and other non-profits compare to the public and private sectors?

"Government" may mean everything from a town of 300 to the National Security Agency. The resources of these entities are very different, as are the data, applications, and threats. Thus, it is possible to say that "government" is both behind and ahead of the private sector, depending on the definition of "government."

More specifically, protection of data is a function of many factors, including authority, budget, available resources, personnel, training, and risk. Most smaller governmental units do not have adequate resources or awareness of the threats and risks. As such, their systems are usually poorly protected. The same is true of some Federal agencies. Mid-sized governmental units (larger cities, most states, many Federal agencies such as NASA, FCC, etc.) may have better security, on average, than the median commercial entity, depending on their clientele and resources. Larger governmental units with high-level awareness of risk (largest cities, some states, national laboratories, Federal agencies such as NSA, FBI, etc.) are likely to have better security than most commercial entities.

NGOs and universities have different data protection needs than some public agencies. They also require a different level of access to resources. Thus, some smaller non-profits and educational institutions may have minimal security in place, and most of that is focused on only a portion of their mission. Other organizations that are frequent targets of attack, and universities with a strong local presence in computing, are likely to have stronger defenses in place. Some of these defenses are as good as those of a major Federal agency or large city.

There is no single, best answer to this question because there are no standards or metrics for security. Organizations often do not have a firm grasp of the risk to their operations and data, and even if they do, they are unable to tell when they have invested "enough" in defenses. Thus, they often do not deploy adequate resources to counter widespread and common threats. Standards and metrics for cyber security is one area sorely in need of more research and study.

1828 L Street, NW Suite 800
Washington, DC 20036

USACM.acm.org

202 659 9711 *tel*
202 667 1066 *fax*

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Responses of Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

To Additional Questions Submitted for the Record

Before the House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
"The Threat of Data Theft to American Consumers"

June 20, 2011

Chairman Bono Mack:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to respond to the Subcommittee's additional Questions for the Record on data breach and data security. I provide written answers to each of your three questions below. Please do not hesitate to let us know if we can be of further service to you in your continued efforts to protect consumers from data theft in an increasingly complex information ecosystem.

1. *In terms of timing of notification, there is a tension between telling people of a breach early, when the full picture may not be known, and waiting until more is known, in which case consumers may not be able to protect themselves. How do you balance those factors?*

CDT believes that businesses should not be required to report breaches prematurely — for example, a mandate of notification within 48 hours of the discovery of the breach could under some circumstances be an undue and counterproductive burden on a company acting in good faith to assess the scope of a breach and prevent further data losses. On the other hand, CDT does not believe businesses should have indefinite or inappropriately lengthy periods to conduct a risk assessment; otherwise it may be too late for victims to act to protect their interests once they are eventually notified. The Federal Trade Commission (FTC) has shied away from putting a specific time limit on notification, instead stating in response to this Subcommittee's questions that notification should occur "as soon as practicable." This position reflects most state laws. For example, California requires notification in the most expedient time possible, without unreasonable delay, consistent with the legitimate need of law enforcement and measures necessary to determine the scope of the breach

and restore the integrity of the system.[1] Other states, such as Wisconsin, require notification within a reasonable time, not to exceed 45 days after discovery of the breach.[2]

CDT supports the standard state language of notification without unreasonable delay, so long as an agency such as the FTC has oversight regarding what is reasonable. CDT would not necessarily be opposed to a specific time limit such as that articulated in Wisconsin law. However, before enacting a defined standards, businesses and consumers should be able to provide public input into what that time limit ought to be. One way to set an appropriate time limit may be to require the FTC to issue a Request For Information on the subject, or to authorize the FTC to issue implementing regulations pursuant to the Administrative Procedure Act on the topic as part of a federal data breach notification law.

2. *You advocate a "notify unless" approach, where a consumer should be notified of a breach involving their personal data unless there is an affirmative determination there is no serious risk of misuse of personal information. You testified that the use of appropriate technical safeguards that prevent unauthorized access should qualify for a determination that no serious risk of misuse exists. What would appropriate technical safeguards be?*

Appropriate technical safeguards are technologies and methodologies that are generally accepted by experts in the field of information security to render personal information unusable, unreadable, or indecipherable to unauthorized parties. However, the presumption that these methodologies and technologies protect the data should be rebuttable by facts indicating otherwise — such as in cases where both encrypted data and the encryption key are breached. Language to this effect appears in the White House Cybersecurity Legislative Proposal on data breach notification.[3] The Department of Health and Human Services (HHS) uses similar language for breaches of health data under HIPAA.[4]

Such methodologies should encompass strong encryption, hash functions, and data destruction consistent with guidelines from the National Institute of Standards and Technology. Because the field of data security evolves — sometimes rapidly — over time, the appropriate technical safeguards should also evolve to meet the threat environment. HHS, for example, has indicated that it would revisit its guidance on appropriate technical safeguards annually.[5]

3. *You advocate data minimization as a core principal for privacy legislation. What is the additional harm from collecting additional information?*

Data minimization is a fundamental component of the Fair Information Practices, a well-established set of principles that form the basis of many privacy laws, including the Privacy Act.

---

[1] Cal. Civil Code 1798.82(a).

[2] Wis. Stat. 134.98(3)(a).

[3] Legislative Language, Data Breach Notification, Executive Office of the President, Office of Management and Budget, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Data-Breach-Notification.pdf, § 102(b)(1)(A).

[4] 45 CFR 164.402.

[5] 74 Fed. Reg. 42740.

The data minimization principle urges businesses to collect and retain only that information which they need for a specific business purpose.

Opinion polls have routinely indicated that Americans have significant concerns about businesses and government agencies collecting and using their personal information.[6] The routine overcollection of personal information can weaken consumers' trust in online services — a vital part of the modern economy.[7]

Businesses that retain sensitive information beyond the period for which that information has a specific use also increase the risk of a severe data breach. For instance, one of Sony's recent data breaches included information from an outdated 2007 database containing the bank and credit accounts of tens of thousands of individuals.[8] The more sensitive information an entity holds, the greater the risk that the information can be compromised, and information that has outlived its business purpose may not necessarily receive the attention necessary to ensure it remains secure.

CDT does not believe that government should issue one blanket directive prescribing the timing of destruction of all consumer data across a range of disparate industries. Such a statutory mandate could inadvertently freeze today's practices into law and discourage future innovation. However, meaningful and flexible data minimization procedures could be enacted either through some combination of legislation requiring reasonable data minimization requirements, FTC rulemaking or guidance, and government-approved industry safe harbor programs.[9] Furthermore, requiring through legislation that businesses periodically review their data holdings with an eye towards removing excess or unnecessary data could also significantly improve information security.

Thank you again for the opportunity to provide testimony to the Subcommittee on this important issue.

For more information, contact Justin Brookman, justin@cdt.org, (202) 637-9800.

---

[6] *See, e.g.*, Byron Achohido, *Most Google, Facebook Users Fret over Privacy*, Feb. 9, 2011 http://www.usatoday.com/tech/news/2011-02-09-privacypoll09_ST_N.htm.

[7] Don Davis, *Consumer Privacy Fears Limit the Growth of m-Commerce, Forrester Finds*, INTERNET RETAILER, June 17, 2011, http://www.internetretailer.com/2011/06/17/barriers-mobile-commerce-growth; Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Department of Commerce "Green Paper" report on commercial privacy), Department of Commerce Internet Policy Task Force, Dec. 16, 2010 http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf at 15 (stating "commenters widely recognized that an erosion of trust will inhibit the adoption of new technologies").

[8] Ian Sherr, *Hackers Breach Second Sony Service*, WALL STREET JOURNAL, May 2, 2011 http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw#articleTabs%3Darticle.

[9] *See* Testimony of Leslie Harris before the House Energy and Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection, The Best Practices Act of 2010 and Other Consumer Privacy Legislation, July 22, 2010, http://democrats.energycommerce.house.gov/documents/20100722/Harris.Testimony.07.22.2010.pdf.

○