SECURING CONSUMERS' DATA: OPTIONS FOLLOWING SECURITY BREACHES

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 11, 2005

Serial No. 109–14

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE
21–635PDF WASHINGTON : 2005

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi, *Vice Chairman*
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *Deputy Staff Director and General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas,
(Ex Officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
MIKE ROSS, Arkansas
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
BOBBY L. RUSH, Illinois
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

SECURING CONSUMERS' DATA: OPTIONS FOLLOWING SECURITY BREACHES

WEDNESDAY, MAY 11, 2005

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

The subcommittee met, pursuant to notice, at 11:05 a.m., in room 2123 of the Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Upton, Cubin, Radanovich, Bass, Pitts, Bono, Terry, Rogers, Myrick, Murphy, Blackburn, Barton (ex officio), Schakowsky, Ross, Markey, and Baldwin.

Staff present: David Cavicke, chief counsel; Chris Leahy, policy coordinator; Will Carty, professional staff; Larry Neal, deputy staff director; Billy Harvard, clerk; Kevin Schweers, communications director; Lisa Miller, press secretary; Consuela Washington, minority counsel; Turney Hall, staff assistant; and Alec Gerlach, staff assistant.

Mr. STEARNS. Good morning. The subcommittee will come to order. My colleagues, today we continue the subcommittee's examination of consumer data security and identity theft. As all of us are keenly aware, our important work is set against the backdrop of almost daily reports of consumer data, security breaches at data brokers, retailers, banks, universities, and the list, of course, goes on. It seems like every corner of our economy has been touched. Understandably, the public is worried. The reported breaches involve everything from elaborate high-tech hacker attacks to simply theft of physical consumer data that had been poorly secured in the first place.

The consumer impact of these breaches has been just as varied. Some cases never result in identity theft or financial loss, while others affect significant consumer populations. With some estimates of those affected ballooning past initial numbers as further investigations reveal even larger cracks in the digital infrastructure.

And while our initial assessment of the extent of this problem for consumers and businesses is still a bit fuzzy, the cracks and vulnerabilities are becoming more apparent to the committee and to the public. Questions are starting to be raised about the inherent security of a large segment of the commercial marketplace. This should concern all of us. The committee understands this con-

cern, and to address it, there are a number of issues that need careful examination.

First, we must ensure that existing Federal law does not leave open ways for certain entities to skirt the objectives of the primary laws governing such areas, including the Fair Credit Reporting Act and the Gramm-Leach-Bliley.

Second, if we determine that existing law is inadequate, we need to get a clearer and more accurate assessment of the scope of the problem across all sectors, assess the current legal tools we have to attack it, and weigh the need for additional regulation and other approaches. Other non-regulatory approaches could include applying good old American technological ingenuity to buttress current consumer data security regulations.

Throughout this series of hearings, we have heard from a number of experts that data security breaches go hand in hand with identity theft, a phenomenon that keeps getting larger and more insidious. The numbers are sobering. At our March hearing, the FTC testified that over 10 million people were victims of identity theft during the 1-year period of its latest survey. The FTC estimated that this figure translates into loss of nearly $48 billion for businesses, almost $5 billion for consumers, and close to 300 million hours spent by those individuals and businesses trying to resolve the problems just generated by these crimes.

We cannot allow our consumer economy to be undermined by these criminals. Consumers, businesses, and the public sector needs to strengthen defenses collectively. The reality is that the bad guys will always be around. It is up to us as consumers, businesses, and public institutions to make sure that our data is locked down and is accounted for. The best offense to combat identity theft is simple prevention coupled with an assurance that entities dealing in consumer data adhere to consistent and comprehensive security standards with a bite.

The accessibility and portability of consumer data in an information-driven market has made controlling who has access to what more difficult than ever. Consumer data breaches and as a result in identity theft continues to grow and affect broader commercial activity at all levels, not just a specific industry or a specific sector.

Consumer data in our modern markets has become a commodity. It is bought and sold. It is processed and analyzed. And it is now an integral ingredient in disciplines as varied as finance, demographics, research, direct marketing, academic study, and law enforcement. I believe the majority of these activities improve our lives and well-being. They make us more productive, allow a higher standard of living, and afford us better personal and national security, particularly in a post-9/11 world.

What it is lacking, my colleagues, however, is a safeguard system in which our personal data is shielded by a robust security no matter where it goes or whoever possesses it. We need to examine approaches that enable robust security measures to surround personal data as it speeds through commerce.

I think this is where advanced technology can play a larger role in helping reduce the incidence of identity theft. Technologies like sophisticated encryption techniques, advanced password authentication systems, as well as better and more widespread use of ad-

vanced data security software all can play an important role in improving our defenses. Technology can also be used to facilitate more uniform best practices in affected sectors that deal in consumer data.

Let me be clear. I do believe that additional measures are necessary, but for those still undecided, this hearing and the proceedings should provide a great deal of information to help everyone make a judgment call here. I think it is a fair thing to say that one thing is certain—criminals cannot be allowed to capitalize on another high-tech nefarious business model to steal and defraud American consumers, businesses, and public institutions. We have seen this happen with spyware and spam. It can't be allowed to happen here.

Therefore, our focus needs to be on first, clearly identifying what is not working before we act on a national scale. But with each new breach we are losing more valuable time to put an end to a new breed of professional cyber criminals and the inappropriate and illegal activities that are slowly corroding consumer confidence in the integrity of information-driven commerce and technology.

I would like to thank our distinguished panel for being here this morning and for joining us today, and we look forward to your testimony. With that, the ranking member, Ms. Schakowsky.

[The prepared statement of Hon. Cliff Stearns follows:]

PREPARED STATEMENT OF HON. CLIFFORD STEARNS, CHAIRMAN, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

Good Morning. Today, we continue the Subcommittee's examination of consumer data security and identity theft. As all of us are keenly aware, our important work is set against the backdrop of almost daily reports of consumer data security breaches at data brokers, retailers, banks, universities—and the list goes on. It seems like every corner of our economy has been touched. Understandably, the public is worried. The reported breaches involve everything from elaborate high-tech hacker attacks to simply theft of physical consumer data that had been poorly secured. The consumer impact of these breaches has been just as varied. Some cases never result in identify theft or financial loss while others affect significant consumer populations, with some estimates of those affected ballooning past initial numbers as further investigation reveals even bigger cracks in the digital infrastructure. And while our initial assessment of the extent of this problem for consumers and businesses is still a bit fuzzy, the cracks and vulnerabilities are becoming more apparent to the Committee and to the public. Questions are starting to be raised about the inherent security of a large segment of the commercial marketplace. This should concern us all.

The Committee understands this concern. And to address it, there are a number of issues that need careful examination. First, we must ensure that existing federal law is not leaving open ways for certain entities to skirt the objectives of the primary laws governing this area, including the Fair Credit Reporting Act and Gramm-Leach-Bliley. Second, if we determine that existing law is inadequate, we need to get a clearer and more accurate assessment of the scope of the problem across all sectors, assess the current legal tools we have to attack it, and weigh the need for additional regulation and other approaches. Other non-regulatory approaches could include applying good old American technological ingenuity to buttress current consumer data security regulations.

Throughout this series of hearings we have heard from a number of experts that data security breaches go hand in hand with identify theft—a phenomenon that keeps getting bigger and more insidious. The numbers are sobering. At our March hearing, the FTC testified that over 10 million people were victims of identity theft during the one-year period of its latest survey. The FTC estimated that this figure translates into loses of nearly $48 billion for businesses, almost $5 billion for consumers, and close to 300 million hours spent by those individuals and businesses trying to resolve the problems generated by these crimes. We cannot allow our consumer economy to be undermined by these criminals. Consumers, business, and the

public sector need to strengthen defenses collectively. The reality is that the bad guys will always be around. It is up to us as consumers, businesses, and public institutions to make sure that our data is locked down and accounted for. The best offense to combat identity theft is simple prevention coupled with an assurance that entities dealing in consumer data adhere to consistent and comprehensive security standards with bite.

The accessibility and portability of consumer data in an information-driven market has made controlling who has access to what more difficult than ever. Consumer data breaches and resultant identity theft continues to grow and affect broader commercial activity at all levels, not just a specific industry or sector. Consumer data in our modern markets has become a commodity. It is bought and sold. It is processed and analyzed. And it is now an integral ingredient in disciplines as varied as finance, demographic research, direct marketing, academic study, and law enforcement. I believe that the majority of these activities improve our lives and wellbeing. They make us more productive, allow higher standards of living, and afford us better personal and national security, particularly in a post 9/11 world. What is lacking, however, is a safeguard system in which our personal data is shielded by robust security no matter where it goes or who possess it. We need to examine approaches that enable robust security measures to surround personal data as it speeds through commerce.

I think this is where advanced technology can play a larger role in helping reduce the incidence of identity theft. Technologies like sophisticated encryption techniques, advanced password authentication systems, as well as better and more widespread use of advanced data security software all can play an important role in improving our defenses. Technology can also be used to facilitate more uniform best practices in affected sectors that deal in consumer data.

Let me be clear, I do believe that additional measures are necessary. But for those still undecided, this hearing and the preceding ones should provide a great deal of information to make a judgment. I think it's fair to say that one thing is certain—criminals cannot be allowed to capitalize on another high-tech, nefarious business model to steal and defraud American consumers, business, and public institutions. We've seen that happen with spyware and spam. It can't be allowed to happen here. Therefore, our focus needs to be on first clearly identifying what is not working before we act on a national scale. But with each new breach, we are losing more valuable time to put an end to a new breed of professional cyber-criminal and the inappropriate and illegal activities that at are slowly corroding consumer confidence in the integrity of information-driven commerce and technology.

I would like to thank our distinguished panel of witnesses for joining us today. We look forward to your testimony. Thank you.

Ms. SCHAKOWSKY. Once again I want to thank you, Chairman Stearns, for holding a hearing on how we can further protect consumers from the stealing of their most personal information. We need to close the canyon-size gaps in the law that are putting consumers and their sensitive, private information at serious risk of invasion—identity theft and other crimes.

I look forward to hearing from our witnesses today about their ideas of what we can do, and I look forward to working with you, Chairman Stearns and Chairman Barton and Ranking Member Dingell and Representative Markey and others, on legislation to restore consumers' control of private information.

The Privacy Rights Clearinghouse has been keeping an ongoing tally of data breaches revealed since news first broke on the ChoicePoint incident. In the past 3 months alone we have learned that approximately 4,736,400 individuals have had their personally identifiable information compromised. Again, that is in just months. And those are the cases about which we know.

The means of access are varied. Computers have been hacked and stolen, backup tapes lost, passwords compromised, information exposed online, and fake businesses established. And it has not just been the data brokers' stockpiles that have been raided. University stores, banks, and government offices have seen their data bases breached and their students, alumni, customers, and constituencies

exposed. If there is personal information to be had, there are criminals out to get it from anyplace and in any way they can.

From the recent wave of breaches we know data insecurity is endemic, and it is time for us to close whatever loopholes there are in privacy laws to ensure that consumers are not stuck with the short end of the stick as they are now. We need to address privacy and data security with comprehensive legislation governing the handling and use of personal and consumer information. I believe we should explore the possibility of giving consumers the power to lock up their information, making it available only when consumers give affirmative consent. We should also look into giving consumers the opportunity to inspect their information, and if it is not accurate, then a chance to correct it. We should also place a heightened responsibility on record keepers to ensure that they are truthfully representing consumers. And we should give victims of lost or stolen information a place to turn, like an office of an omdetsman in order to help them through repairing whatever damage has been done by their information being compromised. We also need to explore the government's use of information compiled by data brokers to make sure that Big Brother is not handing the binoculars to Big Business in order to skirt the Privacy Act.

Inaccuracies can cost people their jobs, insurance, the right to vote, good credit histories, or even their lives. I believe that if consumers have the tools, resources, and the rights to protect their personal information, and if companies were held to a higher standard of accountability, we would not have 4.7 million letters being sent out over 3 months warning consumers that their information could be in the hands of criminals.

We need to keep in mind that perhaps the only reason we know about these breaches is because of tough State laws like California's that made sure these breaches were reported. If those companies with security breaches had to comply only with Federal legislation, there is a good chance we would be hearing from more and more identity theft victims and had no idea what was going on to cause the potential upsurge.

When we craft the legislation to contend with data insecurity, we need to provide a floor and not a ceiling for how personal information is handled and protected. Let the States pressure us to do better instead of us limiting what they can do.

Again, Chairman Stearns, I look forward to working with you and the other members of our committee to do what we can to protect consumers. I thank you.

Mr. STEARNS. I thank the gentlelady. The gentlelady from California, Ms. Bono.

Ms. BONO. Thank you, Mr. Chairman. I just would like to thank you for holding this hearing, but I will waive an opening statement.

Mr. STEARNS. The gentlelady waives. Mr. Ross, is he here? Ms. Baldwin? No. The gentlelady waives. Mr. Pitts, gentleman—waive. Mr. Markey?

Mr. MARKEY. Thank you, Mr. Chairman, very much. Mr. Chairman, in "Bonfire of the Vanities" the novelist Tom Wolfe wrote about "the Bororo Indians, a primitive jungle tribe who live along the Vermelho River in the Amazon Jungles of Brazil." According to Wolfe, the Bororos believed that "there is no such thing as a pri-

vate self." Instead, they "regard the mind as an open cavity, like a cave or a tunnel or an arcade, if you will, in which the entire village dwells and the jungle grows." Wolfe compared this to the situation faced by someone in the middle of a public scandal in the last quarter of the 20th century, when he suggested "one's self—or what one takes to be oneself—is not a mere cavity open to the outside world but has suddenly become an amusement park to which everybody, todo el mundo, tout le monde, comes scampering, skipping and screaming, nerves a-tingle, loins aflame, ready for anything, all you have got, laughs, tears, moans, giddy thrills, gasps, horrors, whatever, the gorier the merrier."

In the 21st Century, Mr. Chairman, we now face the prospect of a world in which all of us—not just Sherman McCoy's caught in the midst of scandal—will be forced to live without a private self: with the entire "village" able to obtain access to some of the most personal aspects of our lives.

In the emerging surveillance society of the 21st Century, the Bororo Indians seeking to inhabit our private selves are the data mining and information brokerage firms. These companies are collecting and selling a vast array of personal information about the American public. For a fee, these companies will tell you someone's Social Security number, their address, phone number, driver's license number, driving record, any criminal record information, court records, insurance claims, divorce records, and even credit and financial information.

Recent press reports have chronicled the adverse privacy consequences of this phenomenon. As we have seen company after company acknowledging that the security and confidentiality of the personal information it holds about American citizens has been compromised. Each week the list of companies who have suffered data security breaches or acknowledged lax practices with respect to access to sensitive personal data has grown longer and longer.

I have introduced three bills aimed at addressing the current threats to personal privacy. My first bill, the Information Protection and Security Act, would subject information brokers to regulation by the Federal Trade Commission, and specifically to a set of new, fair information practice rules that the FTC would be required to issue within 6 months of enactment.

The FTC rules would address the security of information held by information brokers, the right of consumers to obtain access to incorrect information held by the broker, the responsibility of the broker to protect the information from unauthorized users or from users seeking the information for impermissible and unlawful purposes. The bill also provides the enforcement of the bill's substantive provisions by the FTC, the State Attorney General, and a private right of action.

My second bill would generally restrict the purchase and sale of Social Security numbers. And my third bill would allow consumers to block a company from transferring their personal information to entities located in countries that fail to provide adequate and enforcement privacy protection.

In other words, the outsourcing of privacy to countries like India and Pakistan that do not have privacy laws in conformance with the EU or with the United States of America. Our x-rays should

not be going to be read in countries that do not have the same privacy laws which we have. Our tax records should not be going there, our financial records should not be going there, our health records should not be going there. These are personal records to go to the very identity of us as Americans and as a people. I thank you, Mr. Chairman, for having this very important hearing.

[The prepared statement of Hon. Edward J. Markey follows:]

PREPARED STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Thank you, Mr. Chairman.

In Bonfire of the Vanities, the novelist Tom Wolfe wrote about "The Bororo Indians, a primitive jungle tribe who live along the Vermelho River in the Amazon Jungles of Brazil." According to Wolfe, the Bororos believed that "there is no such thing as a private self." Instead, they "regard the mind as an open cavity, like a cave or a tunnel or an arcade, if you will, in which the entire village dwells and the jungle grows." Wolfe compared this to the situation faced by someone in the middle of a public scandal in the last quarter of the 20th century—when, he suggested:

> "... one's self—or what one takes to be one's self—is not a mere cavity open to the outside world but has suddenly become an amusement park to which everybody, *todo el mundo, tout le monde,* comes scampering, skipping and screaming, nerves a-tingle, loins aflame, ready for anything, all you've got, laughs, tears, moans, giddy thrills, gasps, horrors, whatever, the gorier the merrier."

In the 21st Century, we now face the prospect of a world in which all of us—not just the Sherman McCoy's caught in the midst scandal—will be forced to live without a private self—with the entire "village" able to obtain access to some of the most personal aspects of our lives.

In the emerging surveillance society of the 21st Century, the Bororo Indians seeking to inhabit our private selves are the data mining and information brokerage firms. These companies are collecting and selling a vast array of personal information about the American public. For a fee, these companies will tell you someone's Social Security Number, their address, phone number, driver's license number, driving record, any criminal record information, court records, insurance claims, divorce records, and even credit and financial information.

Recent press reports have chronicled the adverse privacy consequences of this phenomenon, as we have seen company after company acknowledging that the security and confidentiality of the personal information it holds about American citizens has been compromised. Each week, the list of companies who have suffered data security breaches, or acknowledged lax practices with respect to access to sensitive personal data, has grown longer and longer.

I have introduced three bills aimed at addressing the current threats to personal privacy. My first bill, the "Information Protection and Security Act," would subject information brokers to regulation by the Federal Trade Commission, and specifically, to a set of new fair information practice rules that the FTC would be required to issue within 6 months of enactment. The FTC rules would address the security of information held by information brokers, the right of consumers to obtain access to and correct information held by the broker, the responsibility of the broker to protect the information from unauthorized users, or from users seeking the information for impermissible or unlawful purposes. The bill also provides for enforcement of the bill's substantive provisions by the FTC, the State Attorney's General, and a private right of action.

My second bill, H.R. 1078, would generally restrict the purchase or sale of Social Security numbers, which has become a ubiquitous personal identifier used by corporations and identity thieves to access sensitive personal information.

My third bill, H.R. 1653, would allow consumers to block a company from transferring their personal information to entities located in countries that fail to provide adequate and enforceable privacy protections.

All three of these bills have been referred to this Subcommittee, and I look forward to hearing the testimony of the witnesses at this morning's hearing, and to discussing the proposals set forth in these bills with them.

Mr. STEARNS. I thank my colleague for a very thoughtful opening statement. And we are going to Mr. Terry. Mr. Terry waives. Ms. Cubin.

Ms. CUBIN. Thank you, Mr. Chairman, and thank you for holding this timely hearing. It is especially timely for me. I also want to thank the witnesses that are here today who have joined us to help us hopefully guide us on shaping future legislation regarding personal data security.

Throughout my tenure on this subcommittee we have continuously addressed issues regarding privacy protection and the ability of third parties to access and distribute personally identifiable information. Though there are most certainly valid and necessary uses of personal data collection, recent breaches of seemingly secure data have demonstrated that there are just as many opportunities for criminal use of this information.

Identify theft, as we all know, is a whole new realm of crime, and America does not currently have the proper legal tools to prevent it, rectify it, or mitigate it. ID theft can invade people's homes, bank accounts, financial assets, often undetected. This can be devastating to victims and Congress must determine the best course of action to help this from happening.

As I said, I think this hearing is timely because just on Monday of this week I was notified that I was one of over 96,000 people in one incident and one of 1.4 million people in another affected by an identity theft incident. According to a letter that I received from the companies to notify me of this breach, stolen personal information included bank account numbers and driver's license numbers and other information that's provided on checks. While I was lucky enough I think—I am not sure at this point—that my Social Security number wasn't stolen and that my address wasn't stolen, millions of Americans aren't that lucky—if you want to call my situation lucky.

Financial institutions whose systems have been breached have an immediate responsibility to notify victims as well as to provide an explanation of the breach of the security system, which did happen with me. Once again I thank—I hope that I was notified of everything. I am hopeful that today's hearing will outline what other further steps must be taken to assist us in identifying victims and rectifying fraudulent bank transactions and correcting inaccurate file information for future dissemination.

I hope this subcommittee will continue to examine this issue in the light of the need for harsher punishment for both data thieves and commercial entities who forfeit personal information, albeit unintentionally.

I thank the chairman and I yield back the balance of my time.

[The prepared statement of Hon. Barbara Cubin follows:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this timely hearing.

I would also like to thank the witnesses who have joined us here today. As we found during the previous hearing, the current laws governing data security are very complex. I anticipate an open dialogue with the panel of witnesses to help guide Members of the Subcommittee in shaping future legislation regarding personal data security.

Throughout my tenure on this subcommittee, we have continuously addressed issues relating to privacy protection and the ability of third parties to access and distribute personally identifiable information. Though there are most certainly valid and necessary uses of personal data collection, recent breaches of seemingly secure

data have demonstrated that there are just as many opportunities for criminal use of this information. Identity theft is a whole new realm of crime, and America does not currently have the proper legal tools to prevent, rectify or mitigate it. ID theft can invade people's homes, bank accounts, and financial assets, often undetected. This can be devastating to victims, and Congress must determine the best course of action to halt this crime.

I myself have just recently been notified that I was a one of over 1.4 million people affected by the DSW identity theft incident. According to the letter DSW sent to notify me of this breach, stolen personal information included bank account and drivers license numbers provided on checks. While the stolen information did not include names, addresses, or Social Security numbers, millions of Americans affected in other data theft incidents have not been so lucky. It is crucial we call attention to the need for consumers to have proper recourse. Financial institutions whose systems have been breached have an immediate responsibility to notify victims, as well as provide an explanation of the nature of the system's breach. I am hopeful today's hearing will outline what further steps must be taken to assist identity theft victims in rectifying fraudulent bank transactions and correcting inaccurate file information for future dissemination.

I hope the subcommittee will continue to examine this issue in light of the need for harsher punishment for both data thieves and the commercial entities who forfeit personal information, albeit unintentionally. I thank the chairman, and I yield back the balance of my time.

Mr. STEARNS. I thank the gentlelady, and it is very appropriate that you bring to our attention that letter. And I thank you very much, and I think that lends credence to why we are attempting to grapple with this problem to come up with a solution. Mr. Radanovich? The gentleman waives. Ms. Myrick?

Ms. MYRICK. I waive also.

Mr. STEARNS. Okay. I think everybody has completed their opportunity for an opening statement. We move now to our witness list. And we welcome them. Before I start, Mr. Ross would like to make an introduction. Mr. Ross.

Mr. ROSS. Thank you, Mr. Chairman and Ranking Member Schakowsky for having this important hearing today to address the issue of protecting consumers' data. I am pleased that we have Jennifer Barrett to testify from Acxiom, which is located in my home State of Arkansas.

Since it was founded in 1969, Acxiom has used technology and consumer data to help some of the largest, most respected companies in the world improve their business results. Acxiom is based in Little Rock, Arkansas and employs more than 6,300 people in eight countries with an annual revenue of about $1.2 billion.

Jennifer Barrett is the chief privacy officer of Acxiom Corporation and is one of the world's leading authorities on information practices and policies and their impact on consumers, commerce, and the global economy. Jennifer has been with Acxiom almost since its inception after earning a degree in computer science and mathematics from the University of Texas, which those of us in Arkansas do not hold against her. She has worked at almost every facet of the company. In the early 1990's she became one of the first executives in any industry to become what is now commonly referred to as a chief privacy officer, assigned to help her company and its clients achieve the critical balance of protecting consumer privacy while preserving the benefits of this new information age. Jennifer is now sought out by leading companies, international business leaders, lawmakers, regulators, and many others for her counsel and views on the responsible uses of data. She has appeared many times before committees and forums here in Wash-

ington, and we appreciate her again offering her insights to us today. So I would like to thank you, and I look forward to the testimony from Mrs. Barrett as well as the other witnesses on the panel today and the questions from the members here as well.

Mr. STEARNS. I thank my colleague.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. GEORGE RADANOVICH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, I would like to thank you for holding this important hearing today on securing consumers' data.

With recent reports from the Federal Trade Commission's study survey indicating that over 10 million people were victims of identity theft during a one year period and estimates that translate into $48 billion loss for businesses and $5 billion loss for consumers, I believe it is evident that the time is right for Congress to determine what needs to be done to protect our constituents from these thieves.

I am happy to report that California has been one of the most active state governments in regulation data security. In 2002 California passed a consumer security breach notification law that requires any state agency, or any person or business that owns or licenses computerized data that includes personal information to disclose any breach of security of the data to any resident of that state whose unencrypted information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to California I would like to commend the states of Georgia, Texas and Illinois who are considering similar legislation.

As we hear from our witnesses today it is important to determine if the current federal laws are sufficient to protect the data security of consumer's and if technologies exist that could aid in protecting sensitive consumer data and prevent unauthorized access to computerized databases.

Recent reports of data security breaches by data brokers, financial institutions, and retailers have raised questions about the sufficiency of current laws to protect consumer information from identity theft.

During the Subcommittee's March hearing on issues related to the Choicepoint breach, the FTC testified that the results of a recent FTC study indicated that over 10 million people were victims of identity theft during the one year period the study's survey covered. The FTC estimates that the losses translate into $48 billion for businesses and $5 billion to consumers.

While there are Federal laws that provide standards for disclosure of consumer information and require certain entities to take steps to safeguard consumer information, there is NO comprehensive Federal law dealing with data security that governs ALL uses of consumer data. There are two main bodies of Federal law that deal with privacy and data security related to certain types of entities and certain uses of information: The Fair Credit Reporting Act and the Gramm-leach Bliley Act; however the universe of entities to which these bodies of law apply is limited.

Several other states have passed or are considering similar legislation, including GA, TX, and Il. A number of federal bills introduced in this Congress are modeled after the CA statute.

The social security number was created to identify each U.S. citizen for the sole purpose of tracking employment and benefits however, over time our social security number has been used by both public and private entities for purposes both related and unrelated to the social security program. The usage of this unique identifier has benefited both businesses and consumers, but unfortunately it has led to misuse and most importantly identity theft.

The FTC has reported that over 10 million people were victims of identity theft in one year and they estimate that this translates into upwards of a $48 billion loss for businesses and $5 billion loss for consumers, but a price tag can not be put on the loss of one's identity.

I look for to hearing our witness' testimony today. Hopefully this will help us determine if our current laws are adequate enough to protect the integrity of our social security numbers and if not, what we need to do to protect them.

PREPARED STATEMENT OF HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you Mr. Chairman for holding this hearing today. I have spent considerable time focusing on information security issues such as the spyware legislation

that this Committee passed unanimously. I'm confident that that bill will be received favorably by the full House as well. Our Committee's work on these issues will continue in earnest, particularly in light of the alarming and ever-growing list of data security breaches recently.

Nothing seems safe. In recent months, we have learned about the loss of personally identifiable information—even including Social Security numbers—from ChoicePoint, LexisNexis, Blockbuster, as well as a company called RuffaloCODY that manages information systems for a number of colleges and universities. Most recently, data tapes belonging to Time Warner were stolen from a storage company called Iron Mountain—a company, I might add, that also stores some sensitive information for the Congress. I suspect that there are more thefts of this nature about which we have not yet learned.

This is simply unacceptable.

In the Internet age, personal information can be accessed in any number of ways and from any number of outlets. To not guard it closely is to open the door to thieves. Sensitive personal information must be secure, and companies that legally gather and distribute this information need to be held accountable if they do not take reasonable steps to ensure that security.

The recent breaches have focused our attention on "data brokers"' who compile public and non-public information in ways that seem downright Orwellian. They can share it, rent it, and sell it. Constraints on these companies and their practices are few and thin. Some of these companies provide an important service for individuals trying to protect their families or investments, as well as for the government trying to protect us all. It is essential that only those who have an appropriate, legitimate reason for having access to such information are allowed to view it. Those who provide this access must be responsible for verifying both the legitimacy of the business or person inquiring, as well as the appropriateness of their reason for doing so. Of course, other entities such as credit card companies, department stores—even the video store, as I mentioned—have sensitive information as well. They must be similarly responsible with the data, and take vigorous steps to protect it.

Congress has not laid out a comprehensive framework for data security and data brokers, and it is clear that we need to act. This Committee must take the lead in developing appropriate safeguards for consumer information, and we will proceed to that end on a bipartisan basis. I am glad that Chairman Stearns has put together a diverse panel to discuss this topic, and to explore options for how we as policymakers can help address the concerns of the American public.

With that, I would like to welcome the witnesses and thank them for their participation. I am very interested to hear what these companies and their industries are doing to help prevent identity theft, and the misuse of personal information in general.

Thank you, and I yield back the balance of my time.

PREPARED STATEMENT OF HON. ED TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you Mr. Chairman for holding this important hearing. Since we last met, the privacy of our constituents has been compromised further and their worries have increased ten-fold. I was encouraged by the feedback that we received in our hearing this past March, but there is much more work to be done.

I was pleased to learn that banks and credit card companies are detecting fraud at a quicker rate and successfully shutting down information-sharing websites before identity theft becomes more rampant and uncontrollable. While I understand that stolen or lost credit cards still account for the largest losses to consumers, the danger these on-line thieves pose must be confronted and dealt with.

According to an article in Monday's Wall Street Journal, the Anti-Phishing Working Group says 2,870 active phishing sites were reported in March alone, and that since last July such sites have increased 28% a month. The article goes on to state that about 980,000 American consumers had encountered identity-theft fraud via phishing in the prior year, costing banks and credit card issuers more than $1.2 billion in direct losses.

I have had a long-standing interest in protecting consumers' privacy. I first began advocating for safeguarding medical records when I found my own records in a public trash bin following a doctor's appointment. In response, I introduced a bill protecting the privacy rights of insurance claimants, which became part of HIPPA.

Since last Congress, I have been working with my colleague, Congresswoman Mary Bono to protect consumers' privacy on the internet from Spyware. Our com-

mittee passed this bill last week and I am hopeful that we can send it to the President's desk before the end of this year.

I look forward to hearing from our witnesses about what went wrong in these recent cases and how we can better protect consumers.

Thank you Mr. Chairman. I yield back the balance of my time.

Mr. STEARNS. We want to welcome Ms. Barrett of Acxiom Corporation; also Mr. Steve Buege, Senior Vice President of Business Information, News and Public Records, North American Legal; Thomson West; Mr. Oliver Ireland, Partner, Financial Services Practice Group, Morrison and Foerster; on behalf of Visa U.S.A., Mr. Daniel Burton, Vice President of Government Affairs, Entrust, Incorporated, McLean, Virginia; and Mr. Daniel Solove, Associate Professor of Law at George Washington University Law School. I thank all of you for attending this morning. And, Ms. Barrett, we will start with you for your opening statement.

STATEMENTS OF JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION; STEVE BUEGE, SENIOR VICE PRESIDENT, BUSINESS INFORMATION, NEWS AND PUBLIC RECORDS, NORTH AMERICAN LEGAL; OLIVER I. IRELAND, PARTNER, FINANCIAL SERVICES PRACTICE GROUP, MORRISON AND FOERSTER, LLP, ON BEHALF OF VISA USA; DANIEL BURTON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, ENTRUST, INC.; AND DANIEL J. SOLOVE, ASSOCIATE PROFESSOR OF LAW, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Ms. BARRETT. Thank you, Chairman Stearns, Ranking Member Schakowsky, Congressman Ross, and distinguished members of this committee. I thank you for the opportunity for Acxiom to participate in this hearing, and I ask for unanimous consent that my written statement be entered in the record.

Mr. STEARNS. By unanimous consent, so ordered.

Ms. BARRETT. Mr. Chairman, let me be blunt. The bad guys are smart and they are getting better organized in using their skills to intelligently but illegally and fraudulently access personal information. Acxiom must therefore remain more vigilant and innovative by constantly improving, auditing, and testing our systems, and yes, even learning from the security breaches in the marketplace.

Information is an integral part of the American economy, and Acxiom recognizes its responsibility to safeguard the personal information it collects and brings to the market. As FTC Chairman Majoras recently stated in her testimony both before the Senate and the House, "There is no such thing as perfect security." And breaches can happen even when a company has taken every reasonable precaution. Although we believe this to be true, no one has a greater interest than Acxiom in protecting its information because our very existence depends on it.

Acxiom's U.S. business includes two distinct components: our customized computer services and a line of information products. Our computer services, which represent more than 80 percent of the company's business, help businesses, not-for-profit organizations, political parties, and government manage their own information. Less than 20 percent of our business comes from our four lines of products involving information—our fraud management products, our background screening products, our directory prod-

ucts, and our marketing products. Our fraud management and background screening products are the only Acxiom products containing sensitive information, and they represent less than 10 percent of our business.

Acxiom would like to take this opportunity to set the record straight in response to a couple of misunderstandings that have developed about the company. First, Acxiom does not maintain one big data base containing dossiers on anyone. Instead, we build and maintain discrete, segregated data bases for each and every product.

Second, Acxiom does not co-mingle client information that comes from the services we provide to our clients with their information products, which we are responsible for. Such activity would constitute a violation of our contracts and consumer privacy.

Third, Acxiom's fraud management products are sold only to a handful of large companies and government agencies who have a legitimate need for them. The information utilized in these products is covered under the safeguards and use rules of the Gramm-Leach-Bliley Act and both State and Federal driver privacy protection laws.

Fourth, Acxiom's fraud management verification services only validate information already in our client's possession. Access to additional information is available only to law enforcement and the internal fraud departments of large financial institutions and insurance companies.

Fifth, our background screening products are covered under the Fair Credit Reporting Act, and we do not pre-aggregate information provided in these services.

Beyond these protections, the following additional safeguards exist: first, because public record information is blended with regulated information in both our fraud management and our background screening products, Acxiom voluntarily applies the more stringent security standards to all such blended data, even though not required to by law. Since 1997 Acxiom has posted a privacy policy on our website describing both our online and all our offline practices, thus voluntarily subjecting the company to the FTC rules governing unfair or deceptive practices. Third, the company has imposed our own internal, more restrictive guidelines for use of sensitive information such as Social Security numbers. And fourth, all of Acxiom's information products and practices have been audited on an annual basis since 1997, and our security policies are regularly audited both by ourselves, as well as by many of our clients.

Two years ago Acxiom experienced a security breach on one of the external file transfer servers used to transfer information back and forth between Acxiom and our clients. Fortunately, the vast majority of the information involved was of a non-sensitive nature, and law enforcement was able to apprehend the suspects and ascertain that none of the information was used to commit identity fraud. Since then, Acxiom has put in place even greater protections for the benefit of both consumers and our clients.

In conclusion, I would like to say that ongoing privacy concerns indicate the adoption of additional legislation may be appropriate. Acxiom supports efforts to pass federally preemptive legislation requiring notice to consumers in the event of a security breach, which

places the consumer at risk of identity fraud. Acxiom also supports the recent proposal from FTC Chairman Majoras for the extension of the GLBA Safeguards Rule.

Mr. Chairman, on behalf of Acxiom I want to express our gratitude for the opportunity to participate, and we will be happy to answer any questions the committee may have.

[The prepared statement of Jennifer Barrett follows:]

PREPARED STATEMENT OF JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION

INTRODUCTION

Chairman Stearns, Ranking Member Schakowsky and distinguished Members of the Committee, thank you taking the time to hold this hearing on consumer data and options following security breaches. Acxiom appreciates the opportunity to participate in today's hearing.

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

It is important that we all recognize that information has become an ever growing and ever more integral part of the American economy. Information is the facilitator of convenience, competition and provides the tools that reduce fraud and terrorism. As such, we believe that it is Acxiom's obligation to provide effective safeguards to protect the information we bring to market regardless of the difficulties encountered in doing so.

Let me be blunt. The bad guys are smart and getting more organized. They will use all of the skills available to them to try to find ways to obtain the information they need to commit fraud. Acxiom must therefore remain vigilant and innovative, and that is why we employ a world-class information security staff to help us fend off criminals who attempt to access Acxiom's data. Acxiom is constantly improving, auditing and testing its systems. Yes, Acxiom is even learning from security breaches when they occur, and we are certain that other responsible companies are doing so as well.

As Chairman Deborah Majoras of the Federal Trade Commission recently stated in her testimony before the Senate, "[T]here is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." Even though we believe that this is true, no one has a greater interest than Acxiom in protecting information because the company's very existence depends on securing personal information pertaining to consumers.

In order to enjoy the benefits provided by a robust information-based economy and also to keep our citizens safe from fraudulent activity, there are no quick fixes or easy solutions. We believe that it is necessary that cooperation exists among policy makers, information service providers, Acxiom's clients, law enforcement and consumers. We applaud your interest in exploring these issues and we very much want to be a resource in helping you achieve the proper legislative balance we all seek.

ABOUT ACXIOM CORPORATION

Founded in 1969, Acxiom is headquartered in Little Rock, Arkansas, with operations throughout the United States, and with processing centers in Arkansas, Illinois, Arizona, Ohio and California. The company also has offices in nine other countries across Europe and Asia. From a small company in Arkansas, Acxiom Corporation has grown into a publicly traded corporation with more than 6,000 employees worldwide

Acxiom's U.S. business includes two distinct components: customized computer services and a line of information products. Acxiom's computer services represent the vast majority of the company's business and they include a wide array of leading technologies and specialized computer services focused on helping clients manage their own customer information. These services are offered exclusively to large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under state and federal law. Finally,

Acxiom helps government agencies improve the accuracy of the personal information they currently hold.

The balance of Acxiom's business comes from information products that are comprised of four categories: fraud management products, background screening products, directory products and marketing products. These four product lines represent less than 20 percent of the company's total business and the fraud management and background screening products represent less than 10 percent. While each product plays a unique role, all of Acxiom's information products help fill an important gap in today's business-to-consumer relationship.

To understand the critical role Acxiom plays in facilitating the nation's economy and safeguarding consumers, it is important to understand what the company does not do. Over the years, a number of myths have developed about Acxiom that require clarification. Please allow us to set the record straight:

- Acxiom *does not* maintain one big database that contains detailed information about all individuals. Instead, the company safeguards discrete databases developed and tailored to meet the specific needs of Acxiom's clients—entities that are appropriately screened and with whom Acxiom has legally enforceable contractual commitments. I cannot call up from the company's databases a detailed dossier on myself or any individual.
- Acxiom *does not* provide information on particular individuals to the public, with the exception of Acxiom's telephone directory products. These products, which are available on several Internet search engines, contain information already available to the public. The other information Acxiom processes is provided only to legitimate businesses for specific legitimate business purposes.
- Acxiom's *does not* have any information in either its directory or marketing products which could be used to commit identity fraud. Acxiom also *does not* include detailed or specific transaction-related information, such as what purchases an individual made on the Internet or what websites they visited. The company's directory products include only name, address and telephone information. The company's marketing products include only information that is general in nature and not specific to an individual purchase or transaction.
- Acxiom *does not* commingle client information that the company processes in its computer services business with any of our information products. Such activity would constitute a violation of the company's services contracts with those clients and a violation of consumer privacy. A client for whom the company performs services may have a different agreement with us as a data contributor, but these two relationships are kept entirely separate.

Acxiom's fraud management products are sold exclusively to a handful of large companies and government agencies—they are not sold to individuals. The company's verification services only validate that the information our client has obtained from the consumer is correct. Only law enforcement, government agencies and the internal fraud departments of large financial institutions and insurance companies have access to additional information.

Acxiom's background screening products provide employment and tenant screening services which utilize field researchers who do in-person, real-time research against public records and make calls to past employers to verify the information provided by the consumer. Where permitted by law, a pre-employment credit report can also be obtained. Acxiom does not pre-aggregate information for these products.

Acxiom's directory information products contain only contact information on consumers such as name, address and telephone number. They are collected so businesses and consumers can locate other businesses or consumers. They are compiled from the white and yellow pages of published U.S. and Canadian telephone directories and from information available from the various directory assistance services provided by the telephone companies.

Acxiom's marketing information products provide demographic, lifestyle and interest information to companies to reach prospective new customers who are most likely to have an interest in their products and to better understand and serve the needs of existing customers. They are compiled from pubic records, surveys and summarized customer information primarily from publishers and catalogers.

RESPECTING AND PROTECTING CONSUMERS' PRIVACY

Acxiom has a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. The company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security policies and privacy practices. There are, as explained below, numerous laws and regulations that govern our business. Ultimately, however, Acxiom's own com-

prehensive approach to information use and security goes far beyond what is required by either law or self-regulation.

Safeguards Applicable to Products Involving the Transfer of Sensitive Information

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law, regulations and our own company policies that help protect against identity fraud. These legal protections and additional safeguards are addressed below:

GLBA, DPPAs, and FTC: Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both state and federal driver's privacy protection acts (DPPAs). These obligations include honoring GLBA and DPPA notice and choice related to sharing and use of the information, the GLBA Safeguard Rules and FTC Privacy Rule and Interagency Guidelines. Any uses of data must fall within one of the permitted uses or exceptions specified in these laws.

FCRA and FACTA: Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). These protections include: the requirement that a consumer authorize the creation of employment reports; notice of adverse actions taken based on such report; and the right of consumers to obtain a copy of such reports and to dispute inaccuracies. Finally, such regulations require that re-verification or correction of disputed information be performed in a timely manner.

Safeguarding Public Record Information: Public records are used in both Acxiom's fraud management and background screening products. Although a heightened level of protection is not mandated for such public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Safeguards Applicable to Other Products

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected, and voluntary compliance with those laws to which our clients themselves are subject.

Telephone Directory Safeguards: Acxiom's directory products comply with all applicable policies regarding unpublished and unlisted telephone numbers and addresses. In addition, because Acxiom recognizes that consumers may object to published listings being available on the Internet, Acxiom *itself* offers an opt-out from such use. Further, Acxiom voluntarily suppresses all telephone numbers found on the Federal Trade Commission's Do-Not-Call Registry and the eleven other state Do-Not-Call registries, when providing phone numbers for targeted telemarketing purposes.

Marketing Product Safeguards: Acxiom's marketing products comply with all the self-regulatory guidelines issued by the Direct Marketing Association. These requirements include notice and the opportunity to opt-out. Consumers have the ability to opt-out from Acxiom's marketing products by calling the company's toll-free Consumer Hotline, accessing its Website, or by writing to the company. Since Acxiom does not have a customer relationship with individual consumers, Acxiom coordinates with its industry clients to research and resolve consumer inquiries.

Additional Safeguards

Acxiom takes seriously its responsibility to assure that all the information we bring to market is appropriate for the use to which it is intended and to provide adequate safeguards specifically aimed at protecting against unauthorized use.

Privacy Policy/FTC Jurisdiction: Since 1997, long before it was a common practice, Acxiom has posted its privacy policy on the company's website. The privacy policy describes both Acxiom's online and offline consumer information products. The policy further describes: what data Acxiom collects for these products; how such data is used; the types of clients to which such data is licensed; as well as the choices available to consumers as to how such data is used. By making these extensive disclosures, Acxiom has voluntarily subjected itself to Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive conduct in the course of trade or commerce, as well as various state statutes governing unfair and deceptive acts and practices.

Consumer Care Department/Consumer Hotline: Acxiom maintains a Consumer Care Department led by a Consumer Advocate whose team interacted with more than 50,000 consumers in the past 12 months by way of answering questions, resolving issues, processing opt-outs, and handling requests for access to Acxiom's fraud management, background screening, directory and marketing products. Acxiom provides consumers who contact the company (through the company website, or by calling a toll-free Consumer Hotline or by writing to the company) the options of: opting-out of all of Acxiom's marketing products; receiving an information report from the company's fraud management and directory products; or receiving a consumer report as specified in the FCRA from the company's background screening products. Acxiom encourages consumers to notify the company if the information in any of these reports is inaccurate and it is the company's policy either to correct the information, to delete it or to refer the consumer to the appropriate source to obtain the requested correction, such as a county or state agency.

Certification and Compliance with Federal and State Law: Acxiom's privacy policy is designed to adhere to all Federal, State, and local laws and regulations on the use of personal information. The company is also certified under the Department of Commerce's European Union Safe Harbor and the Better Business Bureau's Online Seal.

Consumer Education: Acxiom believes that consumers should be educated about how businesses use information. To that end, Acxiom publishes a booklet, entitled "*Protecting Your Privacy in the Information Age—What Every Consumer Should Know About the Use of Individual Information*," which is available for free both on the company's website and upon written or telephone request.

Voluntary Acxiom Policies: Above and beyond the industry-accepted guidelines with which Acxiom complies, Acxiom also has established its own internal guidelines, which are more restrictive than industry standards. For example, Acxiom only collects the specific information required to meet its clients' information needs, and the company properly disposes of the remaining data, when information is compiled from public records. Acxiom has also implemented specific guidelines regarding the use and protection of information that could be involved in identity fraud, such as Social Security numbers.

Information Practice and Security Audits: Acxiom has had a longstanding focus on the appropriate use of information in developing and delivering its information products. While the creation of strong information use policies is a business imperative, assuring these policies are followed is equally important. To this end, all of Acxiom's information products and practices have been internally and externally audited on an annual basis since 1997.

Since many of Acxiom's computer service clients are financial institutions and insurance agencies, Acxiom has been regularly audited for many years by these clients. Furthermore, Acxiom must honor the safeguards and security policies of the company's clients. Since Acxiom's security program is enterprise-wide, it is the company's policy to institute these high levels of protection across all lines of business. These client audits, along with Acxiom's own internal security audits, provide Acxiom with regular and valuable feedback on ways to stay ahead of hackers and fraudsters who may attempt to gain unauthorized access to Acxiom's systems.

Lessons Learned

Two years ago, Acxiom experienced a security breach on one of the company's external file transfer servers. The hackers were employees of an Acxiom client and a client's contractor. As users with legitimate access to the server, the hackers had received authority to transfer and receive their own files. The hackers did not penetrate the firewalls to Acxiom's main system. They did, however, exceed their authority when they accessed an encrypted password file on the server and successfully unencrypted about 10 percent of the passwords, which allowed them to gain access to other client files on the server. Fortunately, the vast majority of the information involved in this incident was of a non-sensitive nature.

Upon learning of the initial breach from law enforcement, Acxiom immediately notified all affected clients and, upon further forensic investigation, the company informed law enforcement regarding a second suspected security incident. Fortunately, in both instances, law enforcement was able to apprehend the suspects, recover the affected information and ascertain that none of the information was used to commit identity fraud. One of the hackers pled guilty and was recently sentenced to 48 months in federal prison. The other is currently awaiting trial.

As a result of the breach, Acxiom cooperated with audits conducted by dozens of its clients, and both the Federal Trade Commission and the Office of the Comp-

troller of the Currency examined Acxiom's processes to ensure that the company was in compliance with all applicable laws and its own stated policies.

This experience taught Acxiom additional valuable lessons regarding the protection of information. For example, Acxiom now requires the use of more secure passwords on the affected server. The process for transferring files has been changed, specifically by keeping information on the server for much shorter periods of time. And while it was always a recommended internal policy, Acxiom now requires that all sensitive information passed across such servers be encrypted. In addition, while Acxiom has had in place a Security Oversight Committee for many years, the company has also now appointed a Chief Security Officer with more than 20 years of IT experience. In short, Acxiom's systems are more secure today as a result of the company's experience and dedication to the privacy of consumers.

The Need For Additional Legislative Safeguards

There has been much discussion, especially in recent weeks, about whether existing federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored legislation would assist Acxiom, the rest of the information services industry and businesses in general in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

Breach Notification: Acxiom supports efforts to pass federal preemptive legislation requiring notice to consumers in the event of a security breach, where such breach places consumers at risk of identity theft or fraud. California implemented similar legislation several years ago, and over thirty other states are involved in passing similar laws. The bottom line is that consumers deserve a nationwide mandate that requires that they be notified when they are at risk of identity theft, so they can take appropriate steps to protect themselves.

Extension of the GLBA Safeguards Rule: Currently, Acxiom voluntarily subjects itself to the GLBA Safeguards Rule with respect to the company's computer services and information products. Acxiom also complies with the California safeguards law (AB 1950). FTC Chairman Majoras recently has proposed an extension of the GLBA Safeguards Rule to the information services industry as a whole. Acxiom supports her recommendation.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing and to assist Congress in identifying how best to safeguard the nation's information and data. Acxiom is available to provide any additional information the Committee may request.

Mr. STEARNS. I thank you. Our next witness is Mr. Buege. Welcome.

STATEMENT OF STEVEN BUEGE

Mr. BUEGE. Chairman Stearns, Congresswoman Schakowsky, members of this distinguished committee, thank you for allowing West to present testimony before this hearing of the Subcommittee on Commerce, Trade, and Consumer Protection. I commend you for continuing its tradition of ardent and principled investigation and legislative oversight of so many of the issues that touch each of us every day.

My name is Steve Buege. I am senior vice president of Business Information, News, and Public Records for West. I oversee this content on Westlaw. I have worked for West nearly 20 years, most recently as head of operations, and prior to that as chief technology officer. I am proud to be associated with West and of West's record in the data privacy arena.

West has served the same niche customer base, legal and government professionals, for over 125 years and throughout our transformation from being a traditional law book publisher to a leader in information technology. In 1975 West introduced its first online

legal research service, Westlaw, and we have been a pioneer in e-commerce ever since.

According to our research, the total U.S. public records market represents about $7 billion annually. Of that, $1 billion is focused on the crime, law enforcement, prosecution area. About $160 million of that is in the legal market. For our business, data bases with full SSNs account for only a fraction of 1 percent of our revenue.

West's customers work in law firms, courts, government, and corporate legal departments. Much of the information they need to do their jobs is, by its very nature, sensitive. We are acutely aware of this and consider ourselves stewards of data privacy.

Given the attention this issue has recently received in Washington and in the media, we have carefully reviewed and further tightened our policies. Throughout this process, our ultimate test was to do the right thing. Our record proves that we are on the right track.

Since February, West has removed access to full SSNs from about 85 percent of the accounts that had it, and blocked this access entirely to all non-government accounts. Today, the only customers who can access full SSNs are government agencies involved in crime prevention, prosecution, and homeland security. Primarily, the Federal courts, Department of Justice, and IRS. We also have some smaller government accounts all in the areas of law enforcement and homeland security as well with access to full SSNs. All of these accounts are carefully vetted. It is important to note that we have never granted ad hoc access to full SSNs and that West serves a specialized B to B market of legal and government professionals, not a consumer-oriented market.

West's policies go well beyond what is required under various privacy laws, yet we recognize the need for more clarity and regulatory guidance. We welcome the opportunity to work with you on a variety of approaches, including establishing a uniform notification system to inform citizens whose data may have been compromised, charging a government agency with regulatory oversight of public data providers similar to the FTC's role with financial institutions, requiring senior management in data companies that deal with SSNs to sign off on their companies' security and privacy arrangements, and legislation that would establish a consistent method for masking SSNs—for example, always obscuring the last four digits.

Thank you for your interest and your hard work and for allowing West to be part of this discussion. I look forward to continuing to work with you on this important matter.

[The prepared statement of Steve Buege follows:]

PREPARED STATEMENT OF STEVE BUEGE, SENIOR VICE PRESIDENT, BUSINESS INFORMATION NEWS AND PUBLIC RECORDS, ON BEHALF OF WEST

INTRODUCTION

Chairman Stearns, Congresswoman Schakowsky, Members of this distinguished Committee: Thank you very much for allowing West the opportunity to present testimony before this hearing of the Energy and Commerce Committee's Subcommittee on Commerce, Trade, and Consumer Protection. I commend you for continuing the Committee's tradition of ardent and principled investigation and legislative oversight of so many of the issues that touch each of us every day.

My name is Steve Buege. I'm senior vice president of Business Information News and Public Records. In that role for West, I oversee our news, business information and public records content on Westlaw, and together with the president and CEO of West, I oversee the policies governing procurement of and access to that information.

Prior to this, I was vice president of Operations for West, where Customer Experience, Technology and Content Operations reported into me. Prior to that, I was Chief Technology Officer for four years. In my work with the company, spanning now some 20 years, I've participated in some of its most important transformations. I have intimate knowledge of its technology, its business and its values. And I am proud of my association with the business.

ABOUT WEST AND OUR CUSTOMERS

West has been serving the same niche customer base—exclusively legal and government professionals—for more than 125 years. Our company founder, John B. West, started West Publishing in 1872 as a regional book and office supply seller for attorneys in the Midwest. Eventually, West covered judicial opinions from every state, circuit and appellate court and the U.S. Supreme Court.

Our core market has remained legal and government customers for more than a century. West maintained this focus on the B2B market while transitioning from a traditional legal book publisher to a leader in the information technology revolution. In 1975, West introduced its first online legal research service, Westlaw. We've been a pioneer in e-commerce ever since. We embraced the Internet, and electronic publishing is at the heart of our business today.

The West name—from West Publishing to Westlaw—has long been known as an authoritative, trustworthy source for the U.S. bench and bar. This market recognizes Westlaw as the premier online legal research service; it offers the world's largest databases of legal research materials, statutes, case law, legal treatises and business information.

West has been acutely focused on security and privacy issues, especially in the last 10 years as access to electronic information has increased significantly. We consider ourselves stewards of data privacy. West was a founding member of the Individual Reference Services Group (IRSG). The 1997 IRSG Principles defined a balance between personal privacy and the important societal benefits of reference services. West used these principles to establish procedures for qualifying its users, with only government agencies and a very small number of professional users receiving qualified access to full Social Security numbers.

Today, West still refers to the IRSG Principles for guidance about our collection and distribution of information. For example, although the Gramm-Leach-Bliley Act's privacy rule permits distribution of information—including full Social Security numbers—to any entity that fits within the exception to the rule, West limits distribution of full Social Security numbers to specific government agencies—going beyond the requirements of GLBA.

OVERVIEW OF THE PUBLIC RECORDS MARKET

According to our research, the U.S. public records market represents about $7 billion dollars annually. Within this space, $1 billion is focused on the crime/law enforcement/prosecution area; approximately $160 million of that space is focused on usage within the legal market. Of this $160 million, only a fraction relates to records with full Social Security numbers. For our legal businesses, databases with full Social Security numbers only account for a fraction of 1 percent of our revenues.

It's important to note that only vetted government customers who deal with law enforcement, investigatory or homeland security issues have access to full Social Security numbers. None of our corporate clients have this access.

OUR PRIVACY POLICIES

West's customers work in law firms, the courts, government and corporate legal departments. Much of the information our customers need to do their jobs and serve our legal justice system is, by its very nature, sensitive.

West has always been a good steward of this sensitive information, and we are deeply committed to ensuring that we achieve the proper balance between making information available for legitimate business and governmental purposes and respecting people's expectations of privacy.

Given the attention this issue has received in Washington and in the media during the past few months, we have carefully reviewed our policies and made significant changes concerning access. Throughout this process, our ultimate test was to do the right thing. Our record proves that we're on the right track.

Since February, West has reviewed the very small number of customers who had access to full Social Security numbers and further restricted which customers are allowed such access. We removed access to full Social Security numbers for about 85 percent of the accounts who had it, and blocked this type of access to all non-government accounts. Today, most customers who can access full Social Security numbers are government agencies involved in crime prevention, prosecution and homeland security—primarily the Federal Courts, the Department of Justice and the IRS. We also have some smaller accounts—all in the areas of law enforcement and homeland security as well—with access to full Social Security numbers. All these accounts are carefully vetted. It's important to note that we have never granted ad hoc access to full Social Security numbers and that West serves a specialized market of legal and government professionals—not a consumer-oriented market.

Opt-in policy

In the past few months, West has worked with our government customers to fully institute an opt-in policy; that is, a policy that assumes a government account will not have full access to Social Security numbers. Under this new policy, accounts that need access to full Social Security numbers will be granted access only to specified and qualified individuals. Moving forward, all new contracts West enters with government agencies will be opt-in only.

Enhanced usage tracking and Westlaw reminders

West also has introduced new procedures to monitor databases that contain Social Security numbers for unusual use patterns, and on a go-forward basis, customers permitted to view full Social Security numbers on Westlaw will see a special notification message—any time—they—access—these databases.—This message will remind the user that he or she is among a—limited—number of people given privileged access to this information, and that it must be used only for appropriate purposes and in compliance with the law and the privacy terms West imposes. This will ensure that individual users are aware of their responsibility in accessing Social Security numbers as well as their unique privilege to use this information.

West's policy goes well beyond what's required under—various privacy—laws. We are committed to working with this Committee to fully explore this complex issue. We also hope to work with you, federal agencies and the industry to ensure that the public is protected from fraud and that those committed to fighting and prosecuting these crimes will have the information they need to do their important work.

PRIVACY GUIDELINES AND REGULATIONS

And that is why I'm here today. West recognizes the need for guidelines, and we would welcome the opportunity to work with you to advance a variety of approaches. From our business perspective, here are some areas where we welcome clarity and guidance:

- Establishing a uniform notification system that informs customers whose data may have been compromised
- Allowing a government agency to have an appropriate regulatory role over public data providers, similar to the regulatory role the Federal Trade Commission currently has regarding data matters in financial institutions
- Requiring senior management in data companies that deal with Social Security numbers to sign off on a business's security and privacy arrangements

Also, you may want to consider the following ideas that haven't been as widely discussed:

- Legislation that would establish a universally applied method for masking Social Security numbers. (Now there are several common ways that entities mask Social Security numbers. Some mask the first five digits and others truncate the last four. This might allow someone to determine a full Social Security number by using two differently masked numbers.)
- Encouraging each business in this space to find an alternative technology solution—instead of Social Security numbers—to create a unique locator that distinguishes one individual with the same name from another. This approach would be specific to each business; it wouldn't be uniform across the industry.

CONCLUSION

Thank you for your interest, your hard work and allowing West to be part of your discussion. I look forward to continuing to work with you on this important matter as we balance individuals' rights to privacy with the national concern for justice and homeland security.

Mr. STEARNS. I thank the gentleman. Mr. Ireland, well, welcome.

STATEMENT OF OLIVER I. IRELAND

Mr. IRELAND. Good morning, Chairman Stearns——

Mr. STEARNS. I just need you to——

Mr. IRELAND. [continuing] Ranking Member Schakowsky, and members of the subcommittee. My name is Oliver Ireland. I am a partner in the Washington, DC office of Morrison and Foerster, and I am pleased to be here today on behalf of Visa U.S.A. to address the issue of consumer information security.

Visa has long recognized the importance of protecting cardholder information. The Visa system provides for zero liability for cardholders for unauthorized transactions. Therefore, Visa members, card issuers incur the costs of fraudulent transactions that may result from unauthorized access to cardholder information and have a strong interest in protecting that information.

Further, existing Federal law obligates financial institutions to protect their customers' information. Under Section 501(b) of the Gramm-Leach-Bliley Act, the Federal banking agencies and the Federal Trade Commission have established information security standards for the financial institution subject to their jurisdiction. But many holders of sensitive personal information, including, for example, employers and retail merchants, are not financial institutions subject to the 501(b) rule. In part, to address this gap, Visa is implementing a comprehensive Cardholder Information Security Plan or CISP. CISP requires all holders of cardholder information, including merchants, to comply with the "Visa Digital Dozen," 12 basic requirements for safeguarding customer information.

Visa also uses sophisticated neural networks to detect and block transactions where fraud is suspected. These networks, coupled with CISP and Visa's zero liability policy provide a high degree of protection from fraudulent credit card transactions to cardholders. Nevertheless, Visa believes that all businesses that maintain sensitive personal information should be subject to uniform national requirements to protect that sensitive information.

Closely related to the issue of information security is the question of what to do if a security breach occurs. Visa believes that where the breach creates a substantial risk of harm to consumers, that the consumers can take action to prevent, the consumers should be notified so that they can take the appropriate action. Both Federal and California law already address this issue. For example, the California law currently requires notice to individuals of a breach of security involving their computerized personal information. Other States have enacted or are considering security breach notification laws. However, the details of these laws differ.

The Federal banking agencies have also issued guidance that requires banking institutions that experience a breach of security involving sensitive customer information to notify customers where misuse of the information has occurred or is reasonably possible.

The fact that States are not addressing notification in a uniform way creates a critical need for a single, national standard for notification. A single standard will avoid confusion among consumers as to the meaning of notices that they receive and among holders of consumer information as to their notification responsibilities.

Further, any legislation on security breach notification should recognize compliance with the banking agency guidance that is already in place as compliance with any Federal notification requirement. Further, such notification requirements should be risk-based to avoid inundating consumers with notices where no action by consumers is required. As FTC Chair Majoras has testified, notices should be sent only if there is a significant risk of harm.

Thank you again for the opportunity to be here today. I would be happy to answer any questions from the members of this committee.

[The prepared statement of Oliver I. Ireland follows:]

PREPARED STATEMENT OF OLIVER I. IRELAND ON BEHALF OF VISA U.S.A. INC.

Good morning Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee. I am a partner in the law firm of Morrison & Foerster LLP, and practice in the firm's Washington, D.C. office. I am pleased to appear before the Subcommittee on behalf of the Visa, U.S.A. Inc., to discuss the important issue of consumer information security.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in developing and implementing technology, products, and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect Visa's members' cardholder information, thereby to protect the integrity of the Visa system.

Visa has substantial incentives to maintain strong security measures to protect cardholder information. The Visa system provides for zero liability to cardholders for unauthorized transactions. Cardholders are not responsible for unauthorized use of their cards. The Visa Zero Liability policy guarantees maximum protection for Visa cardholders against fraud due to information security breaches. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs attributable to the harm and inconvenience that might be felt by cardholders or merchants. Accordingly, Visa aggressively protects the cardholder information of its members.

EXISTING FEDERAL LAWS AND RULES FOR INFORMATION SECURITY

Existing federal laws and regulations also obligate financial institutions to protect the personal information of their customers. Rules adopted under section 501(b) of the Gramm-Leach-Bliley Act of 1999 by the federal banking agencies and the Federal Trade Commission ("FTC") ("GLBA 501(b) Rules") establish information security standards for the financial institutions subject to the jurisdiction of these agencies. Under the GLBA 501(b) Rules, financial institutions must establish and maintain comprehensive information security programs to identify and assess the risks to customer information and then control these potential risks by adopting appropriate security measures.

Each financial institution's program for information security must be risk-based. Every institution must tailor its program to the specific characteristics of its business, customer information and information systems, and must continuously assess the threats to its customer information and systems. As those threats change, the institution must appropriately adjust and upgrade its security measures to respond to those threats.

However, the scope of the GLBA 501(b) Rules is limited. Many holders of sensitive personal information are not financial institutions covered by the GLBA 501(b) Rules. For example, employers and most retail merchants are not covered by the GLBA 501(b) Rules, even though they may possess sensitive information about consumers.

VISA'S CARDHOLDER INFORMATION SECURITY PLAN

Because of its concerns about the adequacy of the security of information about Visa cardholders, Visa has developed and is implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("CISP"). CISP applies to all entities, including merchants, that store, process, transmit, or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers, or the Internet. CISP was developed to ensure that the cardholder information of Visa's members is kept protected and confidential. CISP includes not only data security standards but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

As a part of CISP, Visa requires all participating entities to comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include: (1) install and maintain a working network firewall to protect data; (2) do not use vendor-supplied defaults for system passwords and security parameters; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) develop and maintain secure systems and applications; (7) restrict access to data on a "need-to-know" basis; (8) assign a unique ID to each person with computer access; (9) restrict physical access to data; (10) track all access to network resources and data; (11) regularly test security systems and processes; and (12) implement and maintain an overall information security policy.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Visa is not the only credit card organization that has developed security standards. In order to avoid the potential for imposing conflicting requirements on merchants and others, in December of 2004, Visa, MasterCard, American Express, Discover, and Diners Club collaborated to align their respective data security requirements for merchants and third parties. Visa found that the differences between these security programs were more procedural than substantive. Therefore, Visa has been able to integrate CISP into a common set of data security requirements without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("PCI Standard").

NEURAL NETWORKS TO DETECT FRAUD AND BLOCK POTENTIALLY UNAUTHORIZED TRANSACTIONS

In addition to the CISP program, which helps to prevent the use of cardholder information for fraudulent purposes, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigation and card re-issuance. These networks, coupled with CISP and Visa's Zero Liability, provide a high degree of protection from fraudulent credit card transactions to cardholders.

EXPANSION OF EXISTING REQUIREMENTS

Current protections notwithstanding, Visa believes that an obligation to protect sensitive personal information, similar to the GLBA 501(b) Rules, should apply broadly so that all businesses that maintain sensitive personal information will establish information security programs. Because consumer information knows no boundaries, it is critical that this obligation be uniform across all institutions in all jurisdictions.

SECURITY BREACH NOTIFICATION

Closely related to the issue of information security is the question of what to do if a breach of that security occurs. Visa believes that where the breach creates a substantial risk of harm to consumers that the consumers can take action to prevent, the consumers should be notified about the breach so that they can take appropriate action to protect themselves. Both federal and California law already address this issue. California law currently requires notice to individuals of a breach of security involving their computerized personal information. The California law focuses on discrete types of information that are deemed to be sensitive personal information. The statute defines sensitive personal information as an individual's name plus any of the following: Social Security Number, driver's license number,

California identification card number, or a financial account number, credit or debit card account number, in combination with any code that would permit access to the account. The California law includes an exception to the notification requirement when this personal information has been encrypted. The California law only requires notice to be provided when personal information is "acquired by an unauthorized person." Other states recently have enacted or are considering security breach notification laws; however, the details of some of the laws differ.

In March, the federal banking agencies issued final interagency guidance on response programs for unauthorized access to customer information and customer notice ("Guidance"). The Guidance applies to all financial institutions that are subject to banking agency GLBA 501(b) Rules and requires every covered institution that experiences a breach of security involving sensitive customer information to: (1) notify the institution's primary federal regulator; (2) notify appropriate law enforcement authorities consistent with existing suspicious activity report rules; and (3) notify its affected customers where misuse of the information has occurred or is reasonably possible.

The keen interest that states have shown to legislate on the issue of security breach notification emphasizes the need for a single national standard for security breach notification in order to avoid confusion among consumers as to the significance of notices that they receive and among holders of information about consumers as to their notification responsibilities. In addition, any legislation on security breach notification should recognize compliance with the Guidance as compliance with any notification requirements.

Visa believes that a workable notification law that would require entities that maintain computerized sensitive personal information to notify individuals upon discovering a significant breach of security of that data should be risk-based to avoid inundating consumers with notices where no action by consumers is required. As FTC Chairwoman Majoras recently testified to Congress, notices should be sent only if there is a "significant risk of harm," because notices sent when there is not a significant risk of harm actually can cause individuals to overlook those notices that really are important.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.

Mr. STEARNS. I thank the gentleman. Mr. Burton, welcome.

STATEMENT OF DANIEL BURTON

Mr. BURTON. Thank you, Chairman Stearns, Ranking Member Schakowsky, distinguished members of the subcommittee. I appreciate your holding this hearing and giving me the opportunity to testify. My name is Daniel Burton. I am vice president of government affairs for Entrust, Inc.

Entrust is a world leader in securing digital identities and information. As a security software company, we are in the business of protecting our customers, and by extension, your constituents, with proven technology solutions. Over 1,200 enterprises and government agencies in more than 50 countries rely on Entrust software, including the U.S. Department of Treasury, the Department of Justice, and several nuclear laboratories. So we have a lot of experience in this field.

I would first like to note with great appreciate this subcommittee's longstanding interest in online privacy. You have followed this issue closely for several years and built up considerable expertise. As a result, this committee is very well-positioned to play a leadership role in this debate.

The privacy issues we are facing today are very different than they were a few years ago. Then, much of the debate revolved around limited opt-in and opt-out provisions. Today, with the rampant theft of confidential personal information, the Internet privacy debate is focused squarely on security.

This shift in emphasis represents a sea of change for public policy. For years we have enjoyed the productivity improvements that network computing afforded and tolerated the nuisances that came with it. Today, these nuisances are overshadowed by a much more sinister problem, organized crime.

Just like companies and governments, criminals have realized that the Internet is a powerful business tool. For criminals, gaining access to computerized credit card information, Social Security numbers, and other identifiers is a gateway to ready cash. Computer hackers no longer fit the profile of pimply faced teenagers who lose interest as soon as they get a girlfriend. Increasingly, they are skilled criminals who have a sophisticated business plan, mount wholesale attacks, move quickly around the world, and cover their tracks.

Identify theft is not limited to data brokers. The breaches at ChoicePoint and Lexis-Nexis may have sparked public outrage, but the problem goes much deeper. Discount Shoe Warehouse, the San Jose Medical Group, George Mason University, SAIC, Time Warner, none of these are data brokers, yet all have suffered breaches of highly sensitive personal information.

Focusing remedies exclusively on data brokers is like protecting your home from burglars by locking your doors but leaving your windows wide open. It may make you feel better, but it won't prevent a robbery. Similarly, passing a law that requires only data brokers to issue notifications when their systems are breached will do nothing to safeguard the reams of personal information that are held by other organizations.

It is for this reason that the recent State breach notification laws cover anyone that owns or licenses computerized data that includes personal information. As you know, several States have already passed such bills, and many more are considering them. There is a very real possibility that by this summer we could see over a dozen competing State breach notification laws in effect.

Given the reality of cyber crime, breaches, and State legislation, Congress needs to act. Entrust believes the Federal legislation could help and recommends the following measures for consideration: No. 1, establish a uniform national breach notification policy for unauthorized access to unencrypted personal information. If personal data is appropriately encrypted, notification should not be required. That is because even if the data is stolen, it will show up as random characters that won't make any sense to thieves unless they have the proper access codes. Since not all encryption is reliable, however, Congress should insist that it meets standards developed by the National Institute of Standards and Technology.

No. 2, require second factor authentication for access to sensitive personal information. The FDIC said it best in its report "Putting an End to Account-Hijacking Identify Theft." Its lead recommendation, upgrading existing password-based, single factor customer authentication systems to two factor authentication. Simple user name and passwords are too easily breached. They must be backed up with physical tokens containing secret access codes the legitimate users keep in their possession.

No. 3, encourage enterprises that hold sensitive personal information to use technological and other means to assure compliance

with their privacy policies. Since the majority of breaches come from insiders, organizations can significantly improve data security by deploying automated tools that screen email for privacy violations.

The fourth recommendation is to extend security requirements similar to the Gramm-Leach-Bliley Act safeguards to all entities that retain sensitive personal information.

In conclusion, this subcommittee has a vital role to play in the effort to security computerized personal information. Entrust is doing its best to help organizations implement strong technology safeguards and looks forward to working with you to see that they are complemented with effective public policy.

[The prepared statement of Daniel Burton follows:]

PREPARED STATEMENT OF DANIEL BURTON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, ENTRUST, INC.

Good Morning. Chairman Stearns and distinguished Members of the Subcommittee, thank you for holding this hearing and giving me the opportunity to provide testimony on this important subject. My name is Daniel Burton, and I am Vice President of Government Affairs for Entrust, Inc. In my testimony today, I will discuss the impact of security breaches and what we can do about them.

Entrust is a world leader in securing digital identities and information. As a security software company, we are in the business of protecting our customers—and by extension your constituents—with proven technology solutions that secure digital information. Over 1,200 enterprises and government agencies in more than 50 countries, including the US Department of Treasury, the Department of Justice and numerous nuclear laboratories, rely on Entrust software, so we have a lot of experience in this field. Entrust provides software solutions that protect your digital identity through authentication, enforce policy through advanced content scanning, and protect your information assets through encryption. Our mission is to work with customers to put in place the technologies, policies, and procedures necessary to protect digital identities and information.

I would like to note with appreciation this committee's longstanding interest in on-line privacy. As a company that is on the front lines of the daily battle to protect sensitive information, Entrust applauds your activities and encourages your continued leadership in this area. You have followed this issue closely for several years and built up considerable expertise. As a result, you are well positioned to play a critical role in protecting the privacy of individuals, companies and governments.

The privacy issues we are facing today are very different than they were a few years ago. Then, much of the debate revolved around limited "opt-in" and "opt-out" provisions that determined what kind of consent was necessary to share personal information for marketing purposes. Today, with rampant theft of confidential personal information a reality, the Internet privacy debate is focused on squarely on security.

CRIME ON THE NET

This shift in emphasis—from nuisance to outright crime—represents a sea change for public policy. For years we have enjoyed the productivity improvements that networked computing afforded and learned to live with the nuisances that came with it. We may have been concerned about hacking for "honor" and other pranks, but like early version of spam, viruses and unsolicited marketing campaigns, we tolerated them as a small price to pay for the extraordinary dividends the Internet provided. Today, these nuisances are overshadowed by a much more sinister problem—organized crime.

Just like companies and governments, criminals have come to realize that the Internet is a powerful business tool. As mountains of sensitive personal, corporate and government information have moved onto the net, crime has too. For criminals, gaining access to names, addresses, credit card information, social security numbers and other identifiers is a gateway to ready cash. As a result, computer hackers no longer fit the profile of pimply faced teenagers who lose interest as soon as they get a girlfriend. Increasingly, they are skilled criminals who have a sophisticated business plan, mount wholesale attacks, move quickly around the globe and cover their tracks. Our understanding of these crimes and the role of law enforcement is still evolving, but the stakes are high. If Internet crime causes American consumers to

retreat from online transactions, U.S. business and government will suffer huge productivity reversals that could cripple not only e-commerce, but also the economy at large.

The statistics are staggering. The Federal Trade Commission estimates that 9-10 million Americans are victims of identity theft per year. Total cost to business and consumers is approaching $50 billion. Almost 2 million US adult Internet users had their identities stolen in 2004. Almost 12% of the fraud is online.

As a result, the public temperature is rising. A January 2005 IDC Survey showed that close to 60% of US consumers are concerned about identity theft, and almost 6% have taken the remarkable step of switching banks as a result. A survey that Entrust conducted reaffirmed this concern. It found that 80% of individuals are worried about someone stealing their on-line identity and using it to access their online bank accounts.

The underlying question of this hearing is whether we are doing enough to protect confidential information. The answer, unfortunately, is that as a nation we are not prepared to deal with the reality of cybercrime. The necessary legal framework to safeguard consumers and companies is still incomplete; enforcement efforts and resources are inadequate; and much of the private sector is still in denial.

BIGGER THAN BANKS, HOSPITALS AND DATA BROKERS

The identity theft crisis extends well beyond regulated industries like banking and healthcare that many people view as guardians of their sensitive information. It's even bigger than data brokers, despite all the attention they have received lately. The breaches at Bank of America, Choicepoint and Lexis-Nexis may have sparked public outrage about identity theft, but you only have to look at the kinds of organizations that have announced breaches in recent months to understand that the problem goes much deeper. Discount Shoe Warehouse, Paymaxx, the San Jose Medical Group, the University of California at Berkeley, George Mason University, SAIC, Time Warner—none of these are data brokers, yet they all suffered breaches of highly sensitive personal information. The scope of these breaches demonstrates that the universe of organizations holding sensitive personal information is quite large. Focusing remedies exclusively on data brokers is like protecting your home from burglars by locking the front door and leaving all the windows wide open. It may make you feel better, but it won't do much to prevent a robbery. Similarly, passing a law that requires only data brokers to issue notifications when their systems are breached will do nothing to safeguard the mountains of personal information that are held by other organizations. True success lies in a much broader approach.

It is for this reason that the recent state breach notification laws we see around the country are not limited to banks, healthcare providers and data brokers. It may interest you to know that many of the most proactive states in this arena are represented by members of this Committee. For example, California was the first state to pass such a bill (H.B. 1386). It took effect on July 1, 2003 and requires a state agency, person or business that conducts business in California, and that owns or licenses computerized data that includes personal information to disclose breaches of unencrypted personal information to California residents. Arkansas has also passed a disclosure law (Senate Bill 1167) that covers "individuals, businesses and state agencies that acquire, own or license personal information about the citizens of the State of Arkansas . . ." Florida has a bill (H.B. 481) awaiting the Governor's signature that covers "Any person who conducts business in this state and maintains computerized data in a system that includes personal information . . ." In all, over twenty states have introduced such legislation, and there is a possibility that we could have over a dozen competing and conflicting state breach notification laws in effect by this summer.

Given this backdrop of crime, systematic breaches and proliferating state legislation, Congress needs to act.

TECHNOLOGY AND PUBLIC POLICY

In trying to determine what role Congress should play, it is important to understand some of the key technologies underlying information security. I will focus on two: confidentiality and authentication. Confidentiality means assuring that information is not disclosed to unauthorized persons. E oding or scrambling of information so that it can only be decoded and read by someone with the correct decoding key—is the technology often associated with confidentiality. Encryption comes in different strengths. Many of the state breach notification bills make specific reference to it.

Data in transit, such as e-mail, presents different encryption challenges than stored data. And since stored data is held in a variety of repositories, from mainframes to laptops, and in different ways, such as data bases and directories, it presents unique encryption challenges of its own. Software applications and data bases are typically built for speed, not security, so the issue is not just whether to encrypt them, but how and where to apply it. Not all data must be encrypted, but there is an increasing demand to encrypt sensitive personal data, even if it affects performance.

Authentication means corroborating that a user is who they claim to be. It is often linked closely with authorization, which means that you have the right to access the information in question. Authentication technologies include user name and password (referred to as first factor since they relate to something you know) and physical tokens with secret codes (referred to as second factor since they are something you have). An even stronger form of authentication technology is the digital certificate, which is an electronic identifier that establishes your credentials. Digital certificates are issued by a certification authority. They contain your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Using public key cryptography and digital certificates, the sender can assure that only the intended recipient can—open the message, and the recipient knows that only the authorized sender could have sent the message.

Much of the public policy debate about identity theft has focused on the need to authenticate consumer identities. Just as important, however, is the need to authenticate employer and supplier identities at both ends of a transaction. Since many breaches are internal, proper authentication of the employees, customers and partners who have privileged access to information is critical to preventing identity theft.

THE NEED FOR ADDITIONAL LEGISLATIVE SAFEGUARDS

There has been a lot of discussion about whether existing law is sufficient to prevent identity theft. Although industry at large has traditionally opposed federal legislation in this area, rampant identity theft, the proliferation of security breaches, and the passage of state breach notification laws have caused many companies to change their view. Entrust believes that additional Federal legislation could assist holders of sensitive personal information in their efforts to prevent consumer fraud and identity theft. Specifically, we believe that the following measures deserve consideration.

1. Establish a uniform national breach notification policy for unauthorized access to unencrypted personal information.

Breach notification laws are necessary to inform consumers when their sensitive personal information has been compromised so that they can guard themselves against identity crimes. As mentioned above, several states have passed breach notification laws and many more have introduced this legislation. A uniform national notification standard is needed to preempt conflicting state laws and establish consistent requirements. In weighing such a provision, Congress should keep in mind two important criteria that are enshrined in state law.

First, the notification requirement should apply to *all entities that hold sensitive personal information.* Confidential information is held by a wide variety of institutions, including employers, retailers, lawyers and government agencies. If the Federal notification requirement is limited to data brokers and regulated industries like banking and health-care, none of these other organizations will be covered. If this were the case, organizations like SAIC, Time Warner, George Mason University and Discount Shoe Warehouse—all of whom have suffered breaches and sent out notifications in recent months—would not be required by Federal law to notify those people whose identities had been compromised.

Second, and just as important, if the personal *information is appropriately encrypted, notification should not be required.* The reason for this provision is that unauthorized access to encrypted data reveals only scrambled code that is meaningless. For example, if the personal information of the 600,000 current and former employees of Time Warner had been encrypted on the tapes that were lost, there would have been very little risk of identity theft because the information would have been unintelligible to anyone without the proper access.

There are several different kinds of encryption, however, not all of which are reliable. To insure that the encryption is adequate, Congress should insist on the encryption standards developed by the National Institute of Standards and Technology. Organizations that suffer breaches should not have to issue notifications if

their *data, whether in storage or in transit, is encrypted with a NIST approved encryption algorithm, uses NIST approved key management techniques and has cryptographic operations performed within a FIPS 140 validated cryptographic module.*

2. Require second factor authentication for access to sensitive personal information.

The Federal Deposit Insurance Corporation (FDIC) issued a thorough study of identity theft in its December 2004 report, *Putting an End to Account-Hijacking Identity Theft.* The FDIC's lead recommendation is "Upgrading existing password-based single-factor customer authentication systems to two-factor authentication." Industry analysts have confirmed this view. Jonathan Penn, an analyst at Forrester, has written that "In response to consumers' rising concerns about fraud and identity theft, many organizations are evaluating strong authentication solutions . . ." And John Pescatore, an analyst with Gartner, has written "When you get to the core issue of most identity theft attacks, it really falls back to needing stronger authentication . . ."

The problem with two-factor authentication is that, until recently, it was difficult to administer and prohibitively expensive to implement on a large scale. Fortunately, new technology breakthroughs by Entrust and others have substantially reduced the cost and complexity associated with two factor authentication. These breakthroughs should facilitate the broader use of this technology to organizations that must safeguard large quantities of digital identities.

3. Encourage enterprises that hold sensitive personal information to use technological and other means to assure compliance with their privacy policies.

Since the majority of breaches come from insiders, one way to limit them is for organizations to screen communications for privacy violations. The FDIC has already highlighted this imperative in its safeguards guidance to financial institutions, recommending that they establish controls to prevent employees from providing customer information to unauthorized individuals. Since banks are not the only ones holding sensitive personal information, these controls should be extended to non-financial institutions as well.

Because the majority of electronic data is at some point associated with e-mail, controls that assure outgoing e-mail communications and attachments comply with privacy policies can help reduce identity theft. To the extent that organizations monitor e-mail traffic at all, however, many rely on a manual review of only a small sample of e-mail traffic. Fortunately, technology now exists that has automated compliance controls capable of blocking, archiving, redirecting or securing e-mail communications in real-time. Enterprises that are in the business of holding sensitive personal information should be encouraged to consider adopting it.

4. Extend security requirements similar to the Gramm-Leach-Bliley Act safeguards for financial institutions to all entities that retain sensitive personal information.

This Subcommittee should consider extending the risk management, reporting and accountability requirements documented in FDIC and FTC safeguards guidance to all enterprises that hold sensitive personal information. Title V of the Gramm-Leach-Bliley Act (GLBA) states that financial institutions must establish safeguards for customer records and information. In her testimony before this Subcommittee on March 15, 2005, the Chair of the Federal Trade Commission, Deborah Majoras, noted that to the extent that data brokers fall within the GLBA definition of financial institutions they must abide by these safeguards. As discussed earlier, however, limiting the extension of the GLBA safeguards only to data brokers would overlook the vast numbers of other organizations that hold sensitive personal information and do little to stem the tide of identity theft.

Since any discussion of security safeguards raises questions about technology mandates, it is important to emphasize that the regulatory guidance for implementing the GLBA safeguards addresses such issues as the need to develop a written security plan, to designate appropriate personnel to oversee it, and to conduct a risk assessment. None of these is a technology requirement. Instead, they relate to sound management practices. The National Cyber Security Summit Task Force on Information Security Governance that Entrust CEO Bill Conner co-chaired took a similar approach. In its April 2004 report, *Information Security Governance: A Call to Action,* it concluded that "The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs." It recommended that CEOs have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to their board of directors. In addition, it emphasized the need for organizations to establish a security management structure to assign explicit individual roles, responsibility, authority and accountability.

CONCLUSION

This Subcommittee has an important role to play in the effort to secure personal data. The goal is clear. We should do everything we can to encourage holders of sensitive information to secure it from unauthorized access and, in the event of a breach, to notify individuals so that they can protect themselves. The reality of rampant identity theft is proof that we have no time to waste. The fact that sensitive personal information is held by a wide variety of organizations demonstrates that a narrow solution will be insufficient.

Information security is not only a technical issue, but also a governance challenge. Technology solutions, like encryption, strong authentication and automated e-mail compliance with privacy policies, can do a lot to prevent unauthorized access to personal information. But they must be grounded in the risk management, reporting and accountability that can only be implemented with the active engagement of executive management.

Mr. STEARNS. I thank the gentleman. We are on a vote, but I think we—Mr. Solove, I think we can get your opening statement, and then we will recess and come right back. So go ahead. Welcome.

STATEMENT OF DANIEL J. SOLOVE

Mr. SOLOVE. Mr. Chairman, Congresswoman Schakowsky, members of the committee, thank you for inviting me to appear before you and provide testimony. My name is Daniel Solove, and I am an associate professor of law at George Washington University Law School. I have published over a dozen articles as well as two books about information privacy. My most recent book, "The Digital Person," discusses the issues at this hearing in depth. It was published in December 2004.

The litany of data leaks and improper access to personal data are the symptoms of a significant problem that Congress must address. It is important to understand the nature of the problem, and I think this extends beyond just a security issue.

We are increasingly living with digital dossiers about our lives. These repositories of personal data can affect whether we get a loan, a license, or a job. The central problem that we face today, the central problem is that it is caused by a lack of individual participation and empowerment when it comes to the collection and use of personal data and a lack of accountability among the companies that handle that data.

Today, people lack much participation in how their data is used and disseminated. Identify theft is difficult for victims to detect because they have little knowledge about the information being circulated about them. Therefore, solutions to the problem must provide individuals with greater knowledge and control about how their data is used. People must be provided meaningful remedies when their data is leaked and misused. Without meaningful remedies, mere notice of a leak is akin to a company saying we just had a toxic spill in your backyard. It might cause you harm, so you might want to have periodic medical checkups.

Because people have so little participation and power over their information, it is very hard for them to clean up their records in the event of an identity theft. Congress should ensure that victims of identity theft have appropriate tools to repair the damage quickly.

The harm to victims in an identity theft is facilitated by Social Security numbers, birth dates, and other pieces of personal data

being used by companies as passwords to obtain access to accounts or to sign up for a credit card. If the practice of using Social Security numbers as passwords were halted, the leakage of Social Security numbers would not be so dangerous and damaging to individuals.

The Gramm-Leach-Bliley Act requires security safeguards for personal data maintained by financial institutions. Despite these safeguards, many financial institutions continue to use Social Security numbers as passwords. Why doesn't the FTC enforce these security standards to halt this practice? Well, I can postulate a number of reasons, and I think one of the primary reasons is that these security standards are incredibly vague and they haven't provided adequate guidance. I think to be effective in crafting security standards, they must apply widely and they must be specific without being overly constraining.

Beyond identity theft, people lack the ability to easily locate and fix errors in their records that may cause them harm. People's dossiers are often riddled with inaccuracies. The Fair Credit Reporting Act requires consumer reporting agencies to maintain procedures to ensure maximum possible accuracy. However, many data brokers have data bases they claim fall outside of the Fair Credit Reporting Act. And little is done more systemically to ensure the accuracy of records systems used for background checks and other decisions about people's lives.

I believe that the security breaches that we are facing today are part of a larger problem, one involving information privacy. Information today is protected in a piecemeal fashion based on who holds it. The same piece of data might be protected if it is held by a video rental store but completely unprotected in the hands of data brokers like ChoicePoint.

The current regulation of information has tremendous gaps and loopholes. We have a system that does not provide adequate accountability among the users of personal information. We have a system that, to a large extent, leaves people out in the cold who are victimized by identity theft or harmed by an erroneous report.

Congress must put individuals back in control of their data and ensure that companies are accountable for the way that they handle and use that data. Thank you very much.

[The prepared statement of Daniel J. Solove follows:]

PREPARED STATEMENT OF DANIEL J. SOLOVE, ASSOCIATE PROFESSOR OF LAW, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

I. INTRODUCTION

Mr. Chairman, members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Daniel Solove and I am an associate professor of law at the George Washington University Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles as well as two books, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (NYU Press December 2004) and INFORMATION PRIVACY LAW (Aspen 2003) (with Marc Rotenberg).

The announcement of recent data breaches at a variety of companies and institutions have affected millions of people. As one article notes:

> In breaches reported publicly since February, more than 2.5 million records may have been exposed to thieves at data broker ChoicePoint, retailer DSW,

news and information broker LexisNexis, the University of California at Berkeley and elsewhere.[1]

I will not discuss the series of data breaches that have lead to this hearing, as I am sure that you are all familiar with them. Instead, I will focus my comments on what can be done to address the problems and how we can better protect information privacy. My remarks will focus on two points.

First, I will explain why the problem is larger than just a security problem. Security is one dimension of a larger set of issues involving information privacy. Beyond securing data, the law must ensure that when there is a leak or improper access, the harmful effects are minimized. Doing this requires empowering individuals with tools to better manage their data. Moreover, making companies more accountable for their activities will promote better security, as well as better accuracy, in record systems.

Second, I will discuss why the innovative role of the states should be preserved. Federal legislation must allow room for states to experiment with new approaches and solutions to the problem. Many current federal protections, as well as many of the ideas currently proposed to address the problem, are drawn from state laws.

There are many more specific measures that can be taken to address the problems we are encountering today. Chris Hoofnagle of the Electronic Privacy Information Center and I have written a short essay called *A Model Regime of Privacy Protection,* where we set forward succinctly a series of sixteen legislative proposals. We explain why these proposals are necessary and respond directly to the criticisms of our proposals by a wide array of individuals (some from the industries we propose regulating). The paper is currently available for free at: Daniel J. Solove & Christopher Hoofnagle, *A Model Regime of Privacy Protection* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701

I will avoid repeating the content of this paper, but I recommend that you read it as it may be helpful in crafting specific legislative solutions.

II. BEYOND SECURITY: A PROBLEM OF MANY DIMENSIONS

The litany of data leaks and improper access to personal data are the symptoms of a significant problem that Congress should address. It is important to understand the nature of the problem, as it extends far beyond just a security issue. In my recent book, The Digital Person: Technology and Privacy in the Information Age (NYU Press, December 2004), I observed that the central problem we face is caused by a lack of individual participation and empowerment when it comes to the collection and use of personal information as well as a lack of accountability among the companies that handle the data. In my book, I argued:

> We are increasingly living with digital dossiers about our lives, and these dossiers are not controlled by us but by various entities, such as private-sector companies and the government. These dossiers play a profound role in our existence in modern society.[2]

These repositories of personal information are used in ways that affect key aspects of our lives: whether we get a loan, a license, or a job. However, despite these high stakes:

> At present, the collectors and users of our data are often not accountable to us. A company can collect a person's data without ever contacting that person, without that person ever finding out about it. The relationship is akin to the relationship between strangers—with one very important difference: One of the strangers knows a lot about the other and often has the power to use this information to affect the other's life.[3]

The problem is not that companies dealing with personal information are a bunch of evil-doers bent on harming people. The collection and use of personal information can have many benefits, and the goal of an effective protection of privacy is not to stop information flow, but to empower individuals with greater control over their data and to make companies more accountable for their uses of personal data.

A. Individual Participation

People lack much participation in how their data is used or disseminated. Personal data is readily collected and disseminated without people's knowledge and consent, thus increasing people's vulnerability to identity theft, stalking, and other crimes.

---

[1] Jon Swartz, *Time Warner's Personal Data on 600,000 Missing,* USA Today (May 3, 2005).

[2] DANIEL J. SOLOVE, THE DIGITAL PERSON; TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 115 (2004).

[3] *Id.* at 102.

Identity theft is rising at an staggering rate. In an identity theft, the thief uses a victim's personal information to improperly access accounts, obtain credit in the victim's name, or impersonate the victim for other purposes. In 2003, the FTC estimated that "almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the past year."[4]

The law has attempted to deal with identity theft by enhancing criminal penalties, but this alone has been a dismal failure. The problem is that identity thieves are hard to catch. Gartner, Inc. estimates that only 1 in 700 thieves is successfully prosecuted.[5] A report by the U.S. General Accounting Office describes in great detail the difficulties with criminal investigation and prosecution of identity theft cases.[6]

In contrast, I noted in my book that:

> The identity thief's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in its collection, dissemination, and use. Consequently, it is difficult for the victim to figure out what is going on and how to remedy the situation.[7]

The problem is that the law does not afford people sufficient participation in the way that their information is managed. Identity theft is difficult for victims to detect because they have little knowledge about the information being circulated about them or how that data is being used. The victim's lack of awareness is exploited by the identity thief, who can go on a spree of fraud in the victim's name without the victim finding out about it. Therefore, solutions to the problem must provide individuals with greater knowledge and control about how their data is used.

B. Remedies for Harmed Individuals

People must be provided meaningful remedies when their data is leaked or misused. Without meaningful remedies, mere notice of a leak would be akin to a company saying: "We just had a toxic spill in your backyard. It might cause you harm, and so you might want to have periodic medical checkups." The letter from ChoicePoint to the victims of its data breach began:

> I'm writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address, and Social Security number being viewed by businesses that are not allowed to access such information. We have reason to believe that your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you.[8]

The letter recommended that people review their credit reports, and continue to check them for unusual activity. In other words, "we've had a spill, now you go and protect yourself."

Certainly, requiring disclosure of security leaks is a good first step, but merely sending people a scary letter without providing them with sufficient rights and abilities to address the problems will not suffice.

Identity theft, according to estimates, results in victims spending on average 200 hours and thousands of dollars fixing the damage.[9] Becoming victimized by identity theft is akin to contracting a chronic protracted disease. Because people have so little participation and power over their information, it is very hard for them to cure themselves and clean up their records. Identity theft can be financially and emotionally crippling, and the law does little to help people who have been victimized. States, such as California, have adopted some effective measures to assist victims in dealing with identity theft.[10] I believe that Congress should look to California's measures as it crafts a federal law addressing these issues.

---

[4] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 4, 6 (Sept. 2003). For an excellent account of the rise of identity theft, see BOB SULLIVAN, YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC (2004).

[5] Stephen Mihm, *Dumpster Diving for Your Identity,* N.Y. Times Magazine, Dec. 21, 2003.

[6] U.S. General Accounting Office, Report to the Honorable Sam Johnson, House of Representatives, Identity Theft: Greater Awareness and Use of Existing Data Are Needed 17-18 (June 2002).

[7] DANIEL J. SOLOVE, THE DIGITAL PERSON; TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 115 (2004).

[8] Letter from ChoicePoint to Californians Regarding the Data Breach (Feb. 9, 2005).

[9] Janine Benner, Beth Givens, & Ed Mierzwinski, *Nowhere To Turn: Victims Speak Out on Identity Theft: A CALPRIG/Privacy Rights Clearinghouse Report* (May 2000), at http://privacyrights.org/ar/idtheft2000.htm.

[10] The California Office of Privacy Protection maintains a comprehensive summary of California's privacy statutes: http://www.privacy.ca.gov/lawenforcement/laws.htm.

C. Deactivating Dangerous Data

The data leaks that have occurred recently are made more harmful because of another type of security issue. SSNs, birth dates, and other pieces of personal data are used by other companies as passwords to obtain access to accounts or to sign up for a credit card. It would take great imagination to design a poorer security mechanism than the use of SSNs. This is akin to using a password that anyone can readily obtain in an instant. Companies routinely sell people's SSNs, as it is not illegal to do so. SSNs are also available in many public records.[11] This "password" can then unlock virtually any account or be used to sign up for credit cards. And it is very difficult to change it. As I argued in my book "the SSN functions as a magic key that can unlock vast stores of records as well as financial accounts, making it the identity thief's best tool. . . . [T]he government has created an identification number without affording adequate precautions against its misuse."[12]

If the practice of using SSNs as passwords were halted, the leakage of SSNs would not be as dangerous and damaging to individuals. In our paper, *A Model Regime of Privacy Protection,* Chris Hoofnagle and I propose:

> Companies shall develop methods of identification which (1) are not based on publicly available personal information or data that can readily be purchased from a data broker; and (2) can be easily changed if they fall into the wrong hands. Whereas Social Security Numbers cannot be changed without significant hassle, and dates of birth and mother's maiden names cannot be changed, identifiers such as passwords can be changed with ease. Furthermore, they are not universal, and thus a thief with a password cannot access all of a victim's accounts—only those with that password. Biometric identifiers present problems because they are impossible to change, and if they fall into the wrong hands could prove devastating for victims as well as present ongoing risks to national security. Therefore, passwords are a cheap and effective way to limit much identity theft and minimize the problems victims face in clearing up the damage caused by identity theft.[13]

If businesses and other private sector organization were restricted from using SSNs as passwords, improper access to people's SSNs would not put people in such peril of identity theft and fraud.

The Gramm-Leach-Bliley (GLB) Act of 1999 requires agencies that regulate financial institutions to promulgate "administrative, technical, and physical safeguards for personal information."[14] Despite the fact that FTC regulations under the Gramm-Leach-Bliley Act establish security standards for financial institutions to "[p]rotect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer,"[15] many financial institutions continue to allow easy access to records by using SSNs as passwords. In an article entitled, *Identity Theft, Privacy, and the Architecture of Vulnerability,*[16] I argued:

> The GLB Act requires a number of agencies that regulate financial institutions to promulgate "administrative, technical, and physical safeguards for personal information." On February 1, 2001, several agencies including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision issued standards for safeguarding customer information. On May 23, 2002, the FTC issued similar security standards. Pursuant to the FTC regulations, financial institutions "shall develop, implement, and maintain a comprehensive information security program" that is appropriate to the "size and complexity" of the institution, the "nature and scope" of the institution's activities, and the "sensitivity of any customer information at issue." An information security program consists of "the administrative, technical, or physical safeguards [institutions] use to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information." The regulations set forth three objectives that a security program should achieve:
>
> (1) Insure the security and confidentiality of customer information;

---

[11] SOLOVE, DIGITAL PERSON, supra, at 115-17.

[12] SOLOVE, DIGITAL PERSON, supra, at 116.

[13] Daniel J. Solove & Christopher Hoofnagle, *A Model Regime of Privacy Protection, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701*

[14] 15 U.S.C. § 6801(b) (requiring agencies to promulgate "administrative, technical, and physical safeguards for personal information.").

[15] 16 C.F.R. § 314.3(b) (2002).

[16] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability,* 54 Hastings L.J. 1227 (2003).

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The GLB Act is on the right track in its focus on information security . . . However, the regulations under the GLB Act remain rather vague as to the specific level of security that is required or what types of measures should be taken. The regulations require institutions to designate personnel to "coordinate" the information security program; and to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information." These regulations establish rather broad obvious guidelines; they virtually ignore specifics. Of course, a rule that is too detailed in the standards it required could end up being ineffective as well . . . [S]uch regulations, if too specific, can quickly become obsolete, discourage innovation, and be costly and inefficient. However, rules that are too open-ended and vague can end up being toothless. Although security standards must not be overly specific, they must contain meaningful minimum requirements.

Ultimately, the strength of the GLB Act's security protections will depend upon how they are enforced. . . .

Despite these new security provisions, companies continue to maintain lax security procedures for the access of financial accounts and other personal data. Thus far, the FTC's efforts have been somewhat anemic. With vigorous enforcement, security practices can change. But it remains uncertain whether the FTC and other agencies will undertake such a vigorous enforcement effort.[17]

The FTC has not used the GLB Act to crack down on security, as the spate of security breaches in the news these days have occurred in spite of these regulations. The FTC could have concluded, for example, that the use of SSNs as passwords by so many financial institutions was an insufficient security procedure under the GLB standards. But it did not. Why hasn't the FTC vigorously enforced these security standards?

I can postulate two reasons. First, the security standards only apply to financial institutions rather than all the entities that process significant amounts of personal data. Second, they are rather vague, and as a result, they have not provided adequate guidance. To be effective, security standards must apply widely, not in a piecemeal fashion, and they must be more specific in nature (without being overly constraining).

D. Accuracy

Beyond identity theft, people lack the ability to easily locate and fix errors in their records that can cause them harm. Decisions are being made based on people's dossiers which are often riddled with inaccuracies. Although a recent Wall St. Journal article noted that ChoicePoint says that only .0008% of its 7.3 million background checks in 2004 had incorrect data, the authors had no difficulty finding a number of instances of people harmed by errors in ChoicePoint databases.[18] In one study, 90% of ChoicePoint's reports obtained had at least one error.[19] And there are numerous anecdotal stories reported in the media of significant errors in people's reports.[20]

The issue of accuracy demonstrates a central problem—the companies maintaining personal data are often not accountable to the people to whom the data pertains. Because of this lack of accountability, there are insufficient incentives for data brokers to maintain their records accurately. The Fair Credit Reporting Act (FCRA) requires consumer reporting agencies to maintain procedures to ensure "maximum possible accuracy."[21] However, many data brokers have databases that they claim fall outside of FCRA. And they gather data from various public record systems, which themselves might have errors. An error can infect various databases because of the fluidity by which personal information is transferred. Moreover, because peo-

---

[17] *Id.* at 45-46. The article is available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740

[18] Evan Perez & Rick Brooks, *File Sharing: For Big Vendor of Personal Data, A Theft Lays Bare the Downside,* Wall St. J., May 3, 2005, at A1.

[19] After the Breach: How Secure and Accurate is Consumer Information Held by ChoicePoint and Other Data Aggregators?, Before the California Senate Banking Committee, Mar. 30, 2005 (testimony of Pam Dixon, Executive Director, World Privacy Forum).

[20] *Id. (*testimony of Elizabeth Rosen, Registered Nurse) (noting that the report wrongly reported that she owned a deli store); Bob Sullivan, *ChoicePoint Files Found Riddled With Errors,* MSNBC, Mar 8, 2005, available at http://www.msnbc.msn.com/id/7118767/ (noting that Deborah Pierce's ChoicePoint report wrongly indicated a "possible Texas criminal history").

[21] 15 U.S.C. § 1681e(b).

ple are so out of the loop when it comes to the way their data is collected and used, they might not even discover the error. Little is done more systemically to ensure the accuracy of record systems used for background checks and other decisions about people's lives.

E. Closing the Gaps

The security breaches we are facing today are part of a larger problem, one involving information privacy. This is not a problem that can be solved with what I call the "little more care and little more notice" approach. Certainly setting minimum security standards and providing notice to consumers of security breaches are two important steps. But the larger problem is one of information privacy. In some contexts, personal information is widely collected, used, and disseminated without much control or limitation. Information today is protected in a piecemeal fashion based on who holds it. The same piece of data might be protected if held by a video rental store but completely unprotected in the hands of data brokers such as ChoicePoint or LexisNexis.[22] The current state of regulation of information is very porous, with tremendous gaps and loopholes. The result is that we have, in many respects, lost control over the way personal information is collected, managed, and used. We have a system that does not promote accountability among the users of personal information. We have a system that to a large extent leaves people out in the cold if victimized by identity theft or if harmed by an erroneous report. We have a system that thrusts on consumers the tremendous responsibility of guarding their digital dossiers, a difficult task when so many companies maintain data about them and when people have little knowledge that this is going on. Congress must put individuals back in control of their data and ensure that companies are accountable for the way they handle and use that data.

III. THE PROBLEM WITH PREEMPTION

In any solution that Congress takes, the innovative role of the states must be preserved. Thus, Congress should avoid preempting state laws when crafting federal legislation.

Many of the ideas for reforming the information system in this country emerge from state laws. Justice Brandeis said it well: "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[23] This is especially important in such a rapidly changing field such as information privacy. Not all approaches work, and we need a way to test innovative solutions. Indeed, the law that required ChoicePoint to disclose its security breach was a California law. What if there were federal preemption and such a law never existed? Would we ever have found about the security breach?

Federal legislation that preempts state law will not only shut down the real engines of innovation in the field, but it will have very detrimental long-term effects on federal legislation as well. The grist for federal legislation in privacy is often state regulatory ideas that have worked. The majority of privacy legislation has been enacted at the state level.[24] Many of the federal laws addressing privacy have adopted measures tried-and-tested in the states. The states first tried out the idea of telemarketing do-not-call lists. Many of the reforms in the 2003 federal Fair and Accurate Credit Transactions Act were based on prior state laws.[25] If Congress were to shut down this tremendous source of ideas, federal legislation will lose one of its primary developmental tools. Federal legislation in the future would suffer severely as a result.

I have often heard companies say that it is too onerous complying with so many differing laws in all 50 states. Yet if the federal legislation sets a strong floor of protection, there will be little incentive for the states to do more. In other words, if the federal legislation solves the problems, then there will not be a need for the states to act. Additionally, historically, stronger protections have only been enacted by a handful of states, not all 50. So the reality is not 50 different standards, but a floor of protection for 90% of the states with the remaining 10% adopting a slightly more protective standards. Moreover, other industries have long dealt with differing state protections, such as the auto industry and the insurance industry. Why

---

[22] Video Privacy Protection Act of 1998, Pub. L. No. 100-618, 18 U.S.C. §§2710-11.

[23] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

[24] ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (Privacy Journal 2002).

[25] Edmund Mierzwinski, *Preemption of State Consumer Laws: Federal Interference Is A Market Failure,* Government, Law and Policy Journal of the New York State Bar Association, Spring 2004 (Vol. 6, No. 1, pgs. 6-12).

are the burdens on data brokers any greater? What strikes me as most remarkable is that companies that manage billions of records of data and claim to be able to do so with remarkable depth, precision, and detail say that they cannot comply with a handful of states that have stronger protections.

Most federal privacy laws have not preempted stronger state protections: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, and the Gramm-Leach-Bliley Act.[26] In all these instances, companies have been able to comply with state laws.

IV. CONCLUSION

I am very encouraged that so many in Congress are interested in addressing the problems of data security and information privacy. My recommendations today are: (1) to focus on the larger problem by empowering individuals and making the users of data more accountable; and (2) to avoid preempting the states, as this will retard the development of privacy law for years to come.

Mr. STEARNS. I thank the gentleman. We are going to take a recess. We will quickly vote and we will be right back with the questions from the Members of Congress. So thank you for your patience.

[Brief recess.]

Chairman BARTON. The Chair would recognize himself for 5 minutes. I want to apologize for calling you back from your break, but I have got three meetings going on right now and so this would be my only chance to ask questions.

This is not a Visa card; it is a MasterCard card, but I have got—it says Joe Barton, Campaign, Joe Barton. There is only one of these cards. I hardly ever use it. Five, six times a year maybe, once a month. I got a phone call Monday; somebody in Orlando, Florida had charged $3,500 at two different Wal-Marts on this card. Now, I have been in Wal-Mart; I have been in Orlando to Disneyworld back in January, but I never went to a Wal-Mart. And the people that use—they actually had a card, not just the number, they had the card. And they went in on two different occasions, charged around $3,500. So I got a phone call, and the lady on the phone said had I been to Orlando, Florida? I said yes. She said were you there over the weekend? And I said no. And so we determined that somebody else had used this card.

Now, the gentleman from—I think Mr. Ireland is representing Visa. According to your testimony, there is a very sophisticated system to detect misappropriation or misuse of these cards, so I would assume that that is what happened with me, that it kicked in because it was two large transactions and in an area that I showed almost no use, no geographic use. Is that correct?

Mr. IRELAND. That is correct. The financial institution—bank that issued that card and probably in combination with MasterCard has a system to track authorizations on the card to see whether they fit your pattern and to see whether they fit known fraud patterns. And so they spotted a transaction that they didn't think was you——

Chairman BARTON. Now, who ends up paying for those charges? Does Wal-Mart pay for them? Does the institution that issued this card pay for them?

[26] Respectively at 18 U.S.C. § 2510 et. seq., 12 U.S.C § 3401, 47 USC § 551(g), 18 USC § 2710(f), 29 USC § 2009, 47 USC § 227(e), 18 U.S.C. § 2721, and Pub. L. No. 106-102, §§507, 524 (1999).

Mr. IRELAND. Typically, in a card-present transaction, the institution that issued the card will pay for it.

Chairman BARTON. Now what, if anything, will they do to try to actually track down the person who used this card fraudulently?

Mr. IRELAND. Well, typically, the card issuers will work with law enforcement based on the information they get to see if there is any way they can do it. We are talking in this case about the creation of counterfeit cards, which——

Chairman BARTON. They actually had a card. It wasn't just the number.

Mr. IRELAND. Exactly. Which has been a problem in the past and the credit card issuers have worked to develop security features in the card and other ways to combat card counterfeiting. But they have regular programs that are designed to prevent those kinds of fraud and to try to track them down——

Chairman BARTON. Well, how would whoever got a fraudulent card—because I just almost never use this card. How would they have actually gotten the information, obtained the information to create the fraudulent card?

Mr. IRELAND. I obviously can't answer that in this specific case. But it is possible to create fraudulent cards based on information that may be collected at the point of sale. I believe the Visa rules discourage or prevent the collection of that information, but sometimes enough information is collected at point of sale to create a fraudulent card, No. 1. No. 2, plain old theft may be involved. Somebody may have been able to get a hold of the card, steal it for a period of time and replace it.

Chairman BARTON. I—now what?

[Brief recess.]

Mr. STEARNS. If members are here, we are going to continue to go on. We have another full committee markup that we have to do in this room, and I think we have three out of the five, and we have the chairman here who is in the middle of his questions. So if the witnesses will please take their seats, and we shall continue. And with that, I recognize the chairman of the full committee, Mr. Barton.

Chairman BARTON. And, Mr. Chairman, I had about 2 minutes left on my clock, so if you want to——

Mr. STEARNS. Well——

Chairman BARTON. [continuing] reset the clock——

Mr. STEARNS. [continuing] we will give you whatever you want, sir.

Chairman BARTON. Well, we just want to be fair. I was asking a series of questions based on my personal campaign credit card being stolen over—the number stolen and used down in Florida, what the safeguards are about that. But I want to go to the next line of questions. I want to ask Mrs. Barrett, I would like to outlaw the use of Social Security numbers for any purpose except governmental purposes. What is your reaction to that?

Ms. BARRETT. Well, I think that the Social Security number has become an identifier in many, many aspects of our lives. From a standpoint of Acxiom's business, we limit its use to a very, very small number of instances. So the direct impact on something like—back to us would not be significant. But I am aware of in-

stances where it would create huge problems for either our clients or other businesses. And I——

Chairman BARTON. Well, just this calendar year, we have had I think three instances of people breaking into data systems and stealing hundreds of thousands of records that had Social Security numbers attached to them with quite a bit of personal privacy information. You know, I understand how ubiquitous the Social Security number is, and it is one of the few things that almost every American citizen has and even some non-citizens if they are working in the country. But wouldn't it be possible to create each data base its own identifier so we don't have to use the Social Security number?

Ms. BARRETT. In many cases Acxiom does help our clients, who have the records on these consumers, create their unique customer identifiers. Social Security number, however, has become a key element in identifying someone's identity when you are trying to establish who that person is up front so that——

Chairman BARTON. But you could do it without it. We have had banks a lot longer than we have had the Social Security system.

Ms. BARRETT. You could. I think we need to look carefully at whether it is government uses or other specific uses should be carved out and preserved because of the importance of it——

Chairman BARTON. Mr. Burton——

Ms. BARRETT. [continuing] restricting general uses.

Chairman BARTON. Mr. Burton, do you have a comment on that?

Mr. BURTON. No, I don't. I think our view is if you are keeping any sort of data, Social Security numbers, any sensitive data, it should be encrypted so that even if it is pilfered, it doesn't mean anything to the thieves.

Chairman BARTON. Okay. What about the gentleman, Mr. MacCarthy, who is representing Visa now.

Mr. MACCARTHY. Our sense is that the Social Security number is a key identifier in a lot of the data bases that are important for people who are issuing credit cards, when they are trying to determine whether someone who is applying for credit has a good history. The Social Security number is, in the current systems, a very important way of identifying that person and seeing whether that person has a good credit history. It is not impossible over time to move to a new system, but the legacy systems, the ones that exist now, the ones that help us fight identity theft and fraud all make heavy use of the Social Security number. And a government rule that said you simply can't use that starting tomorrow would create havoc with those systems. So we would ask you to look carefully at the idea of restricting Social Security numbers to just government use. We think right now they are——

Chairman BARTON. Well, I know that you——

Mr. MACCARTHY. [continuing] legitimate commercial uses.

Chairman BARTON. I know that you are not trying to be argumentative and that you had a legitimate business point, but at what point do we say an individual's privacy trumps that? Do we just say it is okay for these Social Security numbers to be stolen and used for all kinds of purposes for which they are not intended because of these legacy systems and all of the valid, legitimate

business reasons why it would be inconvenient to do something differently?

Mr. MACCARTHY. Two things: one is very often a way to fight identity theft and fraud, which hurts consumers, is through the effective use of Social Security numbers. So if you take that weapon away from us, it might actually hurt in protecting people against identity theft and fraud.

The second is there are some uses of Social Security that probably should be restricted. You know, the idea that a Social Security number can be simply published on the Internet or made available for non-business uses, we think that that is the kind of thing that Congress may want to look upon and restrict.

In terms of business practices, it is the current practice and maybe it should begin to be phased out—it is the current practice for Social Security numbers to be used as access numbers to gain access to accounts and other—and that may be something that should, over time, go away as well. The fact that that number is so readily available makes it very, very risky to use as an access device.

Chairman BARTON. And my time is about to expire, but as we get more and more information and more and more centralized, we have to do something. I mean we just have to. You cannot have an individual or a family that their whole financial records, their medical records, all kinds of consumer data is just out there without their permission. And the Social Security number ties that all together and it is so easy for the criminal elements—we have had testimony that organized crime is moving in to identity theft. And so I know there are legitimate business reasons why it is done, but I think the time has come to tip the balance in the favor of the individual privacy and find another way to help businesses determine the identity of people they want to give credit to. With that, Mr. Chairman, I yield back. I thank the witnesses for the inconvenience.

Mr. STEARNS. Just following up with what the chairman said, there is some talk about a second factor ID authentication, and they gave me this card, Mr. Chairman, where, instead of putting your Social Security number, what you would do is put your name and then they would ask you, based upon the permutations in this card, you would give them a number off a card. And rather than—I think that is what you talked about a little bit, Mr. Burton. You might tell the chairman here just before he goes what this second factor ID authentication would do which possibly could replace Social Security.

Mr. BURTON. Yes, well, second factor authentication is an access card and a way to identify a user. I think what it would not do is identify a user in a data base, which I think is what a lot of Social Security numbers do. But what a lot of security experts are saying, we have got to have, for everyone holding sensitive information, says the FDIC recommendation, is to use second factor authentication. And that means not only something that you know, which are passwords which you give you access to an account, but something that you physically have. So even if your password is compromised, the thieves still can't get access. The problem with this technology

to date is that it is quite expensive. It can run $40, $50 per year per user. And so for mass applications, it is simply not feasible.

And the solution that Chairman Stearns and I were discussing is called Identity Guard. Entrust just released it about 4 months ago. And what you do is you enter your user name and password in your account; you then have a card with a unique scrambled set of numbers and letters unique to you, and much like bingo, you are prompted to say, well, what is in column A-1, B-3, C-4, and then you fill in the numbers from this unique card and get access to your account.

What is interesting about this is that that prompt changes every time you log in. So it is not that there is one pin number, there is one password that someone has to steal to get access to your account. Very inexpensive, very easy to deploy, mass market application, and I think these are the kinds of technologies that the private sector is starting to come up with to address questions of access to sensitive information.

Mr. STEARNS. Thank you. You know, listening to your opening statements I sort of put together I think about seven different things that would possibly be in a bill. And I am not sure we would all agree upon these factors. But I thought I would take each one and ask you if you agree or disagree. The first I heard was uniform national notification standards for consumers in the event of a breach. Does anybody not agree with that being part of the bill? Okay. So——

Mr. BURTON. Just a——

Mr. STEARNS. Yes.

Mr. BURTON. [continuing] point of clarification for breach of unencrypted personal information. I think that is how most of the State laws read——

Mr. STEARNS. Okay——

Mr. BURTON. [continuing] so that if there is a breach and the data is encrypted, no one can read it, and so there shouldn't be a notification requirement.

Mr. STEARNS. Okay.

Mr. MACCARTHY. Mr. Chairman——

Mr. STEARNS. Yes, sir.

Mr. MACCARTHY. The one thing we would add to that is compliance with the guidelines that have been put in place by the Federal banking regulators should count as compliance with the national standard that is put in place in the legislation.

Mr. STEARNS. Okay. Good point. The second is Federal preemption with all the States. Anybody disagree with that? Okay. The third is establish an official agency role over public data providers. This was mentioned. Sort of a government agency having broad powers, something like the SEC, dealing with privacy. Does anybody disagree with that or not? It is a little more controversial. And, Ms. Barrett, I think you sort of might have some objection to that.

Ms. BARRETT. Well, I don't know that I have objection. I think that information providers have a responsibility to safeguard the information and use it for responsible purposes. And if there are enough bad actors out there that are using information irrespon-

sibly, we want those out of the marketplace. And if it takes a regulating agency to do it, then we will support that.

Mr. STEARNS. Okay, so that is—yes. This is pretty important now. What you are saying is a government regulating agency should be put in place to help and control, and, you know, you have got to be careful what you ask for here.

Mr. MACCARTHY. The only point I would ask is that the committee recognize the important role that the Federal banking regulators already play in that area——

Mr. STEARNS. Okay.

Mr. MACCARTHY. [continuing] their privacy requirements and their security requirements, notification requirements that are already administered by the banking agencies and by the Federal Trade Commission. And I don't think it would be a good idea to move enforcement from those agencies to a new agency.

Mr. STEARNS. Okay. So maybe the existing Federal Trade Commission or the existing whatever——

Mr. MACCARTHY. Yes.

Mr. STEARNS. [continuing] Gramm-Leach-Bliley where——

Mr. MACCARTHY. Yes, that would work.

Mr. STEARNS. Yes. Opportunity for consumers to inspect and correct any information that is in their data base. Yes?

Ms. BARRETT. Today, we offer the consumer the right to do that. I think that it is—when it comes to correction, it is a complicated environment, so we need to explore how a correction takes place very carefully. But the concept that the information needs to be accurate, and when it is inaccurate, we need to figure out ways to deal with it is one we support.

Mr. STEARNS. The idea is for your consumer credit you can get access to see if it is correct. And so the theory is then why can't you inspect incorrect data that has been collected to see if it is correct too?

Ms. BARRETT. We actually offer the same inspection——

Mr. STEARNS. Okay.

Ms. BARRETT. [continuing] of information in our fraud management systems.

Mr. STEARNS. I am not sure——

Ms. BARRETT. And our——

Mr. STEARNS. [continuing] everybody does though.

Ms. BARRETT. No. I don't believe——

Mr. STEARNS. And so the question, should the Federal Government step in and mandate that all data collection agencies have to provide access to consumers so they can see if the information is correct? That is a little sensitive because there is a lot there that deals with marketing and deals with——

Ms. BARRETT. I was just about to say there are different categories of data.

Mr. STEARNS. Right, different categories.

Ms. BARRETT. And so I think it is important to understand that when we want to put a standard of accuracy in and correction in and access in, that we need to do it in a way where the accuracy of the information is important to the decisionmaking process. We offer access today to all of our what we call reference products

where decisions are being made, identities are being verified with that information.

We actually do not today offer access to our marketing products. We offer an opportunity to see what kind of data we might have about you and then the chance to opt out of that. But since you can't opt out of identity systems like you can't opt out of your credit report——

Mr. STEARNS. Yes.

Ms. BARRETT. [continuing] the inspection process becomes more important.

Mr. STEARNS. Yes, it is a little more nuanced. Someone mentioned to possibly have the security officer sign to corroborate the security at the agency that collects this information. Does anybody disagree with that? It is a little bit like Tosarbi and Zoshley in which the CEO has to sign the accounting—the P and L statement. So it sounds like you might accept that.

The other idea is standard credentialing practices for customers desiring sensitive consumer data. Anybody object to that?

Ms. BARRETT. Let me just comment on that——

Mr. STEARNS. Yes.

Ms. BARRETT. [continuing] I think that credentialing is extremely important. I would caution the committee in terms of how it defines credentialing because the tools we have for credentialing today will not be the same tools that we have in 5 or 10 years——

Mr. STEARNS. Yes.

Ms. BARRETT. [continuing] and so if we do it in a way that allows the evolution of technology and other aspects to be accommodated within the requirement, it may be a good requirement. For instance, I think the Gramm-Leach-Bliley safeguards rule really actually has an implication on credentialing because it says you must have physical, procedural, system, and so on, processes in place to keep the data protected from unauthorized use. And to me credentialing becomes a part of that. So I would just urge that the committee not consider too prescriptive an approach to accommodate wherever we go with technology in the future.

Mr. STEARNS. My time is up. I think the last one I had was to encourage, perhaps through legislation, a technical solution for—well, let me—you know, instead of using your Social Security ID, to try and encourage some other way, work out so that you could access the information without using your Social Security ID. And that is sort of what we talked about in the Chairman Barton talk. So my time has expired. And with that, I recognize the ranking member.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. Mr. Ireland, you, in your testimony, talked about significant risk of harm, and you went back to FTC chairwoman saying notices should be sent only if there is a significant risk of harm. How are we going to define significant risk of harm?

Mr. IRELAND. Well, I think there is obviously a drafting issue here as to precisely the verbiage you use in how you ensure that it doesn't essentially gut the requirement. But there are numerous circumstances where identification information that could otherwise be used for identity theft, upon investigation you find out that it is clearly not going to be used for that purpose.

One thing we have seen is what might be called competitive espionage where one company manages to get a hold of the other company's customer list, and it includes identification information that might be used to open an account. But you know they have no intention of doing that. What they want to do is solicit the company's customers. And a notice in those circumstances to the customer might serve some privacy interest, but there is no real reason for the customer to go put a fraud alert on their account, for example——

Ms. SCHAKOWSKY. Well, who says that it is not of interest to the consumer in that even being solicited might, in their view—harm may not be the correct word, but you heard my colleague, Ms. Cubin, talk about being notified about some breaches which, she said, thankfully are not going to result, she believes, in any illegitimate use. But she, it seems to me, is glad to know that this information has been shared at the very least. And I can't quote you exactly the source, but at one of the many hearings on privacy, apparently a data broker has testified that the unauthorized access of information by a former employee does not constitute a significant risk. I am just a little concerned that the owners of this information are deciding for me what I might consider to be significant harm and then choosing to not provide the information to me, that there has been a breach.

Mr. IRELAND. Well, I would agree with you. I think there is a terminology and a drafting challenge there because you don't want the owners to have unlimited discretion to make that decision. Currently, under the banking agency guidance, for example, banks are required to notify the banking agency about the breach, regardless of risk. And then they are supposed to notify based on risk standard, and that is going to be worked out between the banks and the banking agencies.

There are issues where information is disclosed that have implications for privacy. There are issues where information is disclosed that have implication for credit card fraud. And there are issues where information is disclosed that have implications for identity theft in the form of opening accounts in somebody's name that are fraudulent. And the actions that a consumer would want to take on the basis of those different classes of breaches are different. If you find that you are giving notices to consumers in all of those classes, you may find that the one where they really need to take action by putting a fraud alert, for example, on their file at a consumer reporting agency under the Fact Act, as passed by Congress in 2003, gets lost among other notices that are simply addressing potential privacy issues. So I think the——

Ms. SCHAKOWSKY. You know, I mean——

Mr. IRELAND. [continuing] judgment needs to made——

Ms. SCHAKOWSKY. [continuing] let us not get too——

Mr. IRELAND. [continuing] here——

Ms. SCHAKOWSKY. [continuing] patronizing though about what consumers can really handle. I mean, we may want to deal with how we communicate that and prioritize a sense of urgency. But isn't it also true that financial institutions regulatory guidance doesn't cover breaches of data about business customers, even small business customers who have business accounts? Mr.

MacCarthy said in your absence that we should import that standard. And, you know, we are not covering all—I guess the guidance doesn't cover all consumers but only customers.

You know, we just need to make sure that—I think that we—privacy is a huge deal to people. And I think it varies in its implications, but people don't even like the idea of people just picking through it.

And with that, I just want to ask the question—I realize I am running out of time. How do I determine which data brokers have my information? I mean, does your company have information about me? How do we even know? We know about credit reports, we know how to check them, we can even get them free once a year now. But who has my information? How do I know if I want to know? Maybe each of you could quickly tell me how I know if you have got info on me?

Ms. BARRETT. Well, there are a couple ways if Acxiom had info on you that you might know about it. If you have a question about a client or about a business relationship and you ask them where did that information come from? They might well refer you to Acxiom if we provided the information for whatever that process——

Ms. SCHAKOWSKY. But they might not.

Ms. BARRETT. Well, we actually encourage our clients to do that. And so that is one avenue.

Ms. SCHAKOWSKY. They don't have to.

Ms. BARRETT. It becomes a customer service issue I think for them to——

Ms. SCHAKOWSKY. Okay.

Ms. BARRETT. [continuing] deal with—in terms of you—your relationship with them since they are the business that you have a relationship with.

Ms. SCHAKOWSKY. Okay.

Ms. BARRETT. On our website you can request, as I was talking earlier, a copy of the report of the information that we have since we do allow consumers to have access. Our web address is fairly well-known. While I don't think all consumers know it, many, many do, and you can easily get to it from privacy websites and a number of other places. Those would be the two most common ways.

Ms. SCHAKOWSKY. If we knew about Acxiom we could do that, but, you know, most consumers haven't got a clue of who is even controlling their information. Do you know what I am saying? Is there a website I could go to to say well, here is a whole list of data brokers? Here is a whole list of people—I mean, I know who my credit card companies are, so I can go there. But these other businesses that may have my information and are in the business of information are really not very well-known to people.

Ms. BARRETT. I think that is accurate. And we have actually talked about whether or not there should be a directory if you will or a website where consumers could go and learn who we are. We are certainly not trying to stay in the dark.

Ms. SCHAKOWSKY. Thank you.

Mr. BUEGE. In our case at West we really don't originate any of this information. We obtain it from the credit bureaus and other

aggregators. So in our case if you were to ask us what we have, we would certainly happily and do happily share that with consumers even though, again, we don't serve consumer markets directly. And the answer is it all comes from upstream, so what we end up doing is referring you to the source of the data to have it corrected, removed, whatever.

Mr. IRELAND. The only information we would have would be derivative of the Visa card that you have with your bank. And we act as a servicer to your bank in processing some of that information, as do other servicers. And the place to start to know where that information is is with your bank if it gave you the Visa card.

Mr. BURTON. Entrust is a security software company so we are not a data broker, and we help banks and data brokers protect information, but we don't hold any ourselves.

Ms. SCHAKOWSKY. Thank you all.

Mr. STEARNS. I thank the gentlelady. The gentlelady from Tennessee. Okay. Okay. I think what we are going to do is a second round here. We appreciate having this expertise here.

Mr. Ireland, your testimony states that Visa believes that all holders of sensitive information about consumers should be subject to the same rules. Why shouldn't different types of information be treated differently? Should data security laws differentiate between companies that maintain customer data and those that handle noncustomer data?

Mr. IRELAND. Well, the current banking rules, for example, differentiate—well, depending on whether or not you are the customer or the bank. But Visa adopted the CISP program, for example, because it saw gaps in the banking agency 501(b) and the FTC 501(b) guidance and standards like that. There was some discussion earlier about whether the banking agency standard or the FTC standard is precisely the right standard. And there is no standard that can't be improved in my mind.

But standards like that ought to apply, we believe, to classes of information that would be considered sensitive. And obviously other classes, more sophisticated information systems such as credit reporting agencies are already subject to the Fair Credit Reporting Act. But a basic security standard in our view ought to be adopted for a level of information. And it is characterized in my testimony as sensitive, and you have to sort out what that is.

One of the problems with current State legislation is that different States are defining sensitive information differently. And what you consider sensitive information depends in part on the dialog I had with Ms. Schakowsky about what you are trying to protect. If you are trying to protect against identity theft, the information is the type of information that would enable somebody to open an account with a financial institution, which is information specified in rules under Section 326 of the U.S.A. Patriot Act for example.

If you were talking about credit card account information, that is a somewhat different set of information. If you are talking about privacy interests, you are covering a still broader set of information, but you are still not probably covering information that is not personally identifiable. So as you go about that task I think yes, you have to differentiate between classes of information. But for

the same class of information, the same rules ought to apply, regardless of who has that information I would think.

Mr. STEARNS. If you could waive a wand, do you think Gramm-Leach-Bliley needs to be changed at all?

Mr. IRELAND. I think Gramm-Leach-Bliley has done a very good job of doing what it set out to do, which was to have financial institutions get control of their uses of personal information and give consumers an opportunity to opt out of certain uses of that information. And that has happened. And I think you have a very high level of compliance with that statute. But obviously there is personal information that is outside the scope of that statute, and the unauthorized use and access to that information creates risks to consumers and we think ought to be addressed by security standards.

Mr. BURTON. Mr. Chairman——

Mr. STEARNS. Yes——

Mr. BURTON. [continuing] if I could just comment——

Mr. STEARNS. Go ahead. Sure, Mr. Burton.

Mr. BURTON. [continuing] on Gramm-Leach-Bliley, because I think actually the security safeguards in Gramm-Leach-Bliley are extremely interesting, and I think that we may need to do more. But if you look at what they talk about in terms of what organizations should do to protect security, they don't talk about technology, they don't talk about mandates. They really talk about sound business practices like having a risk assessment for your personal data, making sure there is a security officer in charge of it, making sure that there is regular audits. And I think these kinds of activities are ultimately what is going to drive greater security.

And in the work that Entrust has done, including a Department of Homeland Security Committee we co-chaired, we focused really on information security as a corporate governance issue. And so to the extent that you get CEOs and Boards of Directors focused on this and with regular ports going to them about the state of the security in their organizations, suddenly you will see big progress in the way that data is protected and secured.

Mr. STEARNS. Mr. Buege, we haven't talked about in the event that there are violations and penalties. And do you think monetary penalties are appropriate for entities that disregard basic data base security due to, you know, lack of preparation, due diligence, not following good industry practices? And if so when should a data broker be sanctioned with a fine?

Mr. BUEGE. I think I would say yes, that if a data broker is not exercising appropriate diligence in terms of safeguarding the information, in terms of securing access to it appropriately, that sanctions would be an appropriate remedy. I am not sure I can speculate on, you know, what sorts of sanctions or the magnitude of those but——

Mr. STEARNS. Do you think it should be monetary or——

Mr. BUEGE. Why not? I mean, I wouldn't object to some measures like that in place. I mean, I think if that is what it takes to motivate companies to properly protect this information and to act responsibly in terms of access and systems integrity, I would have no objection to it.

Mr. STEARNS. Anybody else—I mean, that is another area we haven't talked about in the event that we do find somebody who is negligent. What kind of penalty should be enforced or is there, you know, a warning or what? I mean, depending upon obviously the offense, but if you have any feel on that, anybody else?

Ms. BARRETT. I would agree.

Mr. STEARNS. Okay, all right. Well, my time has expired on that, so the gentlelady from Tennessee.

Ms. BLACKBURN. Thank you, Mr. Chairman. And I want to thank each of you for your indulgence. I had just arrived when we had to depart. So I thank you for this. And I think it does, Mr. Chairman, point out the importance of testimony being submitted early because it does allow us to read through that and to prepare and to be ready to come into the hearings.

Ms. Barrett, I think want to begin with you if I may, please, ma'am. And I want to thank all of you for what you are doing and being with us here today. I represent an area in Tennessee that goes from Memphis to Nashville, and we have a lot of individuals that live in this district that are concerned with piracy, intellectual property theft, and, of course, a component of that is identity theft. And so we are pretty focused on this. The banking interests, the insurance interests that are in my district, the healthcare interests that are there, the identity theft comes up repeatedly. So we thank you for this.

And, Ms. Barrett, in your testimony you explained an occurrence of a client illegally obtaining information from your server and how you went about handling that. And my question for you is based on—it was a July 1904 article that was in "U.S.A. Today" that referenced an occurrence of hacking into your server by an individual who ran snipermail.com. So was Snipermail the client that you were referring to?

Ms. BARRETT. Yes, it is.

Ms. BLACKBURN. It is, okay. All right. So they were a client and not just an outside intruder. And so would you explain the vetting process that you went through before agreeing to do business with Snipermail?

Ms. BARRETT. Yes, and let me clarify—let me describe the situation. That——

Ms. BLACKBURN. Okay.

Ms. BARRETT. [continuing] might answer this plus other questions. We have a file transfer server that our clients use when they want to send us a file of data to be processed. They would send that file to this server, and then we would reach outside of our main system, pick it up, and bring it inside our firewall. It was used——

Ms. BLACKBURN. Hold on just one moment. So that transfer server is outside your normal firewall system?

Ms. BARRETT. Yes, it——

Ms. BLACKBURN. Okay.

Ms. BARRETT. [continuing] was password-protected with passwords that each client was assigned. Sometimes the files were coming to us for processing, and then when we finished with that, sometimes we would put the file back on that server to be sent back to the client. In many cases the downstream use of that file

was actually by a vender of our clients. And in the case of Snipermail, there were actually two different breaches—or two different individuals that breached the server in the same way in 2003. One of them was from a client operation. The other one was from a vendor of a client. And we posted files on that server, and the client actually gave the vendor access to the server to come and pick up the files for subsequent processing.

Ms. BLACKBURN. If I may follow up with you on that, then. So in your vetting process with your clients, are you including or requiring some type of vetting process for their vendors with which they plan to share that information?

Ms. BARRETT. We have talked about it since that incident. Since the client—this is client data, not Acxiom data, not part of our information products. We actually rely on our client to do the vetting of their own vendors.

Ms. BLACKBURN. And what is your accountability process with your clients regarding those vendor clients of theirs—the vendors of theirs? Because in essence the client is acting on the behalf of the vendor if you will. So therefore, you still have a contingent liability in that issue.

Ms. BARRETT. And what we have done since that incident is change rather dramatically the processes we use to distribute files to both clients and their vendors, tighten that process up. There are much stricter passwords that are required for that server. It is not a two-way server. There is a server for distribution and a server for receipt. The passwords are changed and verified far more frequently than they were before. And we expect a credentialing process if you will to go on between our client and their vendor.

Ms. BLACKBURN. Okay. Have you sold information on American consumers to foreign companies or foreign governments?

Ms. BARRETT. No.

Ms. BLACKBURN. You have not. Okay, great. All right. I think my time is about out. Mr. Chairman, thank you.

Mr. STEARNS. I thank you. I thank you for coming. We are through with our questions so we are going to adjourn the subcommittee, but I want to thank you for the patience you had during the evacuation here. It is very unusual, but we appreciate you taking the time to come back. We lost the GWU law professor, but we are going to submit questions to him to fulfill everything. But I think you have given us a good idea of what we should do. So your coming here today has helped sort of firm up some of the ideas we had on this bill, and we are hoping, I think, in due time here to get a bill. And so any other things that you might suggest—I have given you the outline, probably 7 or 8 of the things we are thinking about, some of them not as forcibly as the others, but you never know what can happen once you move out of the subcommittee to the full committee. But I am hoping we can mark this up in perhaps the next 30 days. So thank you very much for coming, and the subcommittee is adjourned.

[Whereupon, at 1:37 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF ARMA INTERNATIONAL

ABOUT ARMA INTERNATIONAL

Established in 1956, ARMA International (ARMA) is the non-profit membership organization for the records and information management profession. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, technologists, legal administrators, librarians, and educators. Our mission includes providing education, research, and networking opportunities to information management professionals, as well as serving as a resource to public policy makers on matters related to the integrity and importance of records and information.

ARMA also serves as a recognized standards developer for the American National Standards Institute (ANSI), participating and contributing toward the development of standards for records and information management.[1] ARMA is also a charter member of the information and documentation subcommittee of the International Organization for Standardization (ISO), aiding in the development of its records management standard.[2]

Because of the essential role of effective and appropriate information management in today's economy, ARMA International has a strong interest in issues pertaining to safeguarding consumer information and other personally identifiable information possessed by business and government.

Records and information management plays an important role in the private sector. In this new century, the most valuable commodity of business is information, often in the form of data bases of essential information required by the service sectors of our economy. The greatest responsibility for organizations will be managing and maintaining the integrity of an ever-growing flow of information, including the establishment of appropriate safeguards for sensitive information and in establishing retention schedules complaint with regulatory and statutory requirements. Issues such as what information has intrinsic value and what information will be shared and with whom are critical to the future success of 21st century organizations. These challenges call for increased recognition of the role of managing critical information and providing appropriate protections for personally identifiable information.

Organizations that embrace information management as being strategic and mission critical will ensure their competitive advantage and remain appropriate stewards of information that contains personal and private records.

DATA SECURITY INITIATIVES NEED TO BE SENSITIVE TO A WIDE VARIETY OF FACTORS

Americans demand security and privacy of their personally identifiable information. Identity theft complaints continue to rise.[3] The establishment of new systems that allow easy access and transference of personally identifiable data between parties should to be sensitive to personal privacy and grant assurance to Americans that their data will not be misused or end up in the wrong hands. ARMA believes that these systems must incorporate the best practices of records and information management.

Concerns have also begun to emerge with health care providers, financial institutions, and other users of consumer information sending personally identifiable information overseas for processing. This practice, known as "information offshoring" is becoming more and more common as organizations seek to curb costs by sending data to countries such as India, Pakistan, and Bangladesh for processing. Unfortunately, these nations lack any statutory controls for the protection personally identifiable information and it remains unclear whether existing U.S. laws, such as HIPAA, apply.[4]

---

[1] "Managing Recorded Information Assets and Resources: Retention and Disposition Program" may be viewed at http://www.arma.org/standards/public/document__review.cfm?DocID=22.

[2] "Information and documentation—Records management—Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"). ARMA fully supports ISO 15489-1. ARMA is currently developing additional records management standards beyond ISO 15489.

[3] The Federal Trade Commission reported over 400,000 complaints of identity theft logged into its ID Theft Clearinghouse as of December 2003. See prepared statement of the Federal Trade Commission on Identity Theft: Prevention and Victim Assistance, presented by Betsy Broder, Assistant Director, Division of Planning and Information, Bureau of Consumer Protection, before the Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce (December 15, 2003). http://www.ftc.gov/os/2003/12/031215idthefttestimony.pdf.

[4] In a response to a letter from Representative Edward J. Markey asking whether HIPAA covers personally identifiable information sent overseas for processing, Health and Human Services

Continued

Of primary importance from a records and information management perspective is ensuring the privacy and security of the information. Whatever information management systems are in place must ensure protection of the records and information in these two critical areas. Public sector agencies and private sector entities should not have access to personally identifiable information unless the information is essential to the organization's work. It is important that public and private sector entities identify what information is actually mission critical, who within their organizations should have access to the information, and then ensuring that the information cannot be accessed by unauthorized parties.

Established records and information management policies that follow best practices concerning retention, disposition, categorization, maintenance, or disposal may apply to aggregated data just as they apply to records in other formats.[5] The requirements for protecting records during their use cannot simply be "added on" at the end of a technology implementation. These requirements are integral to the functioning of any system which stores, retrieves and protects information, and therefore must be considered during each phase from design to final implementation and system maintenance.

WHY RECORDS RETENTION AND DESTRUCTION POLICIES ARE IMPORTANT FOR DATA SECURITY

Information is among the most valuable commodities of any organization. In the case of organizations that possess, process, and use sensitive consumer information, this information is a part of the organization's strategic business model. As such, these organizations have a significant responsibility to manage and maintain the integrity and security of this information, including the implementation of appropriate safeguards against unauthorized use and the proper disposal of the information.

ARMA notes that a significant risk of identity theft occurs at a point when a given record should be destroyed—and the best practices of records and information management and a record's retention schedule would require not only appropriate measures to ensure destruction, but also the documentation of the destruction or final disposition action.

Within the context of managing the life cycle of any information, assuring that records and information are destroyed appropriately—at the time and in the manner anticipated by the organization's retention and disposition program, and in compliance with any applicable law or regulation—is as important and deserves the same level of attention and stewardship as assuring that the information is properly maintained—both for the use of an organization in pursuit of its business purposes as well as for safeguarding the information from improper use during the useful life of the information. The appropriate destruction of a record at the end of its life cycle will assist with efforts to curb identity theft, such as the growing problem of "dumpster diving." The same best practices will safeguard the misappropriation of records stored in electronic format.

Safeguards and proper disposal are essential elements of an organization's information retention and disposition program. ARMA believes that any safeguard regime for personally identifiable information must include the formal endorsement by senior management of a written records and information management program. This would include the appropriate investment in personnel, training and organization-wide communications. It would also ensure that third party relationships endorse the same safeguards with appropriate means of ensuring compliance.

In today's distributed work environments, a wide variety of individuals create records and must therefore take responsibility to ensure those records are captured, identified and preserved. It is no longer enough to train administrative staff and assume they will make sure the records end up in the records management program. All members of management, employees, contractors, volunteers and other individuals share the responsibility for capturing records so they can be properly managed throughout the length of their required retention period.

ARMA's comments are informed by recognized practices of documenting the disposal of information and records. ISO 15489-1 Clause 8.3.7, "Retention and disposition[6]" provides: "Records systems should be capable of facilitating and implementing

---

Secretary Tommy Thompson indicated it did not. See letter from Secretary Thompson to Representative Markey dated June 14, 2004 at http://www.house.gov/markey/Issues/iss__health__resp040614.pdf.

[5] See "Managing Electronic Messages as Records (formerly: Guideline for Managing E-mail)" (ANSI/ARMA-9-200x).

[6] ISO 15489-1 Clause 3.9 defines "disposition" to mean "range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments". ISO 15489-1 Clause 3.8 defines "destruction" to mean

decisions on the retention and disposition of records. It should be possible for these decisions to be made at any time in the existence of records, including during the design stage of records systems. It should also be possible, where appropriate, for disposition to be activated automatically. Systems should provide audit trails or other methods to track completed disposition actions."

ISO 15489-1 Clause 9.9, "Implementing disposition" provides in part: "The following principles should govern the physical destruction of records—

1) Destruction should always be authorized.
2) Records pertaining to pending or actual litigation or investigation should not be destroyed.
3) Records destruction should be carried out in a way that preserves the confidentiality of any information they contain.
4) All copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed."

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act), approved by this Committee, contains a provision requiring the Federal Trade Commission and the various banking regulators to develop a disposal rule for sensitive customer information. This rule may provide a model for businesses in other industry sectors for the appropriate disposal of personally identifiable information. In its comments to the disposal rules proposed by the Commission and the various banking regulators, ARMA strongly recommended that an orgnization's safeguards include a formal, written records and information management program, consistent with ISO 15489.

CONCLUSION

ARMA International applauds the leadership of Chairman Stearns and Ranking Member Schakowsky for examining the data security issue. ARMA recommends to the Subcommittee the best practices of records and information management as an effective element for any data security or safeguards initiatives or policies.

PREPARED STATEMENT OF GAIL HILLEBRAND, SENIOR ATTORNEY, CONSUMERS UNION

SUMMARY

Consumers Union,[1] the non-profit, independent publisher of Consumer Reports, believes that the recent announcements by ChoicePoint, Lexis-Nexis, and many others about the lack of security of our most personal information underscores the need for Congress and the states to act to protect consumers from identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports. The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

And as ongoing scandals involving ChoicePoint, Lexis-Nexis, and others point to, American consumers cannot fully protect themselves against identity theft on their own. Even consumers who do "everything right," such as paying their bills on time and holding tight to personal information such as Social Security numbers and dates of birth, can become victim through no fault of their own because the companies who profit from this information have lax security standards.

"process of eliminating or deleting records, beyond any possible reconstruction". *Similarly,* Draft Standard, Section 3, "Definitions," defines "disposition" to mean "a range of processes associated with implementing records retention, destruction, or transfer decisions that are documented in the records retention and disposition schedule or other authorities. Draft Standard, Section 3 defines "destruction" to mean "the process of eliminating or deleting records beyond any possible reconstruction."

[1] Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the state of New York to provide consumers with information, education and counsel about goods, services, health and personal finance, and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with more than four million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

Therefore, Congress and the states must enact new obligations grounded in Fair Information Practices [2] on those who hold, use, sell, or profit from private information about consumers. In this context, Fair Information Practices would reduce the collection of unnecessary information, restrict the use of information to the purpose for which it was initially provided, require that information be kept secure, require rigorous screening of the purposes asserted by persons attempting to gain access to that information, and provide for full access to and correction of information held.

Consumers Union recommends that lawmakers do the following:

- **Require notice of all security breaches:** Impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. Consumers Union supports S. 751, by Senator Dianne Feinstein, which would put these requirements in place. We also believe that S. 768, introduced by Senator Charles Schumer and Senator Bill Nelson, will make an excellent notice of breach law.
- **Require and monitor security:** Impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available. S. 768, as well as S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively, would direct the Federal Trade Commission to develop such standards and oversee compliance with them.
- **Give consumers access to and a right to correct information:** Give individuals rights to see, dispute, and correct information held by information brokers. This is also addressed in the Schumer/Nelson and Nelson/Markey bills.
- **Protect SSNs:** Restrict the sale, collection, use, sharing, posting, display, and secondary use of Social Security numbers.
- **Require more care from creditors:** Require creditors to take additional steps to verify the identity of an applicant when there is an indicator of possible ID theft.
- **Grant individuals control over their sensitive information:** Give individuals rights to control who collects—and who sees—sensitive information about them.
- **Restrict secondary use of sensitive information:** Restrict the use of sensitive personal information for purposes other than the purposes for which it was collected or other uses to which the consumer affirmatively consents.
- **Fix FACTA:** A consumer should be able to access more of his or her Fair and Accurate Credit Transactions Act (FACTA) rights, such as the extended fraud alert, before becoming an ID theft victim. Further, one of the key FACTA rights is tied to a police report, which victims still report difficulty in getting and using.
- **Create strong and broadly-based enforcement:** Authorize federal, state, local, and private enforcement of all of these obligations.
- **Recognize the role of states:** States have pioneered responses to new forms of identity crime and risks to personal privacy. Congress should not inhibit states from putting in place additional identity theft and privacy safeguards.
- **Provide resources and tools for law enforcement:** Provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Law enforcement also may need new tools to promote prompt cooperation from the Social Security Administration and private creditors in connection with identity theft investigations.

After a very brief discussion of the problem of identity theft, each recommendation is discussed.

---

[2] The Code of Fair Information Practices was developed by the Health, Education, and Welfare Advisory Committee on Automated Data Systems, in a report released two decades ago. The Electronic Privacy Information Center has described the Code as based on these five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Electronic Privacy Information Center, http://www.epic.org/privacy/consumer/code__fair__info.html.

The problem of identity theft is large and growing

Current law simply has not protected consumers from identity theft. The numbers tell part of the story:

- According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the last five years, costing businesses and financial institutions $48 billion, plus another $5 billion in costs to consumers.
- Commentator Bob Sullivan has estimated that information concerning two million consumers is involved in the security breaches announced over just the six weeks ending April 6, 2005. *Is Your Personal Data Next?: Rash of Data Heists Points to Fundamental ID Theft Problem,* http://msnbc.msn.com/id/7358558
- Based on a report to the FTC in 2003 which concluded that there were nearly 10 million identity theft victims each year, Consumers Union estimates that every minute 19 more Americans become victims of ID theft.

These numbers can't begin to describe the stress, financial uncertainty, lost worktime productivity and lost family time identity theft victims experience. Even financially responsible people who routinely pay their bills on time can find themselves in a land of debt collector calls, ruined credit and lost opportunities for jobs, apartments, and prime credit. With more and more scandals coming out every week, the time has come for Congress to act to protect the security of our personal information.

Recommendations

Notification:

Notice of security breaches of information, whether held in computerized or paper form, are the beginning, not the end, of a series of steps needed to begin to resolve the fundamental conundrum of the U.S. information U.S. society: collecting information generates revenues or efficiencies for the holder of the information but can pose a risk of harm to the persons whose economic and personal lives are described by that information.

The first principle of Fair Information Practices is that there be no collection of data about individuals whose very existence is a secret from those individuals. A corollary of this must be that when the security of a collection of data containing sensitive information about an individual is breached, that breach cannot be kept secret from the individual. Recognizing the breadth of the information that business, government, and others hold about individuals, Consumers Union recommends a notice of breach requirement that is strong yet covers only "sensitive" personal information, including account numbers, numbers commonly used as identifiers for credit and similar purposes, biometric information, and similar information. This sensitive information could open the door to future identity theft, so it is vital that people know when this information has been breached.

Consumers Union supports a notice-of-breach law which does the following:

- Covers paper and computerized data
- Covers government and privately-held information
- Does not except encrypted data
- Does not except regulated entities
- Has no loopholes, sometimes called "safe harbors"
- Is triggered by the acquisition of information by an unauthorized person
- Requires that any law enforcement waiting period must be requested in writing and be based on a serious impediment to the investigation
- Gives consumers who receive a notice of breach access to the federal right to place an extended fraud alert.

Consumers Union supports S. 751, which contains these elements. S. 768 contains most, but not all, of these elements and in certain other respects provides additional protections.

Three of these elements are of special importance: covering all breaches without exceptions or special weaker rules for particular industries, covering data contained on paper as well as on computer, and covering data whether or not it is encrypted. First, a "one rule for all breaches" is the only way to ensure that the notice is sufficiently timely to be useful by the consumer for prevention of harm. "One rule for all" is also the only rule that can avoid a factual morass which could make it impossible to determine if a breach notice should have been given. By contrast, a weak notice recommendation such as the one contained in the guidance issued by the

bank regulatory agencies [3] cannot create a strong marketplace incentive to invest the time, money, and top-level executive attention to reduce or eliminate, future breaches.

Second, unauthorized access to paper records, such as hospital charts or employee personnel files, are just as likely to expose an individual to a risk of identity theft as theft of computer files. Third, encryption doesn't protect information from insider theft, and the forms of encryption vary widely in their effectiveness. Further, even the most effective form of encryption can quickly become worthless if it is not adapted to keep up with changes in technology and with new tools developed by criminals.

A requirement to give notice of a security breach elevates the issue of information security inside a company. A requirement for swift, no-exemption notice of security breaches should create reputational and other marketplace incentives for those who hold sensitive consumer information to improve their internal security practices. For example, California's security breach law has led to improved data security in at least two cases. According to news reports, after giving its third notice of security breach in fifteen months, Wells Fargo Bank ordered a comprehensive review of all its information handling practices. The column quoted a memo from Wells Fargo's CEO stating in part: "The results have been enlightening and demonstrate a need for additional study, remediation and oversight . . . Approximately 70 percent of our remote data has some measure of security exposure as stored and managed today." [4]

In another example, UC Berkeley Chancellor Robert Bigeneau announced plans to hire an outside auditor to examine data gathering, retention, and security, telling employees: "I insist that we safeguard the personal information we are given as if it were our own." [5] This announcement followed the second announced breach of the security of data held by the University in six months, this one involving 100,000 people.[6]

In the Sarbanes-Oxley Act, Congress recognized the importance of the "tone at the top," and for that reason took steps to require the corporate boards and CEOs work to improve the quality and accuracy of audited financial statements. A strong, clear notice of security breach law, without exceptions, could similarly focus the attention of top management on information security—creating an incentive for a "tone at the top" to take steps to minimize or eliminate security breaches.

Security:

Consumers Union supports S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively. These measures would direct the Federal Trade Commission (FTC)to promulgate strong standards for information security and a strong obligation to screen customers, both initially and with respect to how those customers further protect the information from unauthorized use. They also provide for ongoing compliance monitoring by the FTC. S. 768, the Schumer/Nelson bill, contains similar provisions.

If Congress wanted to take even stronger steps with respect to information brokers, it could require information brokers to undergo annual audits, paid for by the broker and performed by an independent auditor retained by the FTC, with specific authority in the FTC to require corrective action for security and customer screening weaknesses identified in the audit, as well as allowing the FTC to specify particular aspects of information security that should be included in each such audit.

Any federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness. Congress must determine the balance between the public interest in the protection of data and the business interest in the business of information brokering. Security breaches and the

---

[3] That weak recommendation allows a financial institution to decide whether or not its customers need to know about a breach, and the explanatory material even states that it can reach a conclusion that notice is unnecessary without making a full investigation. *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,* 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, 12 CFR Parts 568 and 570. Other reasons why those guidelines are insufficient to substitute for a statutory requirement to give notice include that they do not apply to non-customers about whom the financial institution has sensitive data, that there is no direct or express penalty for violation of the guideline, and that their case-by-case approach will make it extremely hard to determine in which circumstances the guidance actually recommends notice to consumers, complicating the process of showing that an obligation was unmet.

[4] D. Lazarus, "Wells Boss Frets Over Security," *S.F. Chronicle,* Feb. 23, 2005. http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/02/23/BUGBHBFCR11.DTL

[5] "Cal Laptop Security Put Under Microscope," April 6, 2005, *Inside Bay Area,* http://www.insidebayarea.com/searchresults/ci__2642564.

[6] Opinion Page, *Oakland Tribune,* April 5, 2005.

effects on consumers of the ongoing maintenance of files on most Americans by information brokers are issues too important to be delegated in full to any regulatory agency.

Access and Correction:

Two of the basic Fair Information Practices are the right to see and the right to correct information held about the consumer. S. 768, S. 500, and H.R. 1080 all address these issues. While the Fair Credit Reporting Act (FCRA) allows consumers to see and correct their credit reports, as defined by FCRA, consumers currently have no legal right to see the whole file held on them by an information broker such as ChoicePoint and Lexis-Nexis, even though the information in that file may have a profound effect on the consumer. There is also lack of clarity about what a consumer will be able to see even under the FCRA if the information broker has not yet made a report to a potential employer or landlord about that consumer.[7]

Because the uses of information held by data brokers continue to grow and change, affecting consumers in myriad ways, consumers must be given the legal right to see all of the information data brokers hold on them, and to seek and win prompt correction of that information if it is in error.

Protection for SSNs:

The Social Security number (SSN) has become a de facto national identifier in a number of U.S. industries dealing with consumers. Some proposals for reform have emphasized consent to the use, sale, sharing or posting of Social Security numbers. Consumers Union believes that a consent approach will be less effective than a set of rules designed to reduce the collection and use of sensitive consumer information.

Take, for example, an analogy from the recycling mantra: "Reduce, reuse, recycle." Just as public policy to promote recycling first starts with "reducing" the use of materials that could end up in a landfill, so protection of sensitive personal information should begin with reduction in the collection and use of such information. Restrictions on the use of the Social Security number must begin with restricting the initial collection of this number to only those transactions where the Social Security number is not only necessary, but also essential to facilitating the transaction requested by the consumer. The same is true for other identifying numbers or information that may be called upon as Social Security numbers are relied upon less.

Consumers Union endorses these basic principles for an approach to Social Security numbers:

- Ban collection and use of SSNs by private entities or by government except where necessary to a transaction and there is no alternative identifier which will suffice.
- Ban sale, posting, or display of SSNs, including no sale of credit header information containing SSNs. There is no legitimate reason to post or display individuals' Social Security numbers to the public.
- Ban sharing of SSNs, including between affiliates.
- Ban secondary use of SSNs, including within the company which collected them.
- Out of the envelope: ban printing or encoding of SSNs on government and private checks, statements, and the like
- Out of the wallet: ban use of the SSN for government or private identifier, except for Social Security purposes. This includes banning the use of the SSN, or a variation or part of it, for government and private programs such as Medicare, health insurance, driver's licenses or driver's records, and military, student, or employee identification. Any provision banning the printing of SSNs on identifying cards should also prohibit encoding the same information on the card.
- Public records containing SSNs must be redacted before posting.
- There should be no exceptions for regulated entities.
- There should be No exception for business-to-business use of SSNs.

Congress should also consider whether to impose the same type of "responsibility requirements" on the collection, sale, use, sharing, display and posting of other information that could easily evolve into a substitute "national identifier," including drivers license number, state non-driver information number, biometric information and cell phone numbers.

Creditor identity theft prevention obligations:

Information is stolen because it is valuable. A key part of that value is the ability to use the information to gain credit in someone else's name. That value exists only

[7] Testimony of Evan Hendricks, Editor/Publisher, *Privacy Times* before the Senate Banking Committee, March 15, 2005, http://banking.senate.gov/files/hendricks.pdf.

because credit granting institutions do not check the identity of applicants carefully enough to discover identity thieves before credit is granted.

Financial institutions and other users of consumer credit reports and credit scores should be obligated to take affirmative steps to establish contact with the consumer before giving credit or allowing access to an account when there is an indicator of possible false application, account takeover or unauthorized use. The news reports of the credit card issued to Clifford J. Dawg, while humorous, illustrate a real problem—creditor eagerness to issue credit spurs inadequate review of the identity of the applicant.[8] When the applicant is a dog, this might seem funny, but when the applicant is a thief, there are serious consequences for the integrity of the credit reporting system and for the consumer whose good name is being ruined.

As new identifiers evolve, criminals will seek to gain access to and use those new identifiers. Thus, any approach to attacking identity theft must also impose obligations on those who make that theft possible—those who grant credit, goods, or services to imposters without taking careful steps to determine with whom they are dealing.

At minimum, creditors should be required to actually contact the applicant to verify that he or she is the true source of an application for credit when certain triggering events occur. The triggering events should include any of the following circumstances:

- Incomplete match on Social Security number
- Address mismatch between application and credit file
- Erroneous or missing date of birth in application
- Misspellings of name or other material information in application
- Other indicators as practices change

Under FACTA, the FTC and the federal financial institution regulators are charged with developing a set of red flag "guidelines" to "identify possible risks" to customers or to the financial institution. However, FACTA stops with the identification of risks. It does not require that financial institutions do anything to address those risks once identified through the not-yet-released guidelines. The presence of a factor identified in the guidelines does not trigger a statutory obligation to take more care in determining the true identity of the applicant before granting credit. Congress should impose a plain, enforceable obligation for creditors to contact the consumer to verify that he or she has in fact sought credit when certain indicators of potential identity theft are present.

Control for consumers over affiliate-sharing, use of information, use of credit reports and credit scores:

Consumers are caught between the growth in the collection and secondary use of information about them on the one hand and the increasing sophistication of criminals in exploiting weaknesses in how that information is stored, transported, sold by brokers, shared between affiliates, and used to access credit files and credit scores.

Identity theft has been fueled in part by information-sharing between and within companies, the existence of databases that consumers don't know about and can't stop their information from being part of, the secondary use of information, and the granting of credit based on a check of the consumer credit file or credit score without efforts to verify the identity of the applicant.[9] Consumers Union has consistently supported federal and state efforts to give consumers the legal right to stop the sharing of their sensitive personal information among affiliates. Finally, it is essential to stopping the spread of numbers that serve as consumer identifiers that Congress and the states impose strong restrictions on the use of sensitive personal information for purposes other than the purpose for which the consumer originally provided that information.

Fix FACTA:

FACTA has made some things more difficult for identity theft victims, according to information provided to Consumers Union by nonprofits and professionals who assist identity theft victims. Moreover, FACTA gives only limited rights to those who have not yet become victims of identity theft, and FACTA fails to offer a pure

---

[8] Both the news stories about Clifford J. Dawg and a thoughtful analysis of the larger problem of too lax identification standards applied by creditors is found in C. Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors, in Securing Privacy in the Information Age* (forthcoming from Stanford University Press), http://papers.ssrn.com/sol3/papers.cfm?abstract__id=650162.

[9] Secondary use is use for a purpose other than the purpose for which the consumer gave the information.

prevention tool for all consumers. A consumer who asserts in good faith that he or she is about to become a victim of identity theft gets one right under FACTA—the right to place, or renew, a 90 day fraud alert. However, this type of alert places lower obligations on the potential creditor than the extended alert, which is restricted only to identity theft victims.

A consumer should be able to access more of his or her FACTA rights, such as the extended fraud alert, before becoming an identity theft victim. One key FACTA right is tied to a police report, which victims still report difficulty in getting and using.

Here are some key ways to make FACTA work for victims:

- Initial fraud alert should be one year, not 90 days
- Extended alert and other victims' rights, other than blocking of information, should be available to all identity theft victims who fill out the FTC ID theft affidavit under penalty of perjury
- Business records should be available to any consumer who fills out the FTC ID theft affidavit under penalty of perjury
- Consumers who receive a notice of security breach should be entitled to place an extended fraud alert
- Consumers who place a fraud alert have the right under FACTA to a free credit report, but this should be made automatic.

There is also work to do outside of FACTA, including work to develop a police report that could be given to victims that is sufficiently similar, if not uniform, across jurisdictions, so that the victim does not find creditors or businesses in another jurisdiction refusing to accept a police report from the victim's home jurisdiction.

Congress must encourage the states to continue to pioneer prompt responses to identity crime:

Virtually every idea on the table today in the national debate about stemming identity theft and protecting consumer privacy comes from legislation already enacted by a state. Congress must not cut off this source of progress and innovation. Instead, any identity theft and consumer privacy legislation in Congress should expressly permit states to continue to enact new rights, obligations, and remedies in connection with identity theft and consumer privacy to the full extent that the state requirements are not inconsistent with the specific requirements of federal law.

Criminals will always be more fast-acting, and fast-adapting, than the federal government. An important response to this reality is to permit, and indeed encourage, state legislatures to continue to act in the areas of identity theft and consumer privacy. Fast-acting states can respond to emerging practices that can harm consumers while those practices are still regional, before they spread nationwide. For example, California enacted its notice of security breach law and other significant identity theft protections because identity theft was a significant problem in California well before it became, or at least was recognized as, a national crime wave.

Identity theft illustrates how much quicker states act on consumer issues than Congress. According to numbers released by the FTC, there were 9.9 million annual U.S. victims of identity theft in the year before Congress adopted the relatively modest rights for identity theft victims found in FACTA. The identity theft provisions adopted by Congress in FACTA were modeled on laws already enacted in states such as California, Connecticut, Louisiana, Texas, and Virginia.[10]

Strong and broadly-based enforcement:

Consumers need effective enforcement of those obligations and restrictions Congress imposes in response to the increasing threats to consumer privacy, and of the

---

[10] See California Civil Code §§1785.11.1, 1785.11.2, 1785,16.1; Conn. SB 688 § 9(d), (e), Conn. Gen. Stats. § 36a-699; IL Re. Stat. Ch. 505 § 2MM; LA Rev. Stat. §§9:3568B.1, 9:3568C, 9:3568D, 9:3571.1 (H)-(L); Tex. Bus. & Comm. Code §§20.01(7), 20.031, 20.034-039, 20.04; VA Code §§18.2-186.31:E.

The role of the states has also been important in financial issues unrelated to identity theft. Here are two examples. In 1986, California required that specific information be included in credit card solicitations with enactment of the then-titled Areias-Robbins Credit Card Full Disclosure Act of 1986. That statute required that every credit card solicitation to contain a chart showing the interest rate, grace period, and annual fee. 1986 Cal. Stats., Ch. 1397, codified at California Civil Code § 1748.11. Two years later, Congress chose to adopt the same concept in the Federal Fair Credit and Charge Card Disclosure Act (FCCCDA), setting standards for credit card solicitations, applications and renewals. P. L. 100-583, 102 Stat. 2960 (Nov. 1, 1988), codified in part at 15 U.S.C. §§1637(c) and 1610(e). The implementing changes to federal Regulation Z included a model form for the federal disclosure box which is quite similar to the form required under the pioneering California statute. 54 Fed. Reg. 13855, Appendix G.

growth of identity theft. A diversity of approaches strengthens enforcement. Each statutory obligation imposed by Congress should be enforceable by federal agencies, the federal law enforcement structure with the Attorney General and U.S. Attorneys, and State Attorneys General. Where a state is structured so that part of the job of protecting the public devolves to a local entity, such as a District Attorney or City Attorney, those local entities also should be empowered to enforce anti-identity theft and privacy measures in local civil or, where appropriate, criminal courts.

There is also a role for a private right of action. It is an unfortunate reality in identity theft is that law enforcement resources are slim relative to the size of the problem. This makes it particularly important that individuals be given a private right of action to enforce the obligations owed to them by others who hold their information. A private right of action is an important part of any enforcement matrix.

Money and tools for law enforcement:

Even if all the recommended steps are taken, U.S. consumers will still need vigorous, well-funded law enforcement. At a meeting convened by Senator Feinstein which included some twenty representatives of law enforcement, including police departments, sheriffs, and District Attorneys, law enforcement uniformly proposed that they be given tools to more effectively investigate identity theft. Law enforcement costs money, and the law enforcers noted that the multi-jurisdictional nature of identify theft increases the costs and time, it takes to investigate these crimes.

Law enforcers in California and Oregon have noted a strong link between identity theft crime and methamphetamine. The Riverside County Sheriff noted at a March 29, 2005 event that when drug officers close a methamphetamine lab, they often find boxes of fake identification ready for use in identity theft. The drug team has closed the lab; without funding for training and ongoing officer time, there may be no investigation of those boxes of identities.

To prove a charge of attempted identity theft, a prosecutor may need to prove that the real person holding a particular driver's license number, credit or debit card number, or Social Security number is different from the holder of the fake ID. Doing this may require the cooperation of a state Department of Motor Vehicles, a financial institution, or the Social Security Administration. The public meetings of the California High Tech Crimes Advisory Committee have including discussion of the difficulties and time delays law enforcement investigators encounter in trying to obtain this cooperation. Congress should work with law enforcement and groups representing interest in civil liberties to craft a solution to verifying victim identity that will facilitate investigation of identity theft without infringing on the individual privacy of identity theft victims and other individuals.

Law enforcement may have more specific proposals to enhance their effectiveness in fighting identity theft. Consumers Union generally supports:

- Funding for regional identity theft law enforcement task forces in highest areas of concentration of victims, and of identity thieves
- Funding for investigation and prosecution
- An obligation on creditors, financial institutions, and the Social Security Administration to provide information about suspected theft-related accounts or numbers to local, state, and federal law enforcement after a simple, well designed, request process

Consumers Union believes that the time has come for both Congress and state legislatures to act to stem identity theft through strong and meaningful requirements to tell consumers of security breaches; strong and detailed security standards and oversight for information brokers, reining in the use of Social Security numbers, increased control for consumers over the uses of their information, and obligations on creditors to end their role in facilitating identity theft through lack of care in credit granting. This should be done without infringing on the role of the states, with attention to the need to fund law enforcement to fight identity theft, and with attention to the need for private enforcement by consumers. We look forward to working with the Chair and members of the Committee, and others in Congress, to accomplish these changes for U.S. consumers. These recommendations by Consumers Union have been informed by the work of victim assistance groups, privacy advocates, and others.[11]

[11] Many law enforcers, victim assistance workers, and consumer and privacy advocates were engaged in the issue of identity theft prevention long before the most recent ChoicePoint security breach came to light. Consumers Union has worked closely for many years on efforts to fight identity theft and protect consumer financial privacy with other national groups, and with consumer privacy and anti-identity theft advocates and victim assistance groups based in California. Our views and recommendations are strongly informed by the experiences of consumers

reported to us by the nonprofit Privacy Rights Clearinghouse, the nonprofit Identity Theft Resource Center, and others who work directly with identity theft victims. These groups have worked to develop the state laws that are the basis for many of the proposals now being introduced in Congress. Consumers Union is grateful for the leadership of the Privacy Rights Clearinghouse in consumer privacy policy work, the work of the state PIRGs and U.S.PIRG on consumer identity theft rights which includes the preparation of a model state identity theft statute in cooperation with Consumers Union, for the work for consumers on the accuracy of consumer credit reporting issues done over the past decade by the Consumer Federation of America and U.S. PIRG, and for the contributions to the policy debate of organizations such as the Electronic Privacy Information Center, Privacy Times, and others too numerous to mention.