H.R. 2221, THE DATA ACCOUNTABILITY AND PROTECTION ACT, AND H.R. 1319, THE INFORMED P2P USER ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MAY 5, 2009

Serial No. 111–36

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

U.S. GOVERNMENT PRINTING OFFICE
72–885 WASHINGTON : 2012

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

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
PARKER GRIFFITH, Alabama
ROBERT E. LATTA, Ohio

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois
Chairman

JAN SCHAKOWSKY, Illinois
Vice Chair
JOHN SARBANES, Maryland
BETTY SUTTON, Ohio
FRANK PALLONE, New Jersey
BART GORDON, Tennessee
BART STUPAK, Michigan
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
KATHY CASTOR, Florida
ZACHARY T. SPACE, Ohio
BRUCE BRALEY, Iowa
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member
RALPH M. HALL, Texas
DENNIS HASTERT, Illinois
ED WHITFIELD, Kentucky
CHARLES W. "CHIP" PICKERING, Mississippi
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas

CONTENTS

H.R. 2221, THE DATA ACCOUNTABILITY AND PROTECTION ACT, AND H.R. 1319, THE INFORMED P2P USER ACT

TUESDAY, MAY 5, 2009

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

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Bobby L. Rush (chairman) presiding.

Members present: Representatives Rush, Stupak, Barrow, Radanovich, Stearns, Bono Mack, Terry, Murphy of Pennsylvania, Gingrey and Scalise.

Staff present: Christian Fjeld, Counsel; Marc Gromar, Counsel; Valerie Baron, Legislative Clerk; Brian McCullough, Minority Senior Professional Staff; Will Carty, Minority Professional Staff; and Sam Costello, Minority legislative Analyst.

OPENING STATEMENT OF HON. BOBBY L. RUSH

Mr. RUSH. The subcommittee will now come to order.

Today the subcommittee is holding a legislative hearing on two bills: H.R. 2221, the Data Accountability and Trust Act, and H.R. 1319, the Informed P2P User Act. The chair will recognize himself for 5 minutes for the purposes of an opening statement.

Today the subcommittee is holding a legislative hearing on the two above-mentioned bills. They were both introduced by two distinguished members of the subcommittee, my colleagues Ms. Bono Mack and Mr. Barrow, and H.R. 2221, which is the Data Accountability and Trust Act, also known as DATA, was introduced by myself and Mr. Stearns. Ms. Bono Mack and Mr. Barrow introduced H.R. 1319. Both of these bills represent strong bipartisan efforts to address high-profile problems affecting American consumers.

H.R. 1319, the Informed P2P User Act, addresses the increasingly frequent problem of consumers inadvertently exposing their private sensitive information by way of peer-to-peer file-sharing programs. Too often when consumers download these programs onto their computers with the intent of sharing and downloading certain files on the network, they are unaware that they are also sharing other files they otherwise might want to keep private. For instance, recent media reports have focused on consumers unknowingly sharing their tax returns and their Social Security numbers

on P2P networks. Such inadvertent file sharing can be the result of deceptive or misleading disclosures by P2P software companies or they might emanate from simple confusion on the part of consumers. Whatever the case, the intent of H.R. 1319 is to provide consumers with the power of informed consent before they download P2P software onto their computers and share folders and files with network participants.

The second bill that we will be discussing today is H.R. 2221, the Data Accountability and Trust Act. This is the third Congress in which this bill has been introduced. Mr. Stearns as chairman of this subcommittee in the 109th Congress originally introduced the bill as H.R. 4127, and with the help of then-Ranking Member Schakowsky, it eventually passed the full Energy and Commerce Committee by a unanimous vote. However, no further action was taken on the bill as a result of jurisdictional disputes. In the subsequent 110th Congress, I reintroduced the bill as H.R. 958, but we were unable to take any action. Once again in this current Congress, I have reintroduced the bill with Mr. Stearns, Mr. Barton, Ms. Schakowsky and Mr. Radanovich as H.R. 2221 with the intent that it does eventually become law.

H.R. 2221 has two basic components. First, the bill requires that persons processing electronic data that contains personal information must take steps to ensure that the data is secure. Second, the bill establishes a notification procedure and process that a company must take when a data breach occurs in order to allow affected consumers to protect themselves. Companies do not have to initiate such notices of they determine that "there is no reasonable risk of identity theft, fraud or other unlawful acts." H.R. 2221 also imposes special requirements on data brokers but accommodates other laws that govern how certain data brokers are regulated. These bills may require some revision, and while this may not be the first time we have taken up data security, and H.R. 2221 already reflects significant changes forged by compromise made in the 109th Congress, the bill may be dated and in need of an update. This subcommittee is looking forward to working in a bipartisan fashion and seeking bipartisan cooperation based on our historical bipartisanship, and I expect that bipartisanship to be at work on both of these bills.

Lastly, I want to just announce for the record that I have an intention to hold a joint hearing on consumer privacy with Chairman Boucher and the Subcommittee on Communications, Technology, and the Internet and to work on comprehensive legislation. This is just a part of a larger process.

Mr. RUSH. With that, I yield back the balance of my time and recognize now for the purposes of an opening statement the ranking member on this subcommittee, Mr. Radanovich, for 5 minutes.

OPENING STATEMENT OF HON. GEORGE RADANOVICH

Mr. RADANOVICH. Thank you, Mr. Chairman. Good afternoon, everybody.

I would first like to thank the witnesses before us today and the organizations that have offered comments and suggestions assisting the important work of crafting a robust and workable data security bill. Both that bill and the P2P bill that we have, there are

core concerns about the unauthorized or inadvertent sharing of sensitive information. I want to commend Mr. Stearns, Ms. Schakowsky, Mr. Barton, Mr. Dingell, Mr. Whitfield and now Mr. Rush and Mr. Waxman, all of whom were chairmen and/or ranking members who have helped bring attention to these issues. I also want to recognize Ms. Bono Mack's leadership on digital security over the years and on her bill to prevent inadvertent file sharing on peer-to-peer networks.

File sharing presents privacy and security issues but also relates to online safety more generally, and being a father, I am glad to see that a bill that improves children's digital safety and will help protect from some of the atrocities that are being committed using these networks on line.

Huge data security breaches shocked us all starting back in 2005 with the ChoicePoint breach and millions of people in the United States had discovered that they are victims of identity theft. Billions are lost by consumers and by businesses as they spend money and time to repair their finances. Particularly in difficult economic times when credit is increasingly tough to secure, the potential disruption and obstruction of commercial activity in every sector of the U.S. economy cannot be ignored. Internet-based and other electronic transactions are fundamental these days and ensuring consumer confidence in these systems is essential. The Congress, and this committee in particular, are charged with the responsibility to ensure that the entities possessing and dealing in sensitive consumer data keep the doors locked and the alarm on.

The health of our modern network system of commerce demands it. Very simply, H.R. 2221 would create a uniform national data breach notification regime. I believe that notification must be based on the actual risk of potential harm from identity theft or other malfeasance and the mandates that we put on covered entities must be the same across the country. Allowing individual States to alter the rules will only lead to consumer confusion and unnecessary business expenses, costs that will inevitably be passed on to the consumer. Let us get a good bill that robustly protects consumers while not adding requirements that only add costs.

The world has changed since we last considered this bill, and I am anxious to hear about those developments. Some parts of the bill may now be obsolete, given the actions of the private sector, actions by both those who hold sensitive information and by companies who now offer products directly to consumers to monitor their credit. We must take all of this into account and get a workable bill that we can all support.

While the data security bill is one with which the committee has some experience, Ms. Bono Mack's bill, H.R. 1319, is a relatively new one. She was out in front on the issue last Congress, introducing an earlier version of the bill last September. Since then we have seen multiple news stories about the problems the bill attempts to addressing, inadvertent sharing of sensitive files across peer-to-peer networks. I want to state at the outset that it is not the committee's intent to simply demonize P2P software. There are many legitimate and important uses of this innovative program and I am glad that the P2P industry is here to talk about the uses of their products. However, the systems present some interesting

problems as well. Last month the P2P security company Tiversa, who is here to testify, found the schematics of Marine One, President Obama's new helicopter, on a P2P server in Iran. In other reporting it was found that millions of sensitive personal records including Social Security numbers, medical records, credit reports and tax returns with names and addresses were easily found on P2P networks.

The problem of inadvertent sharing is enhanced by the actual architecture of the programs. It is often unclear to a user what may be leaked, and it can be difficult to change settings to prevent it. After Mr. Waxman examined this in the former committee down the hall, it appears that 2 years later many P2P providers have not taken adequate steps to address this. We need to take a close look at the problem and the bill. We do not want to sweep technologies into a potential regime that we do not intend nor do we want to exclude technologies that we can all agree should be covered. How we define P2P software is critical.

Mr. Chairman, I look forward to the comments on these bills and I would like to express my gratitude to the majority for their intent to develop these bills. Thank you, Mr. Chairman.

Mr. RUSH. The chair thanks the gentleman.

The chair now recognizes Mr. Barrow for 2 minutes. Mr. Barrow is a sponsor of one of the bills and certainly I am grateful to him for his legislative work. Mr. Barrow, you are recognized for 2 minutes for the purposes of an opening statement.

OPENING STATEMENT OF HON. JOHN BARROW

Mr. BARROW. Thank you, Mr. Chairman.

We live in a world where digital technology has connected people and their ideas, their information and products, making possible all kinds of new kinds of collaboration and innovation. There is no doubt that this has made us all a lot more productive. It has also made it possible for folks to invade our personal records and reveal private information about us and our families that we choose not to disclose.

The purpose of today's hearing is to discuss threats to data security and ways we can work to fill in the gaps that leave our personal records vulnerable. I had the opportunity to work with Congresswoman Mary Bono Mack on H.R. 1319, the Informed Peer to Peer User Act, and I hope that this hearing will shed some light on the privacy and security risks that are associated with peer-to-peer file-sharing programs. A lot of folks who connect to these networks don't even realize that their most personal and private files are visible to everyone else on the network at any time. A lot of folks are posting their tax returns, financial records and personal messages on the Internet and don't even know it. I hope that our work on this committee will come up with a strategy that will let individuals know in a way that they can understand and use that the information on the computers could be at risk. We have truth in lending and we have truth in labeling. I think it is time we had truth in networking also.

I want to thank Congresswoman Mary Bono Mack for allowing me to work with her on the Informed Peer to Peer User Act and I want to thank Chairman Waxman and Ranking Member Barton

for bringing these important issues to the forefront in our committee, and most importantly, I want to thank every one of you on this panel today for being here to lend your expertise on this important subject.

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

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the other author of one of these bills that we are hearing today, Ms. Bono Mack—I am sorry—Mr. Stearns, I am sorry, the former ranking member of the subcommittee, Mr. Stearns of Florida, who is recognized for 2 minutes for the purposes of an opening statement.

Mr. STEARNS. Thank you, Mr. Chairman, and I—

Mr. RUSH. I didn't mean to confuse you with Ms. Bono Mack.

OPENING STATEMENT OF HON. CLIFF STEARNS

Mr. STEARNS. She is much better looking.

Mr. Chairman, thank you very much, and I think in your opening statement you pretty much outlined my feeling about this. Obviously this is a bill that was introduced on October 25, 2005. It was H.R. 4127, and as you pointed out, we passed this bill by unanimous consent. Ms. Schakowsky and I worked together on that bill and we had compromises. We got the bill. So I am very pleased that you have taken the initiative, the leadership to offer this bill again, and I am very glad to be an original cosponsor with you. I am hoping it has the same kind of success that we had, Ms. Schakowsky and I, because it is a very, very important bill.

Recently some hackers broke into a Virginia State website used by pharmacists to track prescription drug abuse. They took all these names and it is 8 million patients and they deleted them from the site and they are asking for money to replace them, so in a way they are asking for ransom, and if this Virginia website had an encrypted data security full-blown protection of this information, it would have been difficult, if not impossible, for these hackers to get in and to take this information. It is 8,257,000 names. And that is why this bill is so important so I am very pleased to support it.

Also, the gentlelady from California's bill, the Informed P2P User Act, which is again very important. With the diverse connectivity we have in networks, and of course with the increased broadband that we are starting to see, people are going to go more to this peer-to-peer downloading and this centralized resources in your computer and these servers going back and forth between each other, you have got to have some notification to the users what is occurring or a lot of their applications and their information will be also taken.

So it is very appropriate these two bills come together, I think, and Mr. Chairman, I commend you and your staff for bringing them both because in a way we are talking about data security with both of them and protection of the consumer, and I thank you, Mr. Chairman.

Mr. RUSH. The chair thanks the gentleman. Now the chair recognizes Ms. Bono Mack of California for 2 minutes for the purposes of an opening statement.

OPENING STATEMENT OF HON. MARY BONO MACK

Ms. BONO MACK. I thank the chair and Ranking Member Radanovich and the distinguished panel for being here today. Thank you for holding a hearing on important privacy legislation. Today my comments will focus entirely on H.R. 1219, the Informed P2P User Act, but before I dig into the issue of P2P, I would like to thank Ranking Member Barton as well as my colleague, Congressman Barrow, for their willingness to work together on H.R. 1319. As you have seen, this is a bipartisan bill and their support has been essential. I thank them both.

The risks associated with peer-to-peer file-sharing programs has been widely reported by the media and thoroughly investigated by Congress. Many of our witnesses today have testified before other Congressional committees on the dangers associated with P2P file-sharing programs, and each time the committee was given a status update of the dangers. Additionally, industry claimed ignorance and stated they would handle the problem through self-regulation. This hands-off approach has not worked and any set of voluntary best practices put forth by the P2P industry can no longer be seen as credible. To paraphrase Groucho Marx, you want me to believe you and your voluntary measures instead of my own two eyes. How many more medical records and tax returns is it going to take for us to act? How many state secrets will be made available to those who want to harm us? How much more damage are we going to allow P2P file-sharing programs to do to our economy? I believe enough is enough and the time to act is now.

Industry's opportunity to self-regulate has passed. P2P file-sharing programs like Lime Wire and Kazaa before it have proven they are either incapable of solving the problem of inadvertent file sharing on their own or they have absolutely no intention of solving the problem at all. Either way, this behavior is unacceptable, as the committee charged with consumer protection, we have a responsibility to our constituents to act.

I am also aware that some of you have concerns about some of the language of H.R. 1319. Please note that my office is very willing to listen to your concerns and work with you to craft a bill that is not overly broad but still carries out the current intent of H.R. 1319. I believe that if we work together we should be able to produce a bill that protects our constituents and preserves the legitimate use of P2P applications.

I look forward to today's discussion, and I thank the chairman very much for holding this hearing. I yield back.

Mr. RUSH. The chair thanks the gentlelady. Now the chair recognizes the gentleman from Pennsylvania, Dr. Murphy, for the purposes of an opening statement. The gentleman is recognized for 2 minutes.

OPENING STATEMENT OF HON. TIM MURPHY

Mr. MURPHY OF PENNSYLVANIA. Thank you, Mr. Chairman, and by the way, I would also like to welcome a Pittsburgher, Mr. Boback of Tiversa, he and I have spoken a number of times in the past, as well as this incredibly distinguished panel. The expertise you all have, I am excited about you being here.

The sad thing about this is, this is a discussion that has not begun today. I think some of you have testified in past years and I know that Mr. Boback and I have spoken years ago. When we look at what has been released about the documents from Marine One, a couple terabytes of information on the Joint Strike fighter jet, a whole host of so much information, it makes me wonder why anybody trusts to have any files on the computers at all. It reminds me of the way that Rome acted during the time the Barbarians were beginning to invade various parts of Germany, and I am sure some Roman emperor, some Roman generals were saying nothing to worry about, we have this system under control, even when they were sacking Rome, and I believe that is where we are now. It is not safe. The portals created by these peer-to-peer networks are huge and the fact that our Department of Defense keeps anything on any computer that is accessible from the outside still astounds me. I applaud this bill, and I think this is important because it does move a long way towards protecting consumers and families who inadvertently have their files stolen and accessed whether it is their tax records, medical records or anything else. But the best thing we need to remember for so many folks whether they are John and Jane Doe in their home somewhere or it is our defense department or is any corporation that no matter what we do here, they are still responsible for keeping the information inaccessible to the Internet because those folks from other countries who continue to send out press releases denying they are doing it and yet all paths seem to lead back to those countries, we have to understand that the wealth of information we have on our computer networks and what we have done to protect those is all for naught if we continue to put those on computers.

With that, Mr. Chairman, I yield back.

Mr. RUSH. The chair thanks the gentleman. Now the gentleman from Nebraska, Mr. Terry, is recognized for 2 minutes for the purposes of an an opening statement.

OPENING STATEMENT OF HON. LEE TERRY

Mr. TERRY. Thank you, Mr. Chairman. I want to thank you for holding today's hearing, but more specifically, we have been down this road a couple times before and I think it is imperative that we move these bills.

I am going to pile on a little bit Mr. Murphy's comments that I view this as nibbling around the edges of cybersecurity. We are pointing to specific problems and trying to come up with specific solutions. All the while we are losing sight of the forest. I am not saying these shouldn't be done but I just think we need to think about in a grander scheme of cybersecurity and how it all ties in with our national security now, our financial security, and hopefully we can start elevating the level of discussion here but I want to congratulate the authors of both of the bills here. I think you have done a decent job here of finding the right solution for these specific problems and I support them. Yield back.

Mr. RUSH. The chair thanks the gentleman and now the chair recognizes the gentleman from Georgia, Dr. Gingrey, for 2 minutes for the purposes of an opening statement.

OPENING STATEMENT OF HON. PHIL GINGREY

Mr. GINGREY. Mr. Chairman, thank you for calling this hearing today that focuses on two bipartisan pieces of legislation, H.R. 2221, the Data Accountability and Trust Act, and H.R. 1319, the Informed Peer to Peer User Act. I also want to commend both you and Ranking Member Radanovich for your collective leadership and for the spirit of comity in which this subcommittee is operating, Mr. Chairman.

At a time when our society is becoming ever more reliant on technology, whether for e-commerce or HIT, health information technology, we need to ensure the security of an individual's identity and personal information. Unfortunately, we have seen significant breaches of information that have led to identity theft, fraud and allegations that were first reported in the Wall Street Journal that Chinese hackers—it is bad enough what Ranking Member Stearns was saying about the pharmaceutical and prescription drug information but Chinese hackers stole several terabytes of data related to design and electronic systems of the Joint Strike fighter. That is some serious business.

H.R. 2221 is legislation that was first written in the 109th Congress by my colleague from Florida, Mr. Stearns. It is now being spearheaded by you, Mr. Chairman, and I applaud you on this effort. This legislation requires entities holding data that contains personal information to implement enhanced security measures to prevent future breaches. In instances in which unauthorized access does occur, then the consumers must be notified shortly thereafter that their files were compromised.

Similarly, H.R. 1319 is legislation that was introduced by Ms. Bono Mack of California, full committee Ranking Member Barton and my colleague from Savannah, Georgia, Mr. Barrow, and it is designed to protect consumers through additional information about the practice of peer-to-peer file sharing over the Internet. Simply referred to as P2P file sharing around the IT industry, this practice certainly has a number of benefits. However, too often personal information is compromised over the peer-to-peer program for various reasons, many of which of course are inadvertent. H.R. 1319 would add an additional layer of security that would prohibit peer-to-peer programs from sharing files until the program receives informed consent from the user on two separate occasions.

Mr. Chairman, we need to maintain security on the Internet in this growing technologically-based world, and I do support both bipartisan bills. I look forward to hearing from the witnesses, and I yield back.

Mr. RUSH. The chair thanks the gentleman and the chair thanks all the members of the subcommittee for their opening statements.

It is now my pleasure to introduce our outstanding expert panel. These panelists have come from far and near to be with us today, and we certainly welcome them and we certainly want to tell each and every one of you beforehand that we thank you so much for taking the time out from your busy schedule to participate with us in this hearing.

I would like to first of all introduce you now. From my far left is Ms. Eileen Harrington. Ms. Harrington is the acting director of the Bureau of Consumer Protection for the Federal Trade Commis-

sion. Next to Ms. Harrington is Mr. David M. Sohn, who is the senior policy counsel for the Center for Democracy and Technology. Next to Mr. Sohn is Mr. Robert W. Holleyman, II. Mr. Holleyman is the president and CEO of Business Software Alliance. Seated next to him is Mr. Martin C. Lafferty. He is the chief executive officer of Distributed Computing Industry Association. Next to Mr. Lafferty is Mr. Stuart K. Pratt, president and CEO of the Consumer Data Industry Association, and then next to him is Mr. Marc Rotenberg, who is the executive director of the Electronic Privacy Information Center. The gentleman next to Mr. Rotenberg is Mr. Robert Boback. He is the CEO of Tiversa, Incorporated. And lastly but not least, the gentleman seated next to Mr. Boback is Mr. Thomas D. Sydnor. He is the senior fellow and director of the Center for the Study of Digital Property of the Progress and Freedom Foundation.

Again, I want to thank each and every one of the witnesses for appearing today. It is my pleasure to extend to you 5 minutes for the purposes of opening statement, and we will begin with Ms. Harrington.

STATEMENTS OF EILEEN HARRINGTON, ACTING DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; DAVID M. SOHN, SENIOR POLICY COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY; ROBERT W. HOLLEYMAN II, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BUSINESS SOFTWARE ALLIANCE; MARTIN C. LAFFERTY, CHIEF EXECUTIVE OFFICER, DISTRIBUTED COMPUTING INDUSTRY ASSOCIATION; STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION; MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; ROBERT BOBACK, CHIEF EXECUTIVE OFFICER, TIVERSA, INC.; AND THOMAS D. SYDNOR, SENIOR FELLOW AND DIRECTOR, CENTER FOR THE STUDY OF DIGITAL PROPERTY, PROGRESS AND FREEDOM FOUNDATION

STATEMENT OF EILEEN HARRINGTON

Ms. HARRINGTON. Thank you very much, Chairman Rush, Ranking Member Radanovich and members of the subcommittee. I am Eileen Harrington, the acting director of the FTC's Bureau of Consumer Protection. I appreciate the opportunity to appear to present the Commission's testimony on data security and peer-to-peer file sharing. The Commission's views are set forth in its written testimony. My oral presentation and answers to your questions represent my views.

Let me start with data security. Companies must protect consumers' sensitive data. If they don't, that data could fall into the wrong hands, resulting in fraud and consumers losing confidence in the marketplace. The Commission has undertaken substantial efforts described fully in its written testimony to promote data security. Let me highlight three particular efforts for you: our law enforcement activities, our pending rulemaking on health information security and our study of emerging technologies.

Today the Commission announced its 26th law enforcement action against a business that we allege failed to have reasonable

procedures to protect consumers' personal information. Case number 26 is against mortgage broker James Nutter and Company for allegedly failing to implement basic computer security measures. In settling these charges, the company has agreed to maintain reasonable security measures in the future and to periodic outside audits of its security practices. The Commission's data security cases are well publicized and send a strong message to the business community: you must have reasonable data security measures in place.

Second, a few weeks ago the Commission issued a proposed rule to require that consumers be notified when the security of their health information is breached. The proposed rule arises from a mandate in the Recovery Act to address new types of web-based entities that collect or handle consumers' sensitive health information. Covered entities include those that offer personal health records which consumers can use as an electronic individually controlled repository for their medical information. Personal health records have the potential to provide numerous benefits for consumers but only if they have confidence that the security of the health information they put it in will be maintained.

Third, the Commission continues to examine new technologies to identify emerging privacy and data security issues. In February, for example, the Commission staff released a report recommending principles for industry self-regulation of privacy and data security in connection with behavioral advertising. We are also considering a petition submitted by EPIC raising data security concerns about cloud computing services provided by Google.

Finally, a few words about the proposed data security bill, H.R. 2221. The Commission strongly supports the goals of the legislation, which are to require companies to implement reasonable security procedures and provide security breach notification to consumers. We also strongly support the provisions that would give the Commission the authority to obtain civil penalties for violations. We have provided technical comments to committee staff, particularly with regard to the scope of the proposed legislation and the data broker provisions and very much appreciate the opportunity to provide input.

Turning to P2P file sharing, let us be clear about one thing. The FTC's interest is the safety and privacy of consumers' personal documents and information, not copyright piracy. Although P2P technologies may offer benefits to computing, they have also been associated with significant data security risks. The press has reported disturbing instances of sensitive documents being shared via P2P networks. Sensitive documents likely have been shared under three scenarios. First, some consumers may have shared documents because they failed to read or understand information about how to keep files from being shared or did not understand the consequences of altering default settings. Second, some consumers may have unknowingly downloaded malware that caused their files to be made available on P2P networks. Third, some businesses and other organizations that hold sensitive personal information such as tax or medical records have not implemented procedures to block installation of P2P file-sharing software on their company or organization-owned computers and networks. Some of the most highly publicized instances of personal information being shared

over P2P networks occurred because businesses failed to prevent the installation of P2P software on their systems or because their employees placed sensitive corporate documents onto home computers that had downloaded P2P software.

The FTC has worked with the P2P industry as it has set standards for disclosure and default settings that protect consumers' files and information. We have received reports about the performance of seven P2P companies and are currently reviewing them to see whether these companies comply with the industry standards. We will make the results of our review public this summer. We also educate consumers about the risks associated with these programs. In addition to a 2008 consumer alert, the FTC's Internet website, onguardonline.gov, highlights information about the risks of P2P file-sharing software.

Finally, we support legislation that requires distributors of P2P file-sharing programs to provide timely, clear and conspicuous notice and obtain consent from consumers regarding the essential aspects of those programs. H.R. 1319 may provide very useful protections for consumers. The agency has worked with committee staff on previous versions of the bill and we look forward to working with committee staff again regarding this proposed legislation, and we thank you very much for giving the FTC the opportunity to present its views today.

[The prepared statement of Ms. Harrington follows:]

Prepared Statement of

The Federal Trade Commission

"Legislative Hearing on H.R. ___, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act"

Before the

Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
United States House of Representatives

Washington, D.C.
May 4, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, I am Eileen Harrington, Acting Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on data security and peer-to-peer ("P2P") file-sharing technology, and to provide the Commission's thoughts on proposed legislation in both these areas.[1]

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. Since 2001, the Commission has brought 25 law enforcement actions that challenged businesses that allegedly failed to adequately protect consumers' personal information. These cases emphasize the importance of protecting against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis. Additionally, through extensive consumer and business education, the Commission has promoted the importance of data security.

Similarly, since 2004, the FTC has worked to address the risks to consumers presented by P2P file-sharing software programs through three key efforts. First, FTC staff have worked with industry to improve the disclosure of risk information so that consumers can make informed choices regarding their use of P2P file-sharing programs. Second, the FTC has brought law enforcement actions related to P2P file-sharing programs. Finally, the agency has taken steps to educate consumers about the risks associated with these programs.

This testimony describes the Commission's efforts in both areas. Part one of the testimony discusses the Commission's data security program. First, it summarizes the

---

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

Commission's law enforcement actions to protect the security of consumers' data. Second, it highlights key recommendations, rulemakings, and reports issued by the Commission. Third, it discusses the Commission's consumer and business education efforts and fourth, it describes initiatives to address emerging challenges in the data security area. Finally, it provides the Commission's views on H.R. _____.

Part two of the Commission's testimony discusses the agency's work involving P2P file-sharing technology. First, it describe FTC staff's efforts to assist P2P file-sharing application developers to devise best practices to help prevent consumers from inadvertently sharing sensitive data over P2P networks. Second, it describes the Commission's efforts to educate consumers about the potential risks for downloading and using P2P file-sharing software. Finally, it discusses the Commission's views on H.R. 1319.

I. Data Security

Privacy has been one of the Commission's highest consumer protection priorities for more than a decade. The FTC has worked to address privacy issues through law enforcement, regulation, consumer and business education, and policy initiatives.[2] For example, the FTC has promulgated and enforced the Telemarketing Sales Rule ("TSR");[3] helped to maintain and enforce the Do Not Call Registry[4] to respond to consumer complaints about unsolicited and

---

[2] Information on the FTC's privacy initiatives generally may be found at http://www.ftc.gov/privacy/index.html.

[3] 16 C.F.R. Part 310.

[4] The Do Not Call Registry was established by amendments to the TSR. *Id.* Information on the Do Not Call Registry, which is enforced by the FTC, the Federal Communications Commission, and the states, is available at http://www.ftc.gov/donotcall.

unwanted telemarketing; waged a multi-faceted war on identity theft;[5] brought numerous enforcement actions to reduce the incidence of spam and spyware;[6] and conducted numerous workshops and other research to examine privacy issues raised by emerging technologies and business practices.[7] In 2006, the FTC established the Division of Privacy and Identity Protection, a division devoted exclusively to privacy-related issues.

A critical component of privacy is data security. If companies do not protect the sensitive consumer information that they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector.[8]

---

[5] Information for consumers, businesses, law enforcement, and others, is available at the FTC's Identity Theft web site at http://www.ftc.gov/bcp/edu/microsites/idtheft.

[6] For a list of spyware cases, *see* http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm. For spam cases, see www.ftc.gov/bcp/conline/edcams/spam/press.htm.

[7] *See, e.g.*, Federal Trade Commission, Comment Request, 73 Fed. Reg. 37,457 (Jul. 1, 2008) (notice of consumer research regarding consumer interaction with credit reporting agencies following incident of identity theft, and request for comments).

[8] The Commission also has participated in efforts to promote data security in the public sector. For example, the Chairman of the FTC co-chaired the President's Identity Theft Task Force, through which 17 federal agencies worked together to develop a strategic plan to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006). The Task Force made specific recommendations to improve data security in the public sector. Pursuant to these recommendations, the Office of Management and Budget worked to educate all federal agencies on improving data security practices and is monitoring their performance in doing so. In addition, the Office of Personnel Management led an interagency initiative to eliminate unnecessary uses of Social Security numbers ("SSNs") in federal government human resource functions, while individual agencies are eliminating unnecessary uses of SSNs in other aspects of their work. For more information about the Task Force, *see infra* note 41.

A. Law Enforcement

To promote data security through law enforcement, the Commission brings actions against businesses that fail to implement reasonable security measures to protect sensitive consumer data. The FTC enforces several laws and rules that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[9] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[10] and imposes safe disposal obligations on entities that maintain consumer report information.[11] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices[12] in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.

Since 2001, the Commission has used its authority under these laws to bring 25 cases

---

[9] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[10] 15 U.S.C. § 1681e.

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

[12] 15 U.S.C. § 45(a).

against businesses that allegedly failed to protect consumers' personal information.[13] These cases stand for several general principles.

First, businesses that make claims about data security should be sure that they are accurate. The Commission has brought several cases against companies that allegedly misrepresented their own security procedures. In actions against Microsoft.[14] Petco.[15] Tower

---

[13] *See United States v. Rental Research Svcs.*, No. _____ (D. Minn. Mar. 5, 2009); *Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment); *In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[14] *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002).

[15] *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005).

Records,[16] Life is good,[17] and Premier Capital Lending,[18] for example, the FTC challenged claims on the companies' websites that each had strong security procedures in place to protect consumer information. The FTC alleged that, contrary to these claims, the companies did not employ even the most basic security measures.

Second, businesses should protect against common technology threats. In a number of cases, the Commission has alleged that companies failed to protect their customer information from a simple and well-known type of attack – an SQL injection – designed to install hacker tools on the companies' computer networks.[19] In addition, the Commission announced two cases last year – against retailer TJX and data brokers Reed Elsevier and Seisint – alleging that these companies failed to implement simple technologies to counteract certain basic security threats. For example, the Commission alleged that TJX failed to encrypt personal data being transmitted over various computer networks; did not limit wireless access to its networks; and failed to use readily-available security measures, such as firewalls, updated anti-virus software, and strong passwords.[20] Similarly, the Commission alleged that Reed Elsevier and Seisint failed to prevent unauthorized access to sensitive data because they allowed easy-to-guess passwords; failed to

---

[16] *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004).

[17] *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008).

[18] *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008).

[19] *See, e.g., In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007).

[20] *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (Jul. 29, 2008).

require periodic changes of passwords; failed to suspend credentials after a certain number of unsuccessful log-in attempts; and allowed users to store credentials in vulnerable formats.[21]

Third, businesses must know with whom they are sharing customers' sensitive information. One of the Commission's most well-known security cases involved ChoicePoint, which sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.[22]

Fourth, businesses should not retain sensitive consumer information that they do not need. In cases announced against BJ's Warehouse,[23] DSW Shoe Warehouse,[24] and CardSystems Solutions,[25] for example, the Commission alleged that the companies stored unencrypted, full magnetic stripe information on payment cards[26] unnecessarily – long after the time of the transaction, when the companies no longer had a business need for the information. As a result, when thieves gained access to the companies' systems, they were able to obtain hundreds of thousands – in some cases millions – of credit card numbers and security codes.

Finally, businesses should dispose of sensitive consumer information properly. One of

---

[21] *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (Jul. 29, 2008).

[22] *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006).

[23] *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sep. 20, 2005).

[24] *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006).

[25] *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sep. 5, 2006).

[26] Magnetic stripe information is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process.

the Commission's most recent cases – against CVS Caremark – illustrates this principle.[27] In that case, the Commission alleged that CVS Caremark failed to implement reasonable and appropriate procedures for handling personal information about customers and employees, particularly with respect to its practices for disposing of such information. The FTC's action followed media reports that CVS Caremark pharmacies across the country were throwing trash that contained, among other things, pill bottles with patients' names, medication instruction sheets with personal information, and payroll information, into open dumpsters. The FTC coordinated its investigation and settlement with the Department of Health and Human Services, which announced a separate agreement in which the company agreed to pay a $2.25 million fine.[28]

Some of these cases involved unfair or deceptive practices under the FTC Act, while others were brought under the GLB Act and the related Safeguards Rule or the FCRA. Although the Commission has brought its cases under different laws, all of the cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information.[29]

---

[27] *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment).

[28] The FTC also has brought recent cases involving mortgage companies' improper disposal of sensitive customer financial information. *See Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007).

[29] What is "reasonable" will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. The principle recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. At the same time, companies that put consumer data at risk can be liable even in the absence of a known breach.

B. Rulemakings and Recommendations

The Commission's efforts in the data security area also include rulemakings, reports, and recommendations to Congress. This testimony highlights four of these efforts.

First, a few weeks ago, the Commission issued a proposed rule that would require consumers to be notified when the security of their health information is breached.[30] The proposed rule arises from a mandate in the recently-enacted American Recovery and Reinvestment Act of 2009 (the "Recovery Act")[31] designed to address new types of web-based entities that collect or handle consumers' sensitive health information. These entities include (1) those that offer personal health records ("PHRs"), which consumers can use as an electronic, individually-controlled repository for their medical information, and (2) online applications through which consumers can track and manage different kinds of information in their PHRs.[32] These innovations have the potential to provide numerous benefits for consumers, but only if consumers have confidence that the security of their health information will be maintained.[33]

The Commission will continue to apply the "reasonable procedures" principle in enforcing existing data security laws.

[30] *See* 74 Fed. Reg. 17,914 (Apr. 20, 2009). The Commission is accepting public comments through June 1, 2009, and will issue an interim final rule by August 17, 2009.

[31] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, __Stat.__.

[32] For example, consumers can connect a device such as a pedometer to their computers and upload miles traveled into their personal health records.

[33] The Commission's proposed rule is part of a broader scheme set forth in the Recovery Act to address the privacy and security concerns raised by PHRs. Specifically, the Act requires the Department of Health and Human Services ("HHS") to do a study and report, in consultation with the FTC, on potential privacy, security, and breach notification requirements for PHR vendors and related entities that are not covered by the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ("HIPAA"). In the interim, the

Consistent with the Recovery Act, the proposed rule requires PHR vendors and related entities to provide notice to consumers following a breach. The proposed rule further provides that if a service provider to one of these entities experiences a breach, it must notify the entity so that the entity can in turn notify consumers. The proposed rule contains additional requirements governing the standard for what triggers notice; the timing, method, and content of notice; and notice to the FTC and HHS.

Second, the Commission in 2007 issued the Red Flags Rule, which requires businesses and organizations to detect and respond to "red flags" or signs of identity theft. The Red Flags Rule picks up where data security leaves off: It seeks to ensure that, in addition to protecting data collected from consumers, covered entities are on the lookout for signs of identity theft or attempted identity theft.[34] The Red Flags Rule follows from a mandate in the Fair and Accurate Credit Transactions Act of 2003 ("FACTA")[35] that the FTC, the Federal bank regulatory agencies, and the National Credit Union Administration jointly develop rules and guidelines for "financial institutions" and "creditors" to reduce the incidence and impact of identity theft.

The Red Flags Rule and accompanying guidelines require financial institutions and creditors that hold certain consumer accounts, or other accounts for which there is a reasonable

---

Act requires the Commission to issue a temporary breach notification rule (the proposed rule) applicable to these entities. The Act also requires HHS to promulgate final breach notification requirements for entities subject to HIPAA. Because many of the breach notification requirements applicable to FTC-regulated entities are the same as those applicable to HHS-regulated entities, the FTC is consulting with HHS to harmonize the agencies' rules.

[34] 16 C.F.R. § 681.2.

[35] Pub. L. 108-159. The FACTA amended the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*

risk of identity theft, to develop and implement a written "Identity Theft Program" to help spot identity theft. In recent months, the FTC staff has undertaken substantial outreach efforts to educate financial institutions and creditors about the Rule.[36]

Third, a critical component of maintaining data security is limiting the unnecessary use and display of Social Security numbers ("SSNs"), which can be particularly valuable to those seeking to perpetrate identity theft or other privacy harms. Last December, the Commission issued a report containing two key legislative recommendations to address this issue.[37] It recommended that Congress consider establishing national consumer authentication standards. This recommendation recognizes that the first step to minimizing the role of SSNs in identity theft is to make it more difficult for thieves to use them to open new accounts, access existing accounts, or obtain other benefits or services. Thus, the Commission recommended that Congress require private sector entities to establish reasonable procedures to authenticate new or existing customers to ensure that they are who they say they are.[38] Moreover, the report recommended that Congress consider creating national standards to reduce the public display and transmission of SSNs.

---

[36] This outreach has included developing a compliance guide for businesses, distributing general and industry-specific articles, speaking before numerous audiences, responding to individual inquiries by telephone and e-mail, and working with a number of trade associations that are developing model policies or specialized guidance for their members.

[37] *See* FTC Report, "Recommendations on Social Security Number Use in the Private Sector," (December 2008), *available at* http://www2.ftc.gov/opa/2008/12/ssnreport.shtm.

[38] The report recommended that this requirement cover all private sector entities that maintain consumer accounts, other than financial institutions already subject to authentication requirements promulgated by bank regulatory agencies.

Finally, the Commission more broadly has recommended that Congress enact federal legislation to enhance data security across the private sector. In particular, the Commission has recommended legislation requiring all companies that hold sensitive consumer data to take reasonable measures to safeguard it and to notify consumers when the security of their information is breached.[39] In addition, the Commission has recommended that Congress provide it with authority to seek civil penalties in data security cases because of the deterrent value, as equitable remedies such as disgorgement and redress are often inadequate in these cases.[40] These recommendations also were made in an April 2007 report released by the President's Identity Theft Task Force, which was co-chaired by the Attorney General and the FTC Chairman,[41] as well as in the report on SSNs described above.

---

[39] *See* Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, United States Senate, 109th Cong. (Jun.16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[40] *Id. See also* Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007) *available at* http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007) *available at* http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf.

[41] President Bush established the Task Force by Executive Order on May 10, 2006. It was comprised of 17 federal agencies and tasked with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006). The Task Force issued its Strategic Plan, including 31 recommended actions for preventing identity theft and mitigating its consequences, in April 2007. *See* The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Apr. 23, 2007, *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf. In September 2008, the Task Force issued a progress report on the implementation of the Strategic Plan recommendations, most of which have been completed. *See* The President's Identity Theft Task Force Report, Sep. 2008, *available at* http://idtheft.gov/reports/IDTReport2008.pdf.

C. Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the Commission sponsors a multimedia website, OnGuard Online, designed to educate consumers about basic computer security.[42] OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch in 2005 has attracted nearly 10 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected. For example, the FTC's identity theft primer[43] and victim recovery guide[44] are widely available in print and online. Since 2000, the Commission has distributed more than 9 million copies of the two publications, and recorded over 4 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service – in cooperation with the FTC – sent copies of the Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has

---

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

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

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

launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. The Commission has developed a second consumer education toolkit with everything an organization needs to host a "Protect Your Identity Day." Since the campaign launch in 2006, the FTC has distributed nearly 100,000 consumer education kits and over 26,000 Protect Your Identity Day kits.

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security, along with an online tutorial based on the guide.[45] These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. In addition, the FTC has held regional data security workshops for businesses in locations around the country, including workshops in Chicago, Los Angeles, Dallas and, just last week, New York. It also has released nine articles for businesses relating to basic data security issues for a non-legal audience. The articles have been reprinted in newsletters for local Chambers of Commerce and other business organizations.

D. Emerging Privacy and Data Security Issues

As part of its privacy program, the Commission examines new technologies and other developments to identify emerging privacy and data security issues affecting consumers. This

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

testimony highlights three recent initiatives in this area, all of which bear on the security of consumers' personal information.[46]

First, this February, the Commission staff released a report containing principles designed to serve as the basis for industry self-regulatory efforts to address the privacy and data security concerns raised by behavioral advertising.[47] Behavioral advertising is the practice of tracking an individual's online activities in order to deliver targeted advertising tailored to that individual's interests.[48] Although it may provide benefits to consumers in the form of advertising that is more relevant to their interests and the subsidization of free online content, it also raises privacy concerns. In particular, consumers may be uncomfortable about being tracked. Further, without adequate safeguards, consumer tracking data – which sometimes includes sensitive data about children, health, or a consumer's finances – could fall into the wrong hands or be used for unanticipated purposes.

To address these concerns, the FTC staff principles provide for transparency, consumer control, and reasonable security for consumer behavioral data. They also call for companies to obtain affirmative express consent from consumers before they (1) use data in a manner that is

---

[46] Other recent initiatives include, for example, a Town Hall on the privacy and security issues associated with contactless payment mechanisms and a Town Hall and staff report on mobile marketing. *See* Workshop Information Page, "Pay on the Go: Consumers and Contactless Payment," *available at* http://www2.ftc.gov/bcp/workshops/payonthego/index.shtml; Workshop Information Page, "Beyond Voice: Mapping the Mobile Marketplace," *available at* http://www2.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

[47] *See* Press Release, "FTC Staff Revises Online Behavioral Advertising Principles," Feb. 12, 2009, *available at* http://www2.ftc.gov/opa/2009/02/behavad.shtm.

[48] An example of how behavioral advertising might work is as follows: a consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights to New York City.

materially different than promised at the time of collection; and (2) collect and use "sensitive" consumer data for behavioral advertising. Staff will continue to examine this marketplace and take actions to protect consumers as appropriate.

Second, the Commission recognizes that, as more data flows across geographic borders, protecting that data will require international cooperation. In March 2009, FTC staff held a two-day international conference titled "Securing Personal Data in the Global Economy."[49] The conference was co-organized with the Asia-Pacific Economic Cooperation forum and the Organisation for Economic Co-operation and Development. It addressed how companies can manage data security in a global environment where data can be stored and accessed from multiple jurisdictions. The Commission will continue to partner with international organizations and its foreign counterparts to maintain data security across borders without restricting information flows that benefit consumers.

Third, the FTC is examining the practice of cloud computing, which is defined broadly as the provision of internet-based computer services. Cloud computing allows businesses and consumers to use software and hardware located on remote networks operated by third parties. Because cloud computing reduces the need for businesses and consumers to purchase software and hardware themselves, it may be a less costly way for them to manage, store, and use data. Although cloud computing is still an emerging business model, the Commission is seeking to understand its privacy and data security implications for consumers. The Commission also is

---

[49] *See* Workshop Information Page, "Securing Personal Data in the Global Economy," *available at* http://www2.ftc.gov/bcp/workshops/personaldataglobal/index.shtm.

considering a petition submitted by the Electronic Privacy Information Center in March 2009 raising data security concerns about Google's provision of cloud services to consumers.[50]

E. H.R. _____.

Finally, the Commission appreciates the opportunity to comment on H.R. _____. The Commission strongly supports the goals of the legislation to require companies to (1) implement reasonable security policies and procedures and (2) provide notification to consumers when there is a security breach. The Commission also supports the legislation's provisions that would give the Commission the authority to obtain civil penalties for violations.[51]

The Commission would like to make two recommendations in particular at this time. First, the Commission recommends that the proposed legislation not be limited to security of *electronic* information, because the breach of sensitive data stored in paper format can be just as harmful to consumers.[52] In addition, the data broker provisions of the proposed legislation establish a procedure for customers to obtain access to and dispute information held by a broker. The Commission believes it is important to ensure that these provisions (1) are compatible with, and do not displace, the protections afforded to consumers under the FCRA; and (2) are targeted

---

[50] *See* EPIC Complaint Before the Federal Trade Commission, In the Matter of Google, Inc., and Cloud Computing Services, Mar. 19, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[51] As noted above, these provisions are consistent with prior Commission legislative recommendations.

[52] According to one recent survey, a significant number of breaches involve paper documents. *See* Ponemon Institute, *Security of Paper Documents in the Workplace*, (Oct. 2008), *available at* http://www.ponemon.org/data-security.

to uses of information that raise concerns for consumers and are not already covered by the FCRA.[53] The Commission looks forward to working with Congress on this legislation.

II. Peer-to-Peer File Sharing

Since 2004, the FTC has worked to address the risks to consumers presented by P2P file-sharing software programs. In that time, FTC staff has worked with industry to improve the disclosure of risk information on P2P file-sharing software web sites, brought law enforcement actions related to P2P file-sharing,[54] and taken steps to educate consumers about risks associated with the software. In December 2004, the FTC held a public workshop to consider the consumer protection, competition, and intellectual property issues raised by P2P file-sharing. The workshop featured more than forty representatives from the P2P file-sharing software industry, entertainment industry, high-technology research firms, government agencies, academic institutions, and consumer groups. In June 2005, the FTC released a staff report based on the information received in connection with the workshop.[55]

---

[53] Data brokers that collect and sell data to third parties for purposes of making eligibility decisions about consumers - most notably for credit, insurance, or employment - would generally be consumer reporting agencies subject to the access and correction provisions of the FCRA. *See* 15 U.S.C. § 1681 *et seq.*

[54] *FTC v. Cashier Myricks Jr.*, Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sep. 27, 2005) (suit against the operator of the web site MP3DownloadCity.com for making allegedly deceptive claims that it was "100% LEGAL" for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games); *FTC v. Odysseus Marketing, Inc.*, Civ. No. 05-330 (D.N.H., filed Sep. 21, 2005) (suit against the operator web site that encouraged consumers to download free software that they falsely claimed would allow consumers to engage in anonymous P2P file-sharing).

[55] *P2P File-Sharing Technology: Consumer Protection and Competition Issues*, Federal Trade Commission Staff Report (June 2005), *available at* www.ftc.gov/reports/p2p05/050623p2prpt.pdf.

A. Reducing Sensitive Information on P2P Networks

Although P2P technologies make possible significant operational benefits to computing, provide individual users with easy and fast access to content, and enable new business models, they have been associated not only with copyright piracy but also with significant data security risks. Indeed, recent headlines have highlighted disturbing instances of sensitive documents being shared via P2P networks. These have included documents disclosing avionics details of the President's helicopter, financial information of a Supreme Court Justice, and many thousands of tax returns and medical records of ordinary citizens. Sensitive documents may become available on P2P networks because they have been inadvertently shared by consumers and businesses using file-sharing software, or because of malware. Regardless of how this information makes its way to the networks, the Commission is working to reduce its availability by: coordinating with the P2P technology industry to implement safeguards to minimize inadvertent file sharing; initiating law enforcement investigations against companies that fail to take reasonable and appropriate measures to prevent sensitive data from being shared on P2P networks; and educating consumers and businesses about the risks associated with using P2P file-sharing programs and other online activities so that they can better protect themselves.

B. Reasonable and Appropriate Security Measures

Organizations that maintain sensitive consumer data have a duty to protect the data, and that includes taking reasonable and appropriate measures to prevent the sensitive data from exposure on P2P networks. P2P file-sharing applications that connect computers to open file-sharing networks are not likely to be appropriate to install on computers used to store and access sensitive documents. Businesses responsible for the confidential information of others must have

in place procedures to control effectively the ability of their employees and contractors to install such applications on computers with sensitive information, and should educate their employees and contractors about safe computing and data-handling practices. The FTC is investigating instances where companies may have exposed, through P2P software, the sensitive data of thousands of consumers.

C. Protections Against Inadvertent File Sharing – Industry Best Practices and Developments

FTC staff has taken an active role in assisting P2P file-sharing software developers in devising best practices to help prevent consumers from inadvertently sharing personal or sensitive data over P2P networks. In July 2008, the Distributed Computing Industry Association ("DCIA") published Voluntary Best Practices containing useful safeguards against inadvertent file sharing. These safeguards, which apply to the functionality of the software programs themselves, include: warnings to application users and notices about the number and types of files being shared; default settings that limit what is shared upon installation of an application; controls for users to stop sharing any file or folder; protections against any user attempt to share sensitive folders or file types; and simple means to disable the file-sharing functionality. Starting in February 2009, DCIA members began providing the FTC staff with reports outlining the ways in which they believe their applications comply with the best practices. FTC staff is currently assessing, with the assistance of an independent P2P technology expert, whether the member companies' applications, and those of other developers, comply with those best practices.

Even prior to DCIA publishing its "best practices" document, FTC staff observed some improvements in P2P application interface design that should help to protect many consumers against inadvertent sharing of personal documents. Following the Committee's previous hearing

in July 2007, Lime Wire implemented safeguards in its user interface to reduce the risk that users would inadvertently share documents likely to contain sensitive, personal information. For example, as of spring 2008, users of new versions of the LimeWire application could not share their entire hard drives. Warnings would appear to deter users from sharing a "My Documents" folder, and default settings would prevent the sharing of sensitive file types such as word processing documents and PDFs. Independent experts hired by the FTC[56] concluded that even though the interface could still be improved, Lime Wire had provided safer defaults and enhanced protections against inadvertent sharing of user-originated files.[57] Those safeguards appear to have been carried through to, or improved upon in, the current version of the LimeWire application.[58]

D. Consumer Education

In February 2008, the FTC updated its consumer alert entitled, "P2P File-Sharing: Evaluate the Risks."[59] The alert warns consumers about the potential risks from downloading and using P2P file-sharing software, including the risk of inadvertently sharing files or receiving spyware, viruses, infringing materials, or unwanted pornography mislabeled as something else. The alert recommends that consumers carefully set up the file-sharing software so that they do

---

[56] The FTC contracted with Dr. Nathaniel Good and Aaron Krekelberg, experts on human-computer interface design in P2P file-sharing applications. Good and Krekelberg wrote the widely-cited article, *Usability and Privacy: a Study of KaZaA P2P File-Sharing* (2003).

[57] User-originated files are those stored on the user's computer that were not downloaded from the P2P network.

[58] We recognize that P2P technologies have often been misused for copyright infringement itself, a matter that is outside our bailiwick.

[59] *Available at* www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm.

not open access to information on their hard drives such as tax returns, e-mail messages, medical records, photos, or other personal documents.

In addition, the FTC's Internet education web site, OnGuardOnline.gov, contains downloadable information about the risks of P2P file-sharing software, including quick facts about P2P file-sharing, an interactive quiz, and additional lessons, resources, and activities from i-SAFE, an organization involved in Internet-safety education.[60] In addition to providing information on topics such as P2P file-sharing, social networking, identity theft, phishing, spyware, and spam, OnGuardOnline features up-to-date articles from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), including a piece entitled "Risks of File Sharing." OnGuardOnline has had nearly ten million unique visits since its launch. The Commission is pleased to report that some file-sharing software distributors are providing links to the FTC's consumer education materials on P2P file sharing.

E. Legislative Steps to Address Inadvertent File Sharing

Although many P2P file-sharing program developers have voluntarily implemented safeguards against the risk of inadvertent sharing of user-originated files in current versions of their programs, the FTC is supportive of legislation that mandates distributors of P2P file-sharing programs provide timely, clear, and conspicuous notice and obtain consent from consumers regarding the essential aspects of those programs. In this regard, H.R. 1319 may provide useful protections for consumers. It permits the FTC to obtain civil penalties against the distributors who do not meet a baseline standard of providing clear and conspicuous notice, in advance, to consumers about what files a P2P program will share, and for obtaining consent from consumers

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

before making those files available on a P2P network. The proposed legislation also has provisions that should help network administrators keep P2P file-sharing applications that are inappropriate and potentially dangerous off their computer systems and would give the Commission authority to seek civil penalties for violations. The agency has worked with Committee staff on previous versions of the bill and looks forward to working with Committee staff regarding the proposed legislation.

Conclusion

The FTC is committed to ensuring the security of consumers' personal information and will continue to assess the risks associated with P2P file-sharing technology. The FTC thanks this Subcommittee for focusing attention on these important issues, and for the opportunity to describe how the agency has most recently addressed them.

Mr. RUSH. The chair now recognizes Mr. Sohn for 5 minutes.

STATEMENT OF DAVID M. SOHN

Mr. SOHN. Chairman Rush, Ranking Member Radanovich, members of the subcommittee, thank you for the opportunity to participate in today's hearing. The Center for Democracy and Technology is very pleased to see this subcommittee focusing on data privacy and security issues. Based on my conversations with subcommittee staff, I am going to focus my comments this afternoon on the Data Accountability and Trust Act with just a few words at the end about the Informed P2P User Act.

But before I do that, I would like to make a general point. Both of the bills that are the focus of today's hearing reflect the fact that technology has greatly expanded the ability to collect, store, use and share personal data. The modern information economy that this makes possible has many benefits but it also has greatly changed the privacy landscape and it has expanded the risk of inappropriate disclosure of personal data. Unfortunately, the law has simply not kept pace with these changes. In particular, the United States has no general privacy law establishing any kind of fair baseline of principles or expectations to govern consumer privacy, and in the absence of that kind of overall legal framework, when new privacy issues arise, Congress is essentially left to legislate on a one-off basis without any clear guiding principles and without necessarily much consistency. The result, what we have today, is a confusing patchwork of laws in this area. So based on that, CDT would certainly urge the subcommittee to put a high priority on the enactment of baseline federal privacy legislation and we are very happy to hear Chairman Rush saying today that he plans a joint hearing and does plan to work on comprehensive privacy legislation.

Now I would like to turn to the Data Accountability and Trust Act. CDT supports the idea of a nationwide data breach notification standard so long as that standard is as least as effective as the laws already in place at the State level. The key point to understand here is that data breach notification is already the law of the land because it is required by all but a few of the States. So from a consumer perspective, replacing State notification laws with a weak federal standard could actually be a step backwards, and even replacing them with a good federal standard still doesn't offer a lot of tangible progress. The principal consumer gains from H.R. 2221 therefore come from section 2 of the bill, namely the provision for requiring data security procedures and especially the provisions requiring information brokers to let consumers review what is in their data broker files. Based largely on these provisions, the CDT does support the framework set forth in the bill.

My written testimony offers some suggestions for improvements to the bill. For example, the breach notification provisions could be improved by requiring a company that suffers a breach but determines that there isn't enough risk to notify consumers to nonetheless provide a brief explanation to a regulator basically just to keep everybody honest. For the provisions on security standards and consumer access to information broker files, CDT recommends taking a close look at the scope of those requirements. In particular,

the bill uses a definition of personal data that is really quite limited, which may make sense for breach notification provisions but might make less sense for the provisions in section 2.

Preemption deserves a mention as well. It is important to note that preempting State laws in this area is a very significant step. The only reason we are here talking about breach notification today is that notification laws were pioneered by the States and especially California. States were able to do that because the Gramm-Leach-Bliley Act preempted inconsistent State laws but otherwise left States free to experiment. Fortunately, the authors of H.R. 2221 have been careful with preemption. CDT does believe that preemption makes sense for the specific issue of breach notification and the bill does provide for that. I would just say that as the bill moves forward, Congress needs to keep in mind that the price of preemption must be strong federal action and that overbroad preemption has to be avoided. Overall, CDT does appreciate the careful work of Chairman Rush and the other sponsors of this bill and we stand ready to cooperate with them on possible improvements as the bill moves forward.

Finally, just a couple words on the Informed P2P User Act. CDT absolutely supports the principle that file-sharing software should clearly communicate to users how their files may be made available to third parties. Inadvertent sharing of personal files is a very serious privacy matter. As set forth in my written testimony, however, legislating this area does pose some difficulties. CDT has reservations about the potential unintended breadth of the bill and also has some reservations about Congress starting down the path of imposing specific design mandates for software developers. That said, we share the broad goal and my written testimony offers some ideas for modifications to consider if the subcommittee chooses to proceed with the bill.

Thanks again for the opportunity to testify.

[The prepared statement of Mr. Sohn follows:]

CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of David Sohn
Senior Policy Counsel
Center for Democracy & Technology

before the

Subcommittee on Commerce, Trade, and Consumer Protection,
U.S. House of Representatives Committee on Energy and Commerce

Legislative Hearing on

H.R. 2221, the Data Accountability and Trust Act
and
H.R. 1319, the Informed P2P User Act

May 5, 2009

On behalf of the Center for Democracy and Technology, thank you for the opportunity to participate in this hearing on the Data Accountability and Trust Act and the Informed P2P User Act.

CDT is a nonprofit, public interest organization dedicated to promoting privacy, civil liberties, and democratic values on the open and decentralized Internet. CDT has been a leader in the policy debates over privacy issues raised by the Internet and other new technologies, from spyware to data mining to electronic surveillance. In particular, CDT has argued that Congress should take a more comprehensive approach to privacy in order to promote trust and consumer confidence in the digital environment.

CDT applauds the Subcommittee for focusing on the privacy-related legislation that is the subject of this hearing. This testimony will start with some observations about privacy challenges in the modern technological environment and the need for general privacy legislation. It will then offer CDT's analyses of the specific provisions of the Data Accountability and Trust Act and the Informed P2P User Act.

Modern Privacy Challenges and the Need for General Privacy Legislation

The bills that are the subject of today's hearing both address risks that consumers' personal data could be improperly disclosed. Each imposes responsibilities on certain companies for mitigating some of those risks. In addition, each contains provisions aimed at empowering consumers – in one case by ensuring consumers' ability to see and potentially correct their data broker files, and in the other by requiring clear disclosure about file sharing software.

The common background to these bills is that technology has created powerful new ways to gather, store, sort, analyze, locate, correlate, and disseminate data. This has enabled increasingly intensive use of personal data, which can deliver significant benefits. For example, businesses obtain and share personal information in order to facilitate valuable economic transactions and provide more customized services. Large databases of personal information are used to help detect and prevent fraud. The government uses personal information to determine eligibility for government benefits, for tax collection, and to support law enforcement and anti-terrorism efforts.

But the growing use of personal data raises a host of privacy challenges as well. Most consumers have only a limited understanding of the multiple ways that their data is used and shared in today's data economy. Since the widely publicized security breach at ChoicePoint in 2005, there has been a nearly continuous stream of announcements of data security breaches at companies, government agencies, and universities. Consumers are concerned that they lack control over their personal information, and identity theft has become all too frequent.

Despite the unprecedented challenges to privacy in the modern environment, there is still no comprehensive law that spells out consumers' privacy rights in the commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage.

CDT commends the Subcommittee for taking a careful look at the specific bills that are the focus of today's hearing. We also believe, however, that it is important to recognize that the bills address individual corners of a broader puzzle. Having sound practices to protect against and respond to data breaches, as the Data Accountability and Trust Act would require, is only one aspect of the custodial obligations that should apply to those who collect, use, and store personally identifiable information. Similarly, peer-to-peer file sharing software is only one avenue by which consumers may share files and perhaps inadvertently disclose personal information.

CDT would urge this Subcommittee to give high priority to developing a single, consistent regime of baseline privacy standards. Such legislation would be based on the "Fair Information Practices," a set of principles that date back several decades and have been widely acknowledged as the cornerstone for privacy protection. For consumers, baseline privacy legislation would seek to ensure greater control over how personal data is shared and used, and to provide redress for consequences that result from mistaken or inappropriate use or disclosure of that data. For entities collecting, using, or sharing consumers' personal data, legislation would establish accountability for being a responsible custodian of the data.

CDT has testified previously on the need for baseline privacy legislation and would welcome the opportunity to work with the Subcommittee on such a bill.

The Data Accountability and Trust Act, H.R. 2221

The Data Accountability and Trust Act features three principal elements. It would create a nationwide data breach notification standard; require entities that electronically store personal information to implement security safeguards, similar to the safeguards currently required for financial data under FTC rules implementing the Gramm-Leach-

Bliley Act (GLB); and require information brokers to submit to security audits in the event of a data breach and, importantly, to allow consumers to review what is in their individual data files.

CDT supports the concept of a nationwide data breach notification standard, so long as that standard is at least as effective as the laws already in place at the state level. All but a few states have enacted data breach notification laws, so as a practical matter companies today do notify affected individuals in the event of a data breach. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. Moreover, the Subcommittee should recognize that, from a consumer perspective, even a good federal breach notification requirement does not by itself offer much tangible progress over the status quo, since notification is already effectively the law of the land. To be of real benefit to consumers, data security legislation must include some additional protections.

The breach notification provisions in the Data Accountability and Trust Act could be improved, as discussed below, but are much better than some that have been proposed in other federal legislation in the past. The provisions requiring entities with personal data to have data security policies and procedures in place would be helpful and CDT supports them. CDT also supports the idea of requiring information brokers to allow individuals to access their files. While CDT would prefer to address access requirements in general privacy legislation, the ability of consumers to access their files and point out errors would be an important safeguard. The bill's specific language on access may need some modification to ensure its effectiveness, but these provisions could turn out to be the most significant gain for consumers in the bill.

In short, CDT supports the principal elements of the Data Accountability and Trust Act. We hope that the bill can continue to be improved and that the Subcommittee will resist suggestions that would weaken it. CDT's detailed comments and suggestions for improvements with respect to the bills specific provisions are as follows.

Breach notification trigger

The bill's trigger for breach notification, set forth in Section 3(a) and 3(f), requires notification to affected individuals and the FTC in the event of a security breach involving personal data unless it can be determined that there is "no reasonable risk of identity theft, fraud, or other unlawful conduct." CDT supports this formulation, because if a particular security breach truly poses no significant risk to the individuals whose data is involved, it should not be necessary to notify them. Indeed, such over-notification could be counterproductive.

Crucially, the bill's notification trigger permits notification to be avoided only when there is an affirmative determination that no serious risk exists. This creates strong incentives for a company suffering a breach to get to the bottom of what happened – because if it can determine there is no real risk, it will not have to notify its customers. A trigger that required notification only in the event of an affirmative finding of risk would create the opposite incentive – a company might not want to investigate too closely, because finding evidence of risk would trigger the obligation to notify. The current bill's "notify unless" formulation is the right one and should not be changed.

In the absence of any outside scrutiny of risk determinations, however, a company could have an incentive to err consistently on the side of finding little or no risk, in order to avoid the cost or embarrassment associated with notifying customers. Even if the affected individuals were eventually to become victims of identity theft, it would be difficult ever to trace those crimes back to the specific breach, since nobody other than the company and the identity thieves would be aware that the breach even occurred. In short, with nobody in a position to question dubious risk assessments, there could be a temptation to under-notify.

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

CDT therefore recommends modifying the notification trigger so that breaches judged to be non-risky still require a submission of a brief written explanation to a regulatory body such as the FTC.

Requirement for security policies and procedures

Because notice only kicks in after a breach has occurred, CDT supports the provisions of Section 2(a) requiring entities that electronically store personal information to implement security safeguards similar to those contained in FTC rules under the Gramm-Leach-Bliley Act (GLB). CDT believes, however, that the provisions of Section 2(a) should not be limited to "personal information" as that term in defined in the bill.

The bill's current definition of "personal information" is quite narrow, probably because it was drafted with breach notification in mind. For purposes of breach notification, it makes sense to use a relatively narrow definition, to avoid over-notification. But the security practices and procedures required under Section 2(a) should apply broadly to whatever information a company holds about individuals. Making security policies apply to a broader range of personal information is consistent with the FTC's implementation of the security safeguards requirements in GLB: The FTC requires safeguards for essentially "any record containing nonpublic personal information . . . about a customer. (See 16 CFR 314.2 and 313(n)-(o)).

Of course, where data is relatively non-sensitive, companies should not be required to implement excessive security processes; security safeguards should be appropriate to the data's sensitivity. The FTC's GLB rules say this explicitly, and CDT would recommend adding data sensitivity to the list of factors for consideration enumerated under Section 2(a)(1) of the bill.

In addition, CDT would suggest modifying Section 2(a) to include a de minimis exception for persons that own or possess data in connection with purely personal, family, or noncommercial activities. Arguably, if an individual uses his or her computer for online shopping and also keeps personal data on it concerning, say, his or her elderly parents, the person could qualify as a person engaged in interstate commerce who

possesses personal data, and thus would be covered under this part of the bill. Given the small quantity of data such a person has, however, it would make little sense to require a formal written security plan that would satisfy the requirements of Section 2(a)(2).

Consumer access to information broker data

When information brokers collect, maintain, and sell personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy and misuse. For example, if an innocent person finds his or her transactions are wrongly getting flagged as posing fraud risks, he or she could try to investigate and challenge the mistaken data that is causing the problem. An access and correction regime is well established under the Fair Credit Reporting Act (FCRA). CDT strongly supports the effort in Section 2(c)(3) of the Data Accountability and Trust Act to establish similar consumer access rights with respect to companies that aggregate and sell personal data.

Certain details of the current bill language, however, could undermine the provision's effectiveness. First, as discussed above with respect to Section 2(a), the scope of Section 2(c) is sharply limited by its reliance on the term "personal information." Given the bill's narrow definition of that term, the access requirements would apply only where the information broker has such details as a Social Security Number or a financial account number plus password. This narrow conception of personal information may be appropriate for breach notification purposes, but consumer access should not be so limited.

Where access rights apply, Section 2(a) does extend them beyond "personal information" to "any other information . . . that specifically identifies such individual." But the meaning of this phrase is unclear. Taken literally, the language could be read to cover only information that, by itself, would enable somebody to identify the individual. Lots of information that would be important for access purposes would not fall into that category. For example, suppose my information broker file says (wrongly) that I was convicted of a misdemeanor in 2002. This information alone would not allow anyone to identify me – but it is precisely the type of information to which consumer access is important. CDT believes the right of access should extend generally to information that is linked specifically to an identified individual and that the information broker makes available to third parties in the ordinary course of business.

CDT also notes that Section 2(c)(3)(B)(i) and (ii) refer to personal information that the information broker "maintains." Some companies compile information from various databases upon request, however, so it could be argued that they do not "maintain" a full set of information about an individual. The policy behind Section 2(c)(3), however, should be that a consumer can demand to see the data an information broker would provide in the ordinary course of business to a third party who asked for data about that consumer. One way to clarify this would be to track the language from Section 3(c)(A), which uses "collects, assembles, or maintains" instead of just "maintains."

Enforcement provisions

CDT generally supports the bill's enforcement regime. In particular, the bill wisely allows for enforcement by state Attorneys General as well as the FTC.

CDT would caution against, however, the affirmative defense contained in section 4(c) for violations involving data that is available from public records sources. There is a great deal of information that is practically obscure (i.e., publicly available in theory but difficult to access in practice) – because, for example, it exists only in dusty paper files in the basement of a small county courthouse. When companies gather this data and compile it in convenient electronic form, they effectively transform scattered bits of difficult-to-access information into highly usable, searchable, large-scale databases. If those databases later are subject to security breaches, individuals are put at risk – much greater risk than if the information had remained in scattered public records. Therefore, CDT believes that companies compiling personal data from public records should have some responsibilities to be good stewards of that data, and to notify individuals in the event of a security breach. There mere fact that an identity thief in theory could have obtained a person's data from another source would be of little comfort to a victim in a scenario where the thief took advantage of conveniently compiled electronic data and the holder of that data failed to provide notice of the breach.

Preemption

Given the large number of state data breach notification laws, preemption is a serious matter. Nonetheless, CDT believes that a federal data breach notification regime should preempt state breach notification requirements, so long as the federal regime is sufficiently robust. Having multiple and inconsistent rules on when and how to notify would be confusing and burdensome. CDT therefore believes the preemption set forth in Section 6(a)(2) is appropriate.

CDT has reservations, however, about preempting state data security laws covering topics other than notification, as Section 6(a)(1) would do. The information security provisions of the Gramm-Leach-Bliley Act (GLB) preempted inconsistent state laws, but otherwise allowed for state-level experimentation on the difficult question of how to ensure sufficient attention and precautions with respect to data security. CDT would recommend following the model set forth in Section 507 of GLB. Failing that, Congress at a minimum should be sure to preserve the language in 6(a)(1) limiting preemption to provisions that are "similar to any of those required under section 2." This language should preserve a state's ability to come up with an idea that is truly a fresh approach. California's breach notification law, the first in the nation, was a classic example of this. Had GLB broadly preempted state data security laws, it would not have been possible. Preemption should leave room for experimentation at the state level, because data security is likely to be an ongoing problem and nobody should pretend to have all the answers today.

If the bill moves forward with a higher level of preemption than GLB, Congress should keep in mind that the price for strong preemption must be strong substantive protections. If the bill were to be weakened as it moves through the legislative process, preemption would need to be reduced as well.

The Informed P2P User Act, H.R. 1319

Peer-to-peer (P2P) file sharing software is fundamentally a consumer-friendly and empowering technology. Millions of people use it today to share text, software, image, audio, and video files stored on their computers. It has opened new ways for people to

communicate with minimal central coordination and to spread storage and bandwidth costs across a broad user base. It has been a major driver of innovation in the software industry. Unfortunately, it also frequently is used to engage in copyright infringement. Of greatest direct relevance to H.R. 1319, file sharing software can raise privacy concerns, because there is evidence that some users of file sharing software have inadvertently shared sensitive documents like tax returns or electronic check registers.

CDT strongly agrees with the authors of H.R. 1319 that file sharing software should clearly disclose to users whether and how files will be made available for sharing with third parties. Inadvertent sharing of information like financial records, personal files, or correspondence is a serious matter.

It is difficult to measure how common it is today for consumers to share files accidentally. There is reason to believe some progress has been made; in the years since CDT testified on this issue in 2003, the Federal Trade Commission has engaged with major P2P companies to improve their disclosures regarding the risk of inadvertent file sharing. It is undeniable, however, that major file sharing networks have enormous user bases which are likely to include novice users with limited understanding of how the systems work. Distributors of file sharing software therefore have a serious responsibility to make sure that consumers are appropriately informed and that the software is designed to promote safe behavior and avoid confusion regarding the sharing of users' files. They have not always lived up to that responsibility.

CDT also strongly agrees that users should be able to uninstall or disable file sharing software at their own discretion. Indeed, this principle is not limited to file sharing software. The FTC in multiple spyware-related cases has effectively established that it is an unfair practice for downloadable software to prevent consumers from uninstalling it later.

At a minimum, then, the principles embodied in H.R. 1319 reflect basic and fair practices that every developer of file sharing software should follow.

Enacting specific legislation in this area is a more difficult question, for several reasons.

The first challenge relates to scope. It would be hard to limit the reach of this kind of bill to what is commonly understood as P2P file sharing software, as we believe the authors intend. That is because the main thing file sharing software does – namely, enabling the exchange of data files between Internet-connected computers – is common to many kinds of software. Indeed, CDT believes that the definition of "peer-to-peer file sharing program" in H.R. 1319 would apply to many other types of software, including Web browsers, Web servers, anti-malware software, and perhaps even operating systems. If legislation ends up sweeping in many kinds of software, there are likely to be a wider range of issues and complications to consider, as the bill's requirements might not prove appropriate in all contexts.

There also are challenges related to implementation and effectiveness. Some file sharing programs may prove difficult to regulate effectively, either because their authors and distributors are located overseas, or because they are open source programs developed on a decentralized basis and hence lack any corporate entity that could take responsibility for compliance. In addition, it is possible that a major proportion of today's inadvertent disclosure risk stems from older versions of software – with poor user interfaces or inappropriately configured default settings – that still reside on users'

computers. A bill enacted now may have limited ability to address this legacy software problem.

Finally, CDT generally believes Congress should not go down the path of imposing granular design requirements for specific technologies. Software development in particular is a highly innovative field in part because of its largely unregulated environment, enabling individual programmers and small start-ups to focus on drafting code rather than navigating regulatory requirements. Even for more established software companies, specific design requirements are likely to prove burdensome and inappropriate in individual instances. For example, H.R. 1319 requires disclosure and consent at the time of installation. This may be appropriate for most downloadable file sharing software, but what about software that comes pre-installed on a computer? A law that mandates the specific timing or nature of disclosures may prove unworkable with some products or in some technology environments. Moreover, personal data can be mistakenly disclosed in any number of ways, but legislation targeting P2P file sharing picks out a particular technology for regulation. That is why, as discussed above, CDT would prefer to address data privacy issues in the context of general privacy legislation.

CDT is not convinced there are fully satisfactory solutions to the challenges facing efforts to legislate on this topic. One way to try to reduce some of the concerns would be to avoid imposing granular mandates and instead simply require conspicuous disclosure and informed consent regarding file sharing functions before those functions are activated. If Congress believes greater detail is needed, it could direct the FTC to conduct a study or even a rulemaking on the matter. Rules adopted by the FTC would likely be better tailored to specific contexts and special cases than requirements established in statute.

If the Subcommittee decides to proceed with the current legislation, however, CDT would recommend the following specific changes to H.R. 1319.

Narrow the definition of software to which the bill applies.

As discussed above, CDT believes the bill's definition of "peer-to-peer file sharing program" in Section 4(2) would include such software as Web browsers, Web servers, anti-malware software, and probably many others. CDT also believes that the term "peer-to-peer" does not make a useful contribution to defining the bill's reach; the key question from a consumer standpoint is whether software could permit the unintended transmission of personal files to unknown parties, not whether the technical architecture could fairly be described as "peer-to-peer." CDT would suggest using the term "file sharing software" and defining it to include software that features all of the following four elements:

- The software is intended for and marketed to individual consumers.
- The software allows files stored on a user's local computer, including files actively and intentionally created by the user, to be designated as available for sharing with remote computers upon request by remote users.
- At the request of remote computers, and without requiring any further interaction, input, or authorization with or from the local user, the software will transmit to the remote computer (i) information identifying files that have been designated for sharing; and (ii) copies of such files.

- The remote computers capable of receiving such information and files need not have been individually selected or designated as intended recipients by the local user.

Significantly, this definition arguably would still include Web servers. Operation of Web servers by individual consumers is relatively uncommon, however, and Web servers aimed at the enterprise market would be excluded by the first element of the definition above.

Clarify the scope of parties to whom the bill applies.

Section 2(a) imposes requirements on persons that "cause or induce" a computer user to make files available through a file sharing program. These terms are broad and vague enough to leave significant questions about when and whether various Internet intermediaries might be covered by the bill. This creates a risk that parties who are not in any way the creators of software, like companies hosting public software distribution hubs or performing transmission or linking functions, could be held responsible for software that fails to operate as the bill requires. CDT believes that this would be dangerous, and suggests that any bill on this subject should focus narrowly on entities that actually produce software. In addition, as noted above, there are challenges in applying this legislative framework to open source software. CDT would suggest clarifying that Section 2 applies specifically to persons that develop or produce file sharing software intended for large scale or mass market distribution. The reference to "mass market" or some similar term would be important to include, because otherwise the bill could apply to individual hobbyists and tinkerers who are not in any way writing software for the general consumer marketplace.

Clarify the disclosure obligations under Section 2(a)(2).

As discussed above, CDT would advise making the bill's obligations more general and less prescriptive with regard to timing. With regard to the substance of the disclosure obligations, CDT notes that the requirement in Section 2(a)(2)(A) to disclose "which files are to be made available" is not entirely clear. For example, would it require specific notification of individual files in a user's "shared" folder at the time of initial activation, or would informing the user about the existence of the "shared" folder be sufficient? In addition, the language on its face does not appear to require any explanation of how files may be added or removed from the "share" folder in the future. CDT would suggest modifying Section 2(a)(2)(A) and (B) to ensure user disclosure and consent regarding (i) how the user can determine which files are currently designated for sharing; and (ii) what the process is for both adding and removing files from the designated sharing list.

Clarify and narrow the software removal provision.

Section 2(b)(2) applies to any person that caused or induced the installation of certain software. As discussed above with respect to Section 2(a), CDT believes that those terms are open ended and that it would be better to make the provision apply to those who develop file sharing software intended for commercial scale distribution. CDT also believes that the bill should not mandate the affirmative provision of a removal tool, as Section 2(b)(2) arguably does. Allowing removal using the operating system's regular removal function should be sufficient, and CDT recommends modifying the bill to make this clear. For example, the bill could require reasonable and effective means for

consumers to uninstall the software, either through the computer's operating system or other uninstall tool or instructions that can be readily located.

In addition, Sections 2(b)(1) and (2) refer to blocking or removal of a file sharing program "or function thereof." CDT does not believe that legislation should mandate that software allow users to block or remove individual software functions on an a la carte basis. To the extent that this language could be interpreted to impose such a requirement, it would raise complicated technical and policy questions. CDT recommends simply focusing on ensuring the ability to block or remove entire programs.

Conclusion

CDT welcomes the Subcommittee's leadership on data privacy and security issues facing consumers and on the specific bills examined in this hearing today. In particular, CDT would urge the Subcommittee to make general baseline privacy legislation a core part of its agenda on these issues. We stand ready to work with the members of the Subcommittee to craft practical policies to address the privacy challenges that arise in the rapidly changing technological environment. Thank you again for the opportunity to testify.

CENTER FOR DEMOCRACY TECHNOLOGY

FOR MORE INFORMATION

Please contact: David Sohn, (202) 637-9800, dsohn@cdt.org

Mr. RUSH. The chair thanks the gentleman. The chair recognizes now for 5 minutes of opening statement Mr. Holleyman.

STATEMENT OF ROBERT W. HOLLEYMAN II

Mr. HOLLEYMAN. Mr. Chairman, Ranking Member Radanovich, other members of this subcommittee, I want to thank you for the opportunity to testify today. The Business Software Alliance represents the leading developers of software and hardware. Of the software that is sold around the world, roughly 90 percent of that is from companies who are U.S.-based companies and our members believe strongly that the type of inquiry that this committee is engaged in today is important not only to ensure that our customers are using software properly but also to ensure that the promise of electronic commerce and equally important the promise for the type of sensitive data that the government will hold and does hold that we could have greater confidence because that will add enormous efficiencies to our system.

As we look at the issue of breaches, the data is astounding in terms of the problems that we have seen. I won't repeat all of the information that has been so widely covered in the press and by the subcommittee except that I will note that the trend is that data breaches are growing. In 2008, it is estimated that there was a 47 percent increase in data breaches over the prior year, and the average cost of each breach is growing, and for the ninth year in a row, identity theft has topped the list of FTC consumer complaints, about 26 percent of all their complaints, and according to the Privacy Rights Clearinghouse, a staggering 270 million records containing sensitive personal information have been affected since 2005. And certainly we have heard on this panel today, we have heard in your opening statements about Heartland Payment Systems, the single largest fraud-related data loss ever in the United States. Estimates of over $100 million individual credit and debit card accounts were compromised and the consequences of that have been enormous.

And finally, to the point that I made about the importance of government data, nearly 20 percent of all data breaches involve government, federal, State and local governments, and as we move to the promise of governments holding even more sensitive data regarding our health records as people live longer, as our population grows, as we build the kind of openness and confidence in government, we have to ensure that that important nexus is also protected.

With that, Mr. Chairman, I would like to comment on your pending bill. We believe that this bill, Mr. Rush, makes significant contributions to restoring and building a goal of consumer citizen trust. We support its effort to establish a uniform national standard and provide the preemption of State laws. We also believe that it is important to recognize that it would prevent excessive notification. We do need notification but not all breaches are equal, and part of what we need both in business but part of what consumers need is to ensure that when the notification occurs, it is the result of something that is meaningful. Third, we support exempting from notification data that has been rendered unusable, unreadable and indecipherable. We would recommend that the limitation in the bill

that refers to encryption be broader so that we are looking at what the test is, and really this creates market-based incentives that supplement the regulatory authority that is given. It is that combination that will ensure that more holders of data ensure that even if there is a breach, that the party that has carried out the breach or the unlawful entity can't do anything with that data, and that is an important safeguard. Fourth, we believe that your bill takes an appropriate risk-based approach to securing data and we support the grant of authority and would recommend that it be limited to the FTC and State attorneys general rather than extending a private right of actions.

A couple of comments about H.R. 1319. We welcome this effort by Ms. Bono Mack and other members of the subcommittee to address this issue. Consumer privacy can be and is being compromised because of certain peer-to-peer file-sharing applications. We also appreciate this subcommittee's willingness, the committee's willingness to look at the current breadth of this bill to identify where it could be appropriately limited. We do believe that there are two goals in this. One is to protect consumer security and promote trust and the second is to ensure that technological innovation continues to proceed. It is this balance that must be struck and it must be struck carefully. We are all concerned that the bill, if it is in its current form, could pull in some of the very legitimate applications and uses of peer-to-peer technology that are important for every consumer, important for legitimate companies. As it seeks to look at some of the bad actors or some of the peer-to-peer software that we widely know as an anti-piracy organization that have led to the widespread theft of software, music, movies and other content, we also know that the bill in its current form could sweep in any Internet-aware features of software such as automatic updates for anti-virus software such as the crash analysis feature of operating systems or the web browsers on our computers. We know that that is not the intent of this bill but as written it could reach that breadth, and so we would urge the committee to recognize that while some effort should be made, it is important to enhance security. We also want to ensure that the technological progress and growth proceeds and that will benefit all users of legitimate software.

So on behalf of BSA, thank you for this opportunity and look forward to your questions.

[The prepared statement of Mr. Holleyman follows:]

Testimony of Robert Holleyman
President and CEO
Business Software Alliance

Before the Subcommittee on Commerce, Trade and Consumer Protection
House Committee on Energy and Commerce

Legislative Hearing on
H.R. 2221, the "Data Accountability and Protection Act" and
H.R. 1319, the "Informed P2P User Act"

May 5, 2009

Good afternoon. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance.[1] BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world. We appreciate the opportunity to testify today on issues that are important to our member companies.

BSA commends you, Mr. Chairman, and Ranking Member Radanovich, for bringing a focus on data security and privacy in the digital age. This is a matter of great concern for BSA member companies that engage in electronic commerce and provide much of the infrastructure to make e-commerce possible. Unauthorized disclosures of personal information erode public confidence in the online world. Electronic commerce cannot reach its full potential to contribute to global economic growth without the trust of consumers and businesses. BSA believes that legislation, like the two bills under consideration today, are important components in strengthening trust in the online environment.

I would like to address both of the important bills now before this Subcommittee: H.R. 2221, the "Data Accountability and Trust Act," and H.R. 1319, the "Informed P2P User Act." We support the objective of improving security and trust on-line. HR 2221 would make a substantial contribution to this goal and we support the purpose of the bill. H.R. 1319 focuses on one specific aspect of security issues: the threat posed by certain peer-to-peer file sharing programs. It is our sense that the definition in the bill would cover both legitimate multipurpose computer programs as well as those programs that are designed and distributed to enable illicit file sharing and have posed risks of inadvertent file sharing. Thus, we have serious reservations about the bill as drafted. We fear that it

[1] The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cisco Systems, CNC Software/Mastercam, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, and The MathWorks.

would have substantial unintended consequences for legitimate multipurpose products such as the ones BSA members develop and distribute.

H.R. 2221 – The Data Accountability and Trust Act

Consumers' trust in the security and confidentiality of their personal data is eroding. Over the past several years, the number of significant database security breaches has increased dramatically. The stakes are high and getting higher all the time.

- In January 2009, the Identity Theft Resource Center (ITRC) reported that the number of data breaches in 2008 increased 47% compared with 2007. A recently released Ponemon study shows that the average cost of a data breach grew to $202 per record compromised in 2008, up from $197 per record in 2007. And the average security incident cost individual companies $6.6 million per breach in 2008, up from $6.43 million in 2007 and $4.7 million in 2006.
- For the ninth year in a row, identity theft tops the FTC list of U.S. consumer complaints. Of 1,223,370 complaints received in 2008, 313,982 – or 26 percent – were related to identity theft.
- According to the Better Business Bureau identity theft affects an estimated 10 million U.S. victims per year.
- According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 275 million records containing sensitive personal information since 2005.
- Earlier this year, Heartland Payment Systems, Inc. experienced what has been described as the single largest fraud-related data loss ever in United States history. Estimates now are that over 100,000,000 individual credit and debit card accounts were compromised. Since then, customers of more than 600 banks around the country have been victims of debit card fraud, with thieves using data stolen during the Heartland breach.
- Federal, state and local governments are responsible for 20% of all data breaches. Government is the third most targeted sector for cyber attacks and is responsible for 20 percent of all data breaches. The infiltration in particular of federal government networks and the possible theft or exploitation of our information is one of the most critical issues confronting our nation.

BSA believes that federal legislation that promotes improved protection of personal data, as well as notification to consumers when their data has been compromised, can effectively help restore consumer's trust.

Mr. Chairman, we believe that the "Data Accountability and Trust Act" (DATA) makes significant contributions towards achieving this goal. We support in particular the following five objectives.

BSA believes that the first objective of federal data security and data breach notification legislation should be to **establish a uniform national standard and provide preemption of state laws**.

The National Conference of State Legislatures (NCSL) indicated that, as of December 2008, forty-four states, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands

had enacted data breach notification laws.[2] A number of states have also enacted laws that impose a minimum standard of care on organizations that collect and hold sensitive personal data about consumers. This patchwork of state laws has created a compliance nightmare for businesses. Importantly, it can also create confusion for consumers who receive notices from a multiplicity of sources.

Federal legislation establishing a uniform national framework would benefit businesses and consumers alike. Mr. Chairman, we congratulate you on providing the pre-emption of state laws in your bill, and suggest that the scope of preemption be clarified to cover notification to government agencies as well, since this type of notification is covered in your bill.

The second objective of federal breach notification legislation should be to **prevent excessive notification**.

Not all breaches are created equal. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Currently, most state data breach laws require notification in all instances, even when no risk results from the breach. As a result, consumers are likely to become immune to over-notification, and fail to take appropriate action when they are truly at risk. A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm.

Mr. Chairman, your bill provides a risk-based approach to breach notification. We recommend for your consideration that the threshold be slightly raised from *"reasonable risk"* to *"significant risk,"* to ensure that only genuine risk is notified.

Linked to the issue of risk-based notification is the third objective of federal breach notification legislation: **exclude data that has been rendered unusable, unreadable, or indecipherable**.

BSA believes that data security can be enhanced, without a significant and difficult-to-enforce regulatory system, simply by using a market-based incentive for the adoption of strong data security measures. This can be done through an exception to the proposed obligation to notify security breaches in cases where the data is protected, so that even if it *"gets out"* the information cannot be used.

BSA believes this can be achieved if the measure in question satisfies two conditions:

1. It must render data unusable, unreadable, or indecipherable to any party that gains unauthorized access.
2. It must also be widely accepted as an effective industry practice or an industry standard. Examples of such measures include, but are not limited to, encryption, redaction, or access controls.

Under these two conditions, the data that has been accessed cannot actually be used to defraud or inflict harm on data subjects. A breach would not pose a risk to the data subjects. Therefore, the apparent breach does not require notification.

Mr. Chairman, H.R. 2221 provides a market-based incentive for the adoption of strong data security measures. We recommend however that this incentive be made technology

[2] http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

neutral, so that innovators continue to develop new techniques and methods without feeling that legislation has favored one type of measure over another.

We are concerned that your bill may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in your bill, other methods require the sanction of an FTC rulemaking. This puts the FTC, which may not have the adequate technological or business expertise, in the difficult position of deciding what technologies are sufficiently secure to protect what types of data in what environment.

To address this concern, we would propose that you adopt an approach whereby the technology must: 1. Render the data "*unusable, unreadable, or indecipherable,*" and 2. Be "*widely accepted as an effective industry practice or an industry standard.*" Examples of such measures include, but are not limited to, encryption, redaction, or access controls. We believe this gives flexibility for businesses and innovators, but is demanding enough to provide a high degree of protection for consumers, today and tomorrow.

The fourth objective of federal data security legislation should be to **avoid imposing technology mandates and over-regulating data custody**.

Organizations must be able to deploy appropriate and cutting edge security measures and technologies to effectively protect themselves and their customers' sensitive data against current and future threats. This would not be possible if the law mandated the use of specific products or technologies. Laws and regulations should focus instead on requiring the implementation of reasonable and appropriate security measures.

We are pleased that you include in your bill a provision that bars the FTC from "*requir[ing] the deployment or use of any specific products or technologies, including any specific computer software or hardware.*"

We are also heartened that section 2 of your bill – which requires the implementation of security measures to prevent breaches from happening – is risk-based, directing data custodians to analyze and mitigate their risks through appropriate and reasonable measures.

However, we believe it would have been preferable for your bill to simply direct organizations holding consumer data to establish and implement policies and procedures regarding information security practices for the protection of that data. We are concerned that your bill's grant of authority to the FTC to enact a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The potential is high to turn data custody – an activity that is for most companies, whether large or small, only incidental to their core business – into a stifling compliance burden, with little to gain in terms of increased data security.

Finally, the fifth and last objective of federal data security and data breach legislation should be to **provide for appropriate enforcement**.

BSA supports your bill's provision granting the FTC powers of enforcement. The BJ's Wholesale Club, DSW (Designer Shoe Warehouse) and Card System cases are just a few examples of the FTC's strong track record of defending consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We also support your bill's inclusion of state Attorneys General as enforcers when the FTC has not acted.

BSA believes it is also important to prevent excessive litigation. The judicial system is not a desirable forum to determine the adequacy of data security measures. Moreover, allowing

private lawsuits as a result of the occurrence of a data breach would create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits. Therefore, we strongly urge you to include a provision explicitly stating that nothing in the bill is a basis for a private right of action for damages.

H.R. 1319 – The Informed P2P User Act

We applaud Representative Bono Mack and the other cosponsors of H.R. 1319 for focusing attention on the serious harm to consumers that may be caused by some peer-to-peer file sharing applications.

HR 1319's aim is to promote consumer trust and prevent intrusions into sensitive files that reside on a user's computer. It proposes to accomplish this goal by imposing certain notification requirements on "peer-to-peer file sharing programs." We believe that the bill is intended to address a specific type of peer-to-peer software: programs, like Limewire, Bearshare and BitTorrent, that are intended for illicit purposes, such as unauthorized sharing of copyrighted works such as software, music or movies. Often this nefarious use of peer-to-peer technologies also exposes users to identity theft and other intrusions of their privacy.

However, we are concerned that the language of the bill covers much more than this narrow category of software. Many multipurpose products would be subject to regulation under this bill.

The problem that the bill's sponsors have identified is real. The persons who build, and maintain illicit peer-to-peer services make their money by selling advertising and installing spyware and other security threats as part of their software. A key feature of many of these services is that through default functions they establish shared folders from which others can take works. These folders are hard to find on the user's system once they have been installed. Moreover many file-sharing programs are designed to continue to run in the background, even when a user has taken steps to shut it down. Merely closing the window in which it appears, like with other programs, does not stop the program. Finally, disabling file-sharing functions is deliberately hard and complex. In some instances it takes as many as ten or more steps, involving the "advanced" settings on a computer, which is meant to make the average user very hesitant about taking those steps.

But peer-to-peer software covers a broad range of products that enable users in different locations to share files. For example, it enables engineers in Chicago and Palm Springs to work collaboratively on the drawings for a new bridge or airport. It enables colleagues at different locations to collaborate on a presentation or report. Internet telephony is another important and beneficial application of peer-to-peer technology. These software solutions do not pose the kind of risks to users' privacy that motivated this bill. So peer-to-peer software as such is neither good nor bad. Much depends on how the specific tool is designed and used.

Even more importantly, the definition of "peer-to-peer file sharing program" in the bill is not limited to peer-to-peer technology. It covers any software that exchanges information with other computers, including servers and websites. As the bill is now drafted, we believe that it would cover any software that is "Internet aware" – that is, capable of sending and receiving information on the Internet.

Here are some examples of software that appear to be included in the bill's definition of "peer-to-peer file sharing program":

- Operating systems and applications that are capable of determining whether updates are available, downloading the updates, and installing them automatically.
- Operating systems and applications that include a "crash analysis" feature.
- "Groupware" or collaboration tools.
- Web browsers.
- Anti-virus and anti-spyware programs that depend on up-to-date definition files.

We believe the bill in its current form could have substantial and immediate unintended consequences for consumers and developers of general-purpose software products. It could require developers to ensure that their Internet-aware products **disable** features such as automatic updates and crash analysis by default. BSA members and other software developers may well have to redesign their installation procedures to ensure that proper notices are displayed not only at the time that the software is installed, but also at the point in time when any "file-sharing" feature is activated. Under the terms of the bill, all software developers must provide a means to prevent the installation of such features and a means to uninstall them later.

This feature-by feature approach applied to the broad range of beneficial products now covered would be burdensome not only to developers, but to users as well. It would create abundant opportunities for consumer confusion and frustration when expected features are turned off by default. Moreover, leaving automatic updates off by default could result in many customers failing to receive security patches and updates, thus making their computers vulnerable to known security problems.

BSA recommends that the bill be modified to focus narrowly on the kind of software that has, in the past, been shown to create risks to consumers of unintentional exposure of personal information. These are peer-to-peer file sharing applications that are used primarily to exchange copyrighted works that belong to third parties among users of the same application. We recommend that the definition of "peer-to-peer file sharing program" be amended in the following ways:

- The definition should **include** only those programs that are used primarily to transmit or request copies of third-party copyrighted works.
- The definition should **include** only those programs that are used to transmit to, or request copies from, other computers running the same or a compatible peer-to-peer file sharing program.
- The definition should **exclude** programs or features that are used to transmit information to websites and other servers as distinguished from other personal computers on a P2P network.
- The definition should **exclude** programs that are installed onto computers by original equipment manufacturers. OEMs do not install the kinds of programs that are known risks for unintentional disclosure that have prompted this bill.
- The definition should **exclude** programs or features that transmit or request information for purposes that are internal to the functioning and maintenance of the program, such as caching information, updating the program or diagnosing problems with the software.

In addition, BSA recommends that the prohibitions in section 2 of the bill be modified in the following ways:

- The notice and consent requirement should be clarified to ensure that it is **limited to initial installation** of the software and configuration of the software that is part of the installation process.
- The provisions relating to deactivating or uninstalling individual features of a program should be clarified to ensure that **providing either a means of uninstalling or a means of deactivating a feature is sufficient**. As currently drafted the bill could be read to require both.

We believe any legislation such as HR 1319 must balance two key goals: promoting trust by protecting consumer security, and ensuring that technological innovation can continue at a pace dictated by the marketplace and the ingenuity of our engineers to common benefit of users and consumers. In finding this right balance we urge you to make sure that good technologies are not put at-risk by the need to stop bad actors. In other words, ensure that unintended consequences are identified and addressed before this bill becomes law.

* * * *

Mr. Chairman and members of the subcommittee, BSA appreciates the opportunity to provide its input on these two bills. We share the subcommittee's goals of helping to enhance data security, inform and empower consumers, and mitigate the harm from data breach. We are happy to work with you to craft the necessary changes to the bills as the legislative process moves forward.

Mr. RUSH. The chair thanks the gentleman. The Mr. Chairman, Mr. Lafferty, for 5 minutes.

STATEMENT OF MARTIN C. LAFFERTY

Mr. LAFFERTY. Chairman Rush, Ranking Member Radanovich, subcommittee members, thank you for holding this important hearing. I am Marty Lafferty, CEO of the Distributed Computing Industry Association.

Both of the bills under consideration have far-reaching consequences. Our expertise relates primarily to H.R. 1319. DCIA is a trade group focused on P2P and related technologies. Our mission is to foster commercial development of these technologies so that their benefits can be realized by all participants in the distribution chain including content rights holders and Internet service providers. We currently have 125 member companies including P2P, cloud computing, file sharing and social network software distributors, broadband operators, content providers and service and support companies. P2P has evolved greatly in the 8 years since Napster first brought the term P2P file sharing to prominence. Fully licensed ad-supported P2P, subscription P2P, paid download P2P, commercial enterprise P2P, P2P TV, hybrid P2P and live P2P streaming now deserve to be separated from the narrow subset of functionality associated with file sharing. DCIA member companies increasingly use P2P for the delivery of authorized entertainment and corporate communications content where rights holders rather than end users introduce files or live streams for online delivery. We strongly urge the committee to apply the term "file sharing" without the P2P prefix as a more accurate descriptor for the focus of H.R. 1319.

The Committee on Oversight and Government Reform held a hearing on this topic in July 2007 at which one of our member companies testified. Within weeks of that hearing, the DCIA established the Inadvertent Sharing Protection Working Group. Over several months we recruited participants among leading P2P and other tech sector companies and engaged with FTC staff to address issues associated with unintended publishing of confidential data by file sharers. This effort began by providing demonstrations for FTC staff of how current file share programs work in terms of users uploading material for distribution. It continued through a process involving private sector and regulatory participants to develop a program of voluntary best practices for file-sharing software developers to protect users against inadvertently sharing personal or sensitive data. This program was announced in July of 2008. Its summary, included in our written testimony, begins by defining terms relevant to 1319 such as recursive sharing, sensitive file types and user-originated files. It then outlines seven steps that are required to be in compliance: default settings, file-sharing controls, shared folder configurations, user error protections, sensitive file type restrictions, file sharing status communications and developer principles. The principles address feature disablement, uninstallation, new version upgrades and file-sharing settings. In August 2008, the DCIA announced that compliance monitoring would begin in December to allow developers time to integrate required elements of the ISPG program into their planned upgrades

and new releases. Compliance monitoring resulted in reports from top brands that use P2P for downloading, live streaming, open environment sharing and corporate Internet deployments and for both user-generated and professionally produced content. Specifically, seven leading P2P representative program distributors submitted detailed reports to FTC staff in February 2009. In March the DCIA prepared and submitted a summary. We also noted that software implementations of the popular BitTorrent protocol typically require users to conduct a deliberate conversion process from whatever native file format their content is in to a torrent file before it can be published, thus minimizing this risk of user error. The entire report plus data tables of individual company submissions are in our written testimony but here are highlights.

All respondents now have clearly disclosed install default settings that only permit sharing files downloaded from the network. They do not share user-generated files by default. A hundred percent also provide complete uninstallation of their file-sharing software that is simple to do and explained in plain language, for example, by using the standard add/remove program in Windows. And six out of seven, which is all where this is applicable, now offer a simple way to stop sharing any folder, subfolder or file by using easily accessed controls.

In April 2009, subcommittee staff invited the DCIA to participate in redrafting H.R. 1319. We formed a DCIA member subgroup to conduct this work. The process is underway and we are glad to coordinate that work with staff. Among our greatest concerns is that the bill as drafted would have unintended consequences. The present draft goes way beyond the specific concerns discussed here and would apply to additional functionality and technologies that have nothing to do with recursive sharing of sensitive file types. Applying these requirements to numerous products, services and companies would be burdensome and counterproductive. To the extent that legitimate consumer concerns persist in the area that the bill intends to address, we strongly believe they can best be handled by ongoing self-regulation under the oversight of the appropriate federal authority as we initiated with the ISPG.

The bill as constructed would unnecessarily burden U.S.-based technology firms with innovation freeze and constraints while being unenforceable against overseas competitors' software available to U.S. consumers. The great concern also is how it might stifle yet undeveloped new and potentially very useful and valuable software applications. On the other hand, the DCIA has committed to self-regulation through the ISPG to address the subject matter of this bill and is making substantial progress. So rather than a problematic new legal measure, we believe that formalized requirements for compliance with that process will be more effective in achieving the purpose of the bill.

We look forward to working with the subcommittee on these issues in a productive manner and will benefit all your constituents. Thank you for your continued interest in our industry.

[The prepared statement of Mr. Lafferty follows:]

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319
Testimony of Marty Lafferty
CEO, Distributed Computing Industry Association (DCIA)

May 5, 2009

Dear Chairman Rush and Ranking Member Radanovich:

Thank you for holding this important and timely hearing on issues related to H.R. 2221 "The Data Accountability and Trust Act" and H.R. 1319 "The Informed P2P User Act." We greatly appreciate your leadership and that of your colleagues serving on the Subcommittee on Commerce, Trade, and Consumer Protection. We are grateful for this opportunity to share the Distributed Computing Industry Association's (www.DCIA.info) perspective on this critical industry and consumer issue.

Introduction to P2P and File Sharing

The Distributed Computing Industry Association (DCIA) is a non-profit trade organization focused on peer-to-peer (P2P), cloud computing, file-sharing, and related distributed computing technologies.

Our mission is to foster commercial development of these technologies, which are still in their infancy relative to more mature and established Internet-based offerings – so that their benefits can be realized by all participants in the distribution chain, including content rights holders and Internet service providers (ISPs).

The DCIA conducts working groups and special projects, such as the P2P Digital Watermark Working Group (PDWG), P3P Working Group, (P3PWG), P4P Working Group (P4PWG), Consumer Disclosures Working Group (CDWG), P2P PATROL, P2P Revenue Engine (P2PRE), and, most relevant to today's hearing, the Inadvertent Sharing Protection Working Group (ISPG), which we will discuss in more detail.

The DCIA also publishes the weekly online newsletter DCINFO, maintains a searchable database tracing industry history from 2003 with more than 5,000 articles and papers, and conducts several conferences annually focusing on current issues affecting commercial advancement of the technologies we advocate.

We currently have one-hundred twenty-five (125) Member companies, including P2P, cloud computing, file-sharing, and social networking software developers and distributors, Internet service providers (ISPs), content rights holders, and service-and-support companies. An alphabetical list of our Member companies with links to their respective websites can be found on the home-page of our primary site, www.dcia.info.

Wikipedia defines a P2P computer network as using "diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather

than conventional centralized resources where a relatively low number of servers provide the core value to a service or application."

With the old server-client approach, every download required a separate session – between the machine hosting the content and each device receiving it. Especially for large rich media files and entertainment content compilations, this represented an expensive methodology and inefficient use of network resources. P2P brought a way to replicate broadcast economics, where content providers incur virtually no incremental expense – as files are transmitted from one to a thousand or literally millions of users.

With P2P, every user on the network joins in a kind of online cooperative – sharing storage, bandwidth, communication, and even viral marketing – to very efficiently distribute content.

P2P is unique because of this decentralized approach and low-to-no overhead. In essence, P2P affords rights holders minimal hosting and transport costs, plus infinitely scalable capacity, limited only by the size of the user network.

P2P industry players include BitTorrent, the most widely used protocol, now with an enterprise solution and many derivatives; eDonkey, which ceased commercial operation, but has remained popular as the open-source eMule; Bearshare, which despite the company's acquisition by iMesh has also remained popular as a standalone program; LimeWire, a widely-used open-P2P program now integrating a LimeWire Store and new Lime Engine; and Kontiki, spun-off last year by VeriSign and currently used in several major enterprise deployments, including Wells Fargo, GM, and Coca-Cola.

Examples of new and emerging P2P services are Damaka, FrostWire, GigaTribe, Grooveshark, Itiva, LittleShoot, mBit, MyBloop, Ooma, Pownce, Raketu, RedSwoosh, SlapVid, Swapper, Twango, Vudu, and Yoomba... to name a few.

2007 was the year when peer-to-peer television (P2PTV) finally arrived as a huge breakthrough for digital video, the first video-centric offering to take advantage of P2P distribution technology in cooperation with a multitude of partners. Examples include the now Flash-based client-less solution Joost; an online movie festival and customized channels on Babelgum; TV stations now in European market trials at Zattoo; an open-P2P video service, backed by Time Warner called VeohTV; a hybrid client-player, Miro; and our newest Member in this space, TVU Networks.

China has been a pioneer of P2PTV with services like PPLive, PPStream, QQlive, UUsee, Vakaka, and Xunlei – where the cost savings of P2P have brought television to millions of unserved viewers.

2008 was the year of cloud computing or peer-assisted hybrid-P2P content delivery networks. These incredibly sophisticated platforms give rights holders enormous flexibility in managing online delivery of their copyrighted works. Cost, speed, and access terms-and-conditions can each be precisely controlled. Downloads to play in real-time, downloads to play later, and live streaming can all be supported with the unprecedented advantages of P2P. Leading examples in this category are Abacast, Pando Networks, CloudShield, Octoshape, GridNetworks, Solid State, Ignite Technologies, and Velocix.

Since 2000, P2P has grown into the dominant Internet traffic generator. Velocix reported that, by 2005, P2P surpassed web traffic as a major part of the value proposition for broadband access. Due to relative file-size, video now represents 65% of P2P volume, music 11%, and software-and-games 24%.

Sandvine likewise reports that P2P currently accounts for the largest aggregate share of bandwidth utilization by category. And given the asymmetrical structure of most broadband networks, this is especially striking on the upstream side.

MultiMedia Intelligence sees P2P traffic growing by 400% in the next five years, from 1.6 to 8 petabytes per month, with licensed P2P growing at ten times that rate as authorized offerings come into their own; and new advancements, such as P4P and hybrid services, take hold.

Insight Research projects that the worldwide market for P2P and file-sharing will surpass $28 billion per year in revenue for carriers and ISPs over the next three years.

P2P-based companies generate income in a number of ways. We have traditional media business models for P2P; such as QTRAX with ad-supported music; iMesh with subscription sales; Vuze with paid downloads; and now Spotify with all three – plus P2P streaming.

P2P telephony with Skype, created 2.6 billion dollars for investors when acquired by eBay. Other examples include premium content delivery from Pando, digital rights management from BuyDRM, client filtering from Audible Magic, payment services from Clickshare and Javien, interactive advertising from Ultramercial and HIRO-Media, super-distribution patents from Digital Containers, spoofing and marketing from MediaSentry – just acquired by MediaDefender, interdiction from Friend Media and BayTSP, and P2P measurement from BigChampagne.

The DCIA believes collaboration among three groups is essential for success in the P2P marketplace: Content, with rights holders for music, movies, and games; Operations,

with P2P software developers and distributors; and Platform, with ISPs, plus service-and-support companies.

Therefore our Member companies include leading P2Ps like BitTorrent, Kontiki, Pando, and LimeWire; progressive entertainment firms like Nettwerk Music Group, ROK Entertainment, and PlayFirst games; and major platform companies like AT&T, Cisco Systems, and Verizon.

We also have many up-and-comers like Oversi, Abacast, PeerApp, ARTISTdirect, Brand Asset Digital, CUGate, Altnet, Raketu, and RightsFlow, cable and international ISPs like Comcast and Telefonica, as well as global consulting firms KPMG and FTI.

Most important for the purposes of this 2009 hearing is that we distinguish between P2P and file sharing.

P2P has evolved in the eight years since Napster first brought the term-of-art "P2P File Sharing" to prominence – and notoriety – to the point that P2P now encompasses many more technologies than file sharing, most of which do not deserve the negative connotations of copyright infringement and consumer risks that are still associated with rudimentary file-sharing functionality.

Fully licensed ad-supported P2P, subscription P2P, paid download P2P; commercial enterprise P2P, P2PTV, hybrid P2P CDNs, and live P2P streaming that are increasingly prominent as we reach the end of the first decade of this century deserve to be separated in terms of regulatory considerations from the narrow sub-set of functionality associated with file sharing per se.

DCIA Member companies increasingly use P2P technologies for the delivery of licensed entertainment and/or corporate communications content where rights-holders, rather than end-users, introduce files and/or live streams for online redistribution.

We strongly urge the subcommittee to apply the term "File Sharing" (without the P2P prefix) to its proposed legislation, as a more precise, current, and accurate descriptor.

Relevant Background

By way of introduction, we respectfully call your attention to our related letter of July 18, 2007 to the U.S. House of Representatives Committee on Oversight and Government Reform:

> We commend you for your leadership in conducting a Hearing scheduled for July 24th to explore potential privacy and security concerns associated with the use of

P2P file-sharing programs, and greatly appreciate the opportunity to comment on this important issue.

The DCIA has taken several steps to address such matters since our inception in 2003 and continues to seek further advances. We have worked closely with the Federal Trade Commission (FTC) on this and related issues. We have also provided witnesses and testimony for previous Congressional Hearings that in part addressed this subject.

We were particularly impressed with your report entitled "File-Sharing Programs and Peer-to-Peer Networks: Privacy and Security Risks." The DCIA is also familiar with the March 2007 Patent and Trademark Office (PTO) report and the more recent correspondence between the Committee and two leading US-based P2P software developers and distributors regarding consumer disclosures, default settings, recursive sharing, un-installation procedures, etc.

As we suggested to the PTO in March, please allow us to offer the Committee the DCIA's professional assistance in accelerating adoption of technological advances and related business practices to further protect P2P users against inadvertent sharing of private data.

In our view, because of both the technical complexity and relatively fast-moving innovation in this area, a federally mandated and closely monitored private sector initiative, rather than even the best intentioned legislative measure, will produce the most beneficial effect to the public and to government agencies whose sensitive and confidential information must be protected as a matter of national security.

We currently conduct several working groups tackling a number of issues, including consumer security concerns, such as the inadvertent sharing of files. These working groups can extend beyond our Membership as needed to ensure that the output of their work is widely adopted on a voluntary basis across the distributed computing industry.

The DCIA is willing to create a new working group or to charge an existing one with responding to the concerns that the PTO report has uncovered as may be more precisely delineated during your upcoming Hearing. We look forward to working with the Committee in a productive manner on these issues in a way that will significantly benefit all of your constituencies.

We will contact your offices to follow-up after the Hearing. Thank you very much for your continued interest in our developing industry.

Formation of the ISPG

Following up on the above referenced hearing, within weeks the DCIA established a new working group called the Inadvertent Sharing Protection Working Group (ISPG)

Over a period of the next several months, the DCIA recruited participants among leading P2P file-sharing companies and other representatives of the technology sector with relevant expertise and engaged with FTC staff to address issues associated with inadvertent sharing of personal and sensitive data by users of file-sharing software applications.

This process began by providing an overview and detailed demonstrations for FTC staff of how current major file-sharing software applications work in terms of users uploading files for redistribution via user networks.

It continued through an iterative process involving private sector and federal regulatory participants to develop a program for voluntary best practices for file-sharing software developers to implement to protect users against inadvertently sharing personal or sensitive data.

A document summarizing the program was completed by ISPG participants and posted on the DCIA website at www.dcia.info/activities/ispg/inadvertentsharingprotection.pdf in July 2008.

In publicly announcing the program, the DCIA expressed gratitude for the participation of industry-leading companies in a collaborative process with regulatory agency representatives that resulted in an excellent work product.

We noted that while adoption would be a voluntary decision to be made by each company on an individual basis, we were confident of wide acceptance, and would not only encourage, but also monitor compliance.

The summary document begins with a glossary defining terms specifically related to subject matter concerns, such as "recursive sharing," "sensitive file type," and "user-originated file," as well as protective measures, such as "affirmative step."

It then outlines seven steps that are required to be in compliance with the program. These include 1) default settings, 2) file-sharing controls, 3) shared-folder configurations, 4) user-error protections, 5) sensitive-file-type restrictions, 6) file-sharing status communications, and 7) developer principles.

The developer principles for file-sharing software applications address feature disablement, uninstallation, new-version upgrades, and file-sharing settings.

Finally, the document includes an eighth optional step for added consumer protection that relates to inactive states of the file-sharing application (fully disconnected from the user network and running in the background).

At the time of the program's announcement, leading file-sharing application LimeWire's CEO George Searle said, "LimeWire is committed to providing a great file-sharing product that people love to use and that provides for their personal safety. We have actively participated in key developmental aspects of this program and believe it will help protect users from the inadvertent sharing of personal or sensitive information."

Top commercial P2P software provider Kontiki's President Eric Armstrong added, "Kontiki, which offers secure peer-assisted content delivery technology, supports the provisions of this program. We believe this DCIA initiative will be valuable to users and creators of software for redistribution of user-originated content."

Major P2P content delivery solutions provider Pando Networks' CEO Robert Levitan concluded, "At Pando Networks, we believe users should always be in control of any P2P application on their desktop. We support this effort that will benefit the entire industry by advancing consumer safety in the large and growing P2P marketplace."

ISPG Program

Following is the verbatim ISPG Program of Voluntary Best Practices for [P2P] File-Sharing Software Developers to Implement to Protect Users against Inadvertently Sharing Personal or Sensitive Data. (Note that brackets around uses of the term P2P indicate our recommended deletions).

DEFINITIONS:

(1) "Affirmative Step" means an action that requires the user to select a non-default choice presented by the application's user interface.

(2) "Recursive Sharing" means the automatic sharing of subfolders of any parent folder designated for sharing.

(3) "Sensitive File Types" means file types which are known to be associated with personal or sensitive data, for example, those with file extensions such as .doc or .xls in Windows Office, .pdf in Adobe, or the equivalent in other software programs.

(4) "Sensitive Folders" are those often used to store personal or sensitive data, for example, the "My Documents" folder in Windows or the equivalent on another operating system.

(5) "Shared Folder" means a folder that is designated, at the point of installation, for users to store files that other users of the respective file-sharing network can download from the user's computer.

(6) "User-Originated Files" means any files stored on a user's computer prior to installation of the file-sharing application and any files subsequently stored on a user's computer that a user has not downloaded from the respective file-sharing network.

REQUIRED – TO BE CONSIDERED IN COMPLIANCE

(1) An application's default settings for file sharing at the point of software installation: may permit redistribution of files the user subsequently downloads from the respective [P2P] network if this behavior has been disclosed to users clearly and conspicuously in advance; and shall not share User-Originated Files.

> (A) In order for User-Originated Files or pre-existing folders to be shared, the user must take Affirmative Steps subsequent to the point of installation. These steps shall include clear, timely, and conspicuous plain-language warnings about the risks of inadvertent sharing of personal or sensitive data.
>
> (B) There shall be a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality shall be clear, timely, and conspicuous.

(2) There shall be a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file shall be clear, timely, and conspicuous.

(3) The Shared Folder shall not contain any User-Originated Files at the point of initial installation of the [P2P] software. The user must place User-Originated Files and pre-existing folders in the Shared Folder individually. The user must take Affirmative Steps to share additional folders.

(A) Recursive Sharing shall be disabled by default and may be enabled only after the user takes Affirmative Steps.

(B) The user must have clear and precise options to control Recursive Sharing if a user enables it. All subfolders that are going to be shared should be conspicuously noted, for the user to review and confirm.

(4) For User-Originated Files that are made available for distribution by taking the Affirmative Steps outlined above, additional protection shall be provided against known instances of potentially-harmful user error.

(A) To share the entire contents of a Sensitive Folder, the user must take Affirmative Steps and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files.

(B) Any attempt to share a complete drive (e.g., the "C" or "D" drive, a network drive, or external drive) or a user-specific system folder (e.g., a "Documents and Settings" folder in Windows) must be prevented.

(5) When the default setting for file sharing has been changed by the user to permit distribution of User-Originated Files in accordance with the foregoing requirements, files with Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

(A) The user must take Affirmative Steps to change the default settings to enable sharing of files with Sensitive File Types.

(B) There shall be a simple way for the user to stop sharing files with Sensitive File Types by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop sharing Sensitive File Types shall be clear, timely and conspicuous.

(6) The user shall be presented with a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. The user shall be shown a prominent warning when a large number of files or folders are shared.

(A) If a large number of files is shared (e.g., greater than 500), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared files.

(B) If a large number of subfolders is shared (e.g., greater than 4), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared folders.

(7) Developers shall also implement the following principles:

(A) Disabling of file-sharing features, including but not limited to those outlined above, shall be simple to do and explained in plain language, with consistent terminology (i.e., terms such as "Default Setting," "File Extension," "Recursive Sharing," and "Shared Folder" shall always have the same meaning whenever used in communications from the P2P file sharing software provider).

(B) Complete uninstallation of the [P2P] file-sharing software also shall be simple to do and explained in plain language (e.g., by using the standard "Add/Remove Program" functionality on Windows or its equivalent on other operating systems).

(C) [P2P] file-sharing software developers shall make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software, which contain the features outlined above, as soon as they are commercially available (i.e., after successfully completing beta testing). Previously-chosen sharing selections should be reconfirmed by the user upon installation of the new version of the software. In the reconfirmation process, users shall be warned, consistent with the foregoing requirements, before Sensitive Folders are shared and users must take Affirmative Steps to continue sharing Sensitive Folders and their subfolders. By default, Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

(D) When the user subsequently chooses to upgrade to a different or newer version of the [P2P] file-sharing software, or to reinstall the same version of the software, either (a) if the software upgrade or reinstallation does not materially affect other user-controllable settings (including aspects of the user-interface and share settings addressed in this document), then it shall not change the file-sharing settings previously chosen by the user; or (b) if the software upgrade or reinstallation does materially change or require user-controllable settings to be reset, then it shall require file sharing settings to be reset by the user as described above. If the upgrade or reinstallation uses the previously set file-sharing settings, the application shall warn users that those settings will be used, remind the user that changes to those settings can be made in the designated area in the software, and warn users if Sensitive Folders or Sensitive File Types are being shared.

OPTIONAL – FOR ADDED CONSUMER PROTECTION

(8) When the user chooses no longer to use the [P2P] file-sharing software in a given online session, the user shall be presented with a choice of either i.) turning the software completely off (i.e., fully disconnecting from the [P2P] network); or ii.) having the software continue to run in the background (i.e., still contributing resources to the [P2P] network to help facilitate content redistribution).

> (A) There shall be a simple way for the user to fully disconnect from the [P2P] network by using controls provided in a designated area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to fully disconnect from the [P2P] network shall be clear, timely, and conspicuous.
>
> (B) When the [P2P] file-sharing software is in use and running in the background, the application shall clearly alert the user that the software is still running (e.g., in the "System Tray" on Windows or its equivalent on another operating system).

ISPG Compliance

In August 2008, the DCIA announced that compliance monitoring would begin in December 2008 to allow software developers reasonable time to introduce required elements of the new ISPG program into their upcoming upgrades and new releases.

Monitoring began as scheduled and resulted in the completion of compliance report submissions from top brands that use P2P for downloading, live streaming, open-environment sharing, and corporate intranet deployments, and to distribute both user-generated and professionally produced content.

Specifically, seven (7) leading P2P program developers and distributors submitted detailed reports in February 2009, which were provided to FTC staff.

In March 2009, the DCIA prepared and submitted a summary report noting that there had been very significant progress on this important issue; and that providing users of file-sharing programs with as safe and valuable an experience as possible remained a top industry priority.

We also noted that, in addition, DCIA Member companies increasingly use P2P technologies for the delivery of licensed entertainment and/or corporate communications content where rights-holders, rather than end-users, introduce files and/or live streams for online redistribution.

Following is a summary analysis of the ISPG compliance report submissions followed by the data tables upon which this analysis was based.

It should be noted, too, that software implementations of the popular BitTorrent protocol typically require users to conduct a deliberate conversion process from whatever native file-format their content is in to a torrent file before it can be shared, thus minimizing this risk of user error.

All respondents now have default settings for file sharing at the point of software installation that only permit redistribution of files the user subsequently downloads from the respective user network, which is disclosed to users clearly and conspicuously in advance. They do not share user-originated files by default. Some, like LimeWire, by default do not even permit this sort of redistribution where the download was of a document file type.

100% of respondents also provide complete uninstallation of the P2P or file-sharing software that is simple to do and explained in plain language (e.g., by using the standard "Add/Remove Program" functionality on Windows or its equivalent on other operating systems).

100% of respondents for whom this principle is applicable now offer a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file are clear, timely, and conspicuous.

A similar number of respondents make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software that contain these safety features. And during such upgrades, great care is taken regarding both the file-sharing settings themselves and communications regarding them.

Five times more respondents comply than do not with the user being presented a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. Users are also shown prominent warnings when a large number of files or folders are shared.

Where this principle is applicable, which was for the majority of respondents, four times more respondents than not offer additional protection against known instances of potentially-harmful user error.

These include requiring that a user must take affirmative steps to share the entire contents of a sensitive folder, and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files; and that any attempt to share a complete drive (e.g., the "C" or "D" drive, a network drive, or external drive) or a user-specific system folder (e.g., a "Documents and Settings" folder in Windows) must be prevented.

Furthermore, in each of the 57% of cases where applicable, in order for user-originated files or pre-existing folders to be shared, the user must take affirmative steps subsequent to the point of installation. These steps include clear, timely, and conspicuous plain-language warnings about the risks of inadvertent sharing of personal or sensitive data.

A similar number provide a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality are clear, timely, and conspicuous.

For those respondents whose services include a shared folder, none now contain any user-originated files at the point of initial installation of the software. The user must place user-originated files and pre-existing folders in the shared folder individually. The user must take affirmative steps to share additional folders.

Recursive sharing has been disabled by default and may be enabled only after the user takes affirmative steps in all but 14% of applicable instances. For the non-complying applications, this is expected to be addressed in upcoming new releases. The same ratios apply to users having clear and precise options to control recursive sharing if a user enables it. All subfolders that are going to be shared shall be conspicuously noted for the user to review and confirm.

At this point, an even number of respondents, where the following principle applies, comply with not permitting sensitive files to be distributed by the user network when the default setting for file sharing has been changed by the user to permit distribution of user-originated files in accordance with the foregoing requirements.

Results were similar for providing a simple way for the user to stop sharing files with sensitive file types by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface, and with instructions on how to stop sharing sensitive file types that are clear, timely and conspicuous.

Fewer currently require users to take affirmative steps to change the default settings to enable sharing of files with sensitive file types. We will continue to closely examine this critical area.

Data Tables

(1) An application's default settings for file sharing at the point of software installation: may permit redistribution of files the user subsequently downloads from the respective [P2P] network if this behavior has been disclosed to users clearly and conspicuously in advance; and shall not share User-Originated Files.

Percentage of Respondents Complying: 100%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 0%

(A) In order for User-Originated Files or pre-existing folders to be shared, the user must take Affirmative Steps subsequent to the point of installation. These steps shall include clear, timely, and conspicuous plain-language warnings about the risks of inadvertent sharing of personal or sensitive data.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%

(B) There shall be a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality shall be clear, timely, and conspicuous.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%

(2) There shall be a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file shall be clear, timely, and conspicuous.

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%

(3) The Shared Folder shall not contain any User-Originated Files at the point of initial installation of the [P2P] software. The user must place User-Originated Files and pre-existing folders in the Shared Folder individually. The user must take Affirmative Steps to share additional folders.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%

(A) Recursive Sharing shall be disabled by default and may be enabled only after the user takes Affirmative Steps.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 57%

(B) The user must have clear and precise options to control Recursive Sharing if a user enables it. All subfolders that are going to be shared should be conspicuously noted, for the user to review and confirm.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 57%

(4) For User-Originated Files that are made available for distribution by taking the Affirmative Steps outlined above, additional protection shall be provided against known instances of potentially-harmful user error.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 29%

(A) To share the entire contents of a Sensitive Folder, the user must take Affirmative Steps and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files.

Percentage of Respondents Complying: 43%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 43%

(B) Any attempt to share a complete drive (e.g., the "C" or "D" drive, a network drive, or external drive) or a user-specific system folder (e.g., a "Documents and Settings" folder in Windows) must be prevented.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 29%

(5) When the default setting for file sharing has been changed by the user to permit distribution of User-Originated Files in accordance with the foregoing requirements, files with Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 43%

(A) The user must take Affirmative Steps to change the default settings to enable sharing of files with Sensitive File Types.

Percentage of Respondents Complying: 14%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 57%

(B) There shall be a simple way for the user to stop sharing files with Sensitive File Types by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop sharing Sensitive File Types shall be clear, timely and conspicuous.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 43%

(6) The user shall be presented with a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. The user shall be shown a prominent warning when a large number of files or folders are shared.

Percentage of Respondents Complying: 71%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 14%

(A) If a large number of files is shared (e.g., greater than 500), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared files.

Percentage of Respondents Complying: 0%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 100%

(B) If a large number of subfolders is shared (e.g., greater than 4), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared folders.

Percentage of Respondents Complying: 0%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 100%

(7) Developers shall also implement the following principles:

(A) Disabling of file-sharing features, including but not limited to those outlined above, shall be simple to do and explained in plain language, with consistent terminology (i.e., terms such as "Default Setting," "File Extension," "Recursive Sharing," and "Shared Folder" shall always have the same meaning whenever used in communications from the [P2P] file-sharing software provider).

Percentage of Respondents Complying: 14%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 71%

(B) Complete uninstallation of the [P2P] file-sharing software also shall be simple to do and explained in plain language (e.g., by using the standard "Add/Remove Program" functionality on Windows or its equivalent on other operating systems).

Percentage of Respondents Complying: 100%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 0%

(C) [P2P] file-sharing software developers shall make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software, which contain the features outlined above, as soon as they are commercially available (i.e., after successfully completing beta testing). Previously-chosen sharing selections should be reconfirmed by the user upon installation of the new version of the software. In the reconfirmation process, users shall be warned, consistent with the foregoing requirements, before Sensitive Folders are shared and users must take Affirmative Steps to continue sharing Sensitive Folders and their subfolders. By default, Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%

(D) When the user subsequently chooses to upgrade to a different or newer version of the [P2P] file-sharing software, or to reinstall the same version of the software, either (a) if the software upgrade or reinstallation does not materially affect other user-controllable settings (including aspects of the user-interface and share settings addressed in this document), then it shall not change the file-sharing settings previously chosen by the user; or (b) if the software upgrade or reinstallation does materially change or require user-controllable settings to be reset, then it shall require file-sharing settings to be reset by the user as described above. If the upgrade or reinstallation uses the previously set file-sharing settings, the application shall warn users that those settings will be used, remind the user that changes to those settings

can be made in the designated area in the software, and warn users if Sensitive Folders or Sensitive File Types are being shared.

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%

OPTIONAL – FOR ADDED CONSUMER PROTECTION

(8) When the user chooses no longer to use the [P2P] file-sharing software in a given online session, the user shall be presented with a choice of either i.) turning the software completely off (i.e., fully disconnecting from the [P2P] network); or ii.) having the software continue to run in the background (i.e., still contributing resources to the [P2P] network to help facilitate content redistribution).

Percentage of Respondents Complying: 43%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 57%

(A) There shall be a simple way for the user to fully disconnect from the [P2P] network by using controls provided in a designated area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to fully disconnect from the [P2P] network shall be clear, timely, and conspicuous.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 71%

(B) When the [P2P] file-sharing software is in use and running in the background, the application shall clearly alert the user that the software is still running (e.g., in the "System Tray" on Windows or its equivalent on another operating system).

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 71%

Compliance Report Follow Up

After submitting the compliance report summary, there were two follow-up items based on FTC staff review of the compliance reports.

One related to a company that had not yet eliminated recursive sharing in its default mode. In March 2009, the CEO of this company committed that in the subsequent version of this software that by default sharing would not be recursive.

The other related to a separate company that in the FTC staff's view had not adequately complied with Sections 1 and 7(C) and (D).

The DCIA engaged with senior management and technology leaders at this company to address these outstanding compliance issues as expeditiously as possible, resulting in the company's commitment to make changes in the subsequent release of its software scheduled for June 2009.

In April 2009, the company made the following additional commitment:

> Please see the descriptions below regarding the outstanding ISPG Voluntary Best Practices fulfillment issues identified by the FTC [Sections 1, 7(C), 7(D)]. Where noted, the specific comments below indicate intended functionality for the next version of our software, the beta of which will be released in June as we originally committed, which is the soonest that this can reasonably be accomplished given our internal technical resources and the non-consumer-facing changes necessary for their implementation.
>
> However, the Company will be able to integrate the notification discussed regarding the Voluntary Best Practice Section (1) within 3-5 weeks of the date of this letter, sooner than our original commitment.
>
> By way of overview, in all instances dealing with sensitive file types (including but not limited to .doc, .wpd, .pdf, .exc.) our software by default does not share these types of files with the [P2P] network, even if they were shared in the prior version of our software. Period. This change was initiated with the current version of our software. This version will not share sensitive file types no matter whether these document file types exist in a folder that a user elects to share with the [P2P] network, no matter whether a user shared these sensitive file types previously in the prior version of our software, and no matter whether a user is using our software's library to manage his/her personal files. Sharing sensitive file types with the entire [P2P] network is only possible if a user changes his/her settings

by going to Tools -> Options -> Security -> and clicking Configure under the category of "Unsafe Categories" and disregards the following warning: "We strongly recommend you do not enable these settings." Should a user continue beyond this point, he/she then has to affirmatively "check" a box stating "Allow me to share documents with the [P2P] Network" and then click "O.K.", and then disregard the following warning: "Enabling these settings makes you more prone to viruses and accidently sharing private documents."

Following is more information about the changes designed to protect users against inadvertently sharing personal or sensitive data.

Current version of our software and beyond - General foundational changes:

1. By default (see 3 below regarding changing default settings), if a user tries to share a sensitive file type with the [P2P] Network, our software will not let him/her do it even if the file was previously shared in the prior version. This will be the case even if that user previously shared that file, and it will apply no matter where that user stored or stores the file on his/her computer or whether or not that file is managed by the user in his/her library.

2. By default, if a user shares a folder containing sensitive file types, our software will not share the sensitive file.

3. In order to share sensitive file types, a user must affirmatively undertake the following: go to Tools -> Options -> Security -> and click Configure under the category of "Unsafe Categories" and disregard for the following warning: "We strongly recommend you do not enable these settings." If the user elects to continue, in the "Configure" section, he/she must then check the box "Allow me to share documents with the [P2P] Network," and then click "O.K.", and then disregard the following warning: "Enabling these settings makes you more prone to viruses and accidently sharing private documents."

a. NOTE: changing this setting will still not share users' documents and will not automatically share any sensitive file types, rather it merely allows users to share them if they affirmatively elect to share a particular file at a later point in time.

Regarding the ISPG Voluntary Best Practices fulfillment issues -

Voluntary Best Practice Section 1 – for release within 3-5 weeks

1. To begin, mere installation and activation of our software will not result in the receipt or sharing of files with other users of our software without further affirmative steps taken by the user.

2. Effective on the beta release of the next version of our software, during the first-launch following installation the user will be told that files downloaded from the [P2P] network will be shared automatically with the [P2P] network and how to change this setting.

Voluntary Best Practice Sections 7(C), 7(D) – for June release.

1. Beginning with the current version of our software and for all versions thereafter, our software by default does not share sensitive file types. Even if they were shared previously in the prior or earlier version of our software, the current version "un-shares" ALL sensitive file types.

2. As our software loads a user's library, if it finds any sensitive file types being shared, a warning of such will be given to the user along with instructions on how to disable sharing the sensitive file type.

3. In the event a user (1) was using an earlier sub-version of our current major release, AND (2) affirmatively changed his/her setting in that version to allow sharing of sensitive file types AND (3) affirmatively chose to share a specific file or files of this type (because merely enabling the sharing of sensitive file types does not automatically share such files, rather the user must choose specific files to share), our software will display a notification substantially similar to this: "You are sharing a sensitive file type and doing this can lead to identity theft. Click here to stop sharing sensitive file types and prevent this from happening."

H.R. 1319

In April 2009, Subcommittee staff invited the DCIA to participate in redrafting the subject proposed legislation. We agreed to do so and formed a DCIA Member company sub-group of interested parties to conduct this work.

This process is now underway and the DCIA would be glad to coordinate this work with Subcommittee staff.

Our basic principles in undertaking this redraft were to seek to help improve the language of the measure by making it more specific to user behavior and software functionality, and to express its provisions more precisely and in plain language.

Among our greatest concerns was that the bill as drafted would have unintended consequences that would make some of the most advanced implementations of P2P, which involve licensed content distributors, uncompetitive.

For example, even those that don't include a user-generated content (UGC) component still cause the user's computer to seed files. And because the proposed legislation applies to the use of the user's bandwidth without their knowledge, it could apply to almost any application that relies on distributed computing.

We believe the proposed legislation was precipitated by an increasingly outdated concern over a very specific feature of a small number of applications, some of which no longer exist.

Our Member companies and ISPG participants, specifically those that rely on P2P technologies, no longer have that feature – recursive sharing of sensitive file types – or are in the process of phasing it out.

The present bill goes way beyond that specific concern, however, and would appear to apply to additional functionality and technologies that have nothing to do with recursive file sharing.

Applying the requirements of the bill to all these products, services, and companies is unnecessary and would be burdensome and counter-productive. The problem the bill is intended to address is limited to a small number of companies, and these are the ones to which the ISPG best practices already apply.

To the extent that legitimate consumer concerns persist in the area that the bill is meant to address, we strongly believe they can best be handled by ongoing self-regulation under the oversight of the appropriate federal authority that we have initiated with the ISPG.

Nevertheless to meet our commitment to Subcommittee staff to work on a redraft, certain of the changes our sub-group is considering are to more precisely define the file-sharing user error to be prevented by means of the contemplated legislative safeguards.

This includes a narrower description of the inadvertent making available of sensitive or personal information on a computer through the use of file-sharing software applications.

We are further seeking to define the sensitive file types that should be covered by a precisely targeted measure.

We are also attempting to address the practical realities of timing as well as content for optimally effective consumer-protecting notices and obtaining of informed consent at various stages in the accessing, installing, and activation of such software and its various modes of functionality, and relevant differences for various genres of content.

Regarding the uninstallation provisions, our sub-group is also reviewing this language against previously developed consumer disclosure guidelines as well as generally established practices for best-of-class related software applications, again taking into account multiple modes of file-sharing software operation and functionality that should be under the clear control of the user.

We have requested legal counsel to review the proposed enforcement regime and provide advice to the sub-group.

It is likely that the defined terms would be substantially changed as a result of the above work effort, and the list slightly expanded to include such additional items as the file-sharing function itself, which involves searching, discovery, and copying of files.

It would also need to involve such essential file-sharing software application defining terms as shared directory, data files versus streaming content, etc.

CONCLUSION

Based on the demonstrated success to date of the ISPG in putting in place a system for effective self regulation, the potential harm of unintended consequences from overbroad impact of a bill of this sort, and the fundamental principle that legislation should embolden technological advancement rather than hinder it, the DCIA and our Member companies are opposed to the passage of this legislation.

The bill would likely unnecessarily burden U.S.-based technology firms with compliance with an innovation-freezing measure, while being unenforceable against overseas firms whose software is available to U.S. consumers. Of great concern to us is how this bill might stifle yet undeveloped new and potentially very useful and valuable software applications.

Our legal review up to this point suggests that no matter the changes in the bill's construction, no matter any amount of rewording, it will still not only stifle its purported target from possible improvements that would better address the problem the bill intends to address, but it will also potentially still apply to any type of data transmitting software, including Internet applications, desktop applications, e-mail applications,

instant messaging (IM), cloud computing, social networks, fully licensed P2P deployments, hybrid peer-assisted CDNs, etc.

The foregoing summarizes some of the very real difficulties in trying to develop legislation such as this.

Rather than an overly broad, outdated, and potentially stifling legal measure, we believe that the Subcommittee's acknowledgment and formalization of requirements for compliance with the ISPG's self-regulatory process will be more effective in achieving the stated purpose that the bill is intended to accomplish.

As we noted previously, because of both the technical complexity and relatively fast-moving innovation in this area, a federally mandated and closely monitored private sector initiative, rather than even the best intentioned legislative measure, will produce the most beneficial effect to the public and to government agencies whose sensitive and confidential information must be protected as a matter of national security.

Nonetheless, the DCIA and our Member companies will continue to review the bill in an effort to find a way to reconstruct it as requested to achieve the Subcommittee's goals.

If the Subcommittee chooses to move the bill forward, we will be there to aid in the redrafting process and to help the Subcommittee address opposition to the bill.

On the other hand, the DCIA has committed to industry self-regulation through the ISPG to address the subject matter of this bill, and is making substantial progress.

As a further commitment, the DCIA is willing to charge our existing ISPG with responding to additional concerns that may be raised today, and as may be more precisely delineated by Subcommittee staff following up on the hearing. We look forward to working with the Subcommittee in a productive manner on these issues in a way that will significantly benefit all of your constituencies.

Thank you very much for your continued interest in our developing industry.

Respectfully,

Martin C. Lafferty
Chief Executive Officer
Distributed Computing Industry Association (DCIA)

Attachment: Testimony of DCIA Member Company Solid State Networks

Cc: Subcommittee on Commerce, Trade, and Consumer Protection
The Honorable John Barrow
The Honorable Bruce L. Braley
The Honorable G. K. Butterfield
The Honorable Kathy Castor
The Honorable Diana DeGette
The Honorable Phil Gingrey
The Honorable Charles A. Gonzalez
The Honorable Bart Gordon
The Honorable Gene Green
The Honorable Mary Bono Mack
The Honorable Jim Matheson
The Honorable Doris O. Matsui
The Honorable Tim Murphy
The Honorable Sue Wilkins Myrick
The Honorable Frank Pallone, Jr.
The Honorable Joseph R. Pitts
The Honorable John P. Sarbanes
The Honorable Steve Scalise
The Honorable Jan Schakowsky
The Honorable Zachary T. Space
The Honorable Cliff Stearns
The Honorable Bart Stupak
The Honorable John Sullivan
The Honorable Betty Sutton
The Honorable Lee Terry
The Honorable Anthony D. Weiner
The Honorable Ed Whitfield
The Honorable Joe Barton (ex officio)
The Honorable John D. Dingell (ex officio)
The Honorable Henry A. Waxman, CA (ex officio)

U.S. House of Representatives Committee on Energy and Commerce

Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319

Testimony of Rick Buonincontri

CEO, Solid State Networks

May 5, 2009

Dear Chairman Rush and Ranking Member Radanovich:

Solid State Networks is a leading developer of content delivery software for online content distribution. Our customers are content publishers (primarily game developers and publishers) that want to improve the user experience for consumers that want to access their digital content and lower their own delivery costs. Peer-to-peer (P2P) delivery technology is a key component that has been incorporated into our products. The P2P technology that we employ utilizes simultaneous byte requests from multiple sources, including other users accessing the same content, to enable fast and efficient data transfers. This type of P2P technology provides a scalable method of distributing the demand for bytes across many sources, including other computers that are requesting similar bytes. A computer will typically only exchange a small fraction of any content that has been requested from the publisher with any other computers in the network. It is technically impossible for consumers to expose any files, data or sensitive information to other users as a result of using our software. The system contains no facility to enable a computer to disclose the existence of files to anyone, including other users. Thus, there is absolutely no opportunity for a consumer to inadvertently share user generated content.

It is also worth noting that Solid State Networks products cannot be used for "file sharing" purposes by consumers. We have not and do not make tools that are used by file-sharing communities. Our software has not and does not enable the search, discovery, or copying of files from one computer to another using our software. Nor does our software enable consumers to access content posted by other users via websites that index content for download. Since the day of our company's inception, our objective has been to make provide commercial P2P software solutions for the benefit for content publishers.

Preventing consumers from inadvertently sharing sensitive information and files via file sharing networks has been shown to have widespread support from within the P2P software industry, including Solid State Networks. However, H.R. 1319 is strongly opposed by most companies within the industry for a variety of reasons. Solid State Networks also strongly opposes this bill for the following reasons:

1. H.R.1319 is overly broad in scope. For example, it does not differentiate between "P2P technology" software that, inherent in the design, poses no threat of enabling inadvertent disclosure of information and "file sharing" software that enables the searching, discovery, and copying of files directly from one computer to another using the software. This broad definition

threatens to negatively impact companies using P2P technology that cannot possibly enable the disclosure of sensitive information.

2. The P2P software industry has already mobilized to address the concerns represented by H.R. 1319. These companies recognize that the long term viability and acceptance of P2P hinges on the ability to secure trust with the consumers that use their products. Concerted efforts at self-regulation will provide more opportunity to adapt to the rapid technological changes that will occur in the years to come.

3. H.R. 1319 has the potential to limit the ability of game companies to provide immersive interactive experiences. P2P technology has been in use by game developers to enable the personal interaction among players for many years. Billions of files, in the form of game patches and updates, have been delivered via P2P technology without any reported instances of disclosure of non-game related information. Yet adherence to H.R. 1319 would impose extreme burden that most, if not all, players would consider as to make the games unplayable. Additionally, the ability of game developers to meet the growing demand for customization and personalization by players would be adversely impacted. Providing the tools to enable players to create and share their own experiences within the game with other players will become difficult, if not impossible, under the broad restrictions contained in H.R. 1319.

Thank you for the opportunity to present this testimony on behalf of Solid State Networks and the companies that benefit from our products. I hope that I have conveyed the serious potential for unintended and adverse impacts posed by H.R. 1319 on industries that are unrelated to file sharing.

Respectfully,

Rick Buonincontri
Chief Executive Officer
Solid State Networks

Cc: Subcommittee on Commerce, Trade, and Consumer Protection
The Honorable John Barrow
The Honorable Bruce L. Braley
The Honorable G. K. Butterfield

U.S. House of Representatives Committee on Energy and Commerce

Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319

Testimony of Rick Buonincontri

CEO, Solid State Networks

The Honorable Kathy Castor
The Honorable Diana DeGette
The Honorable Phil Gingrey
The Honorable Charles A. Gonzalez
The Honorable Bart Gordon
The Honorable Gene Green
The Honorable Mary Bono Mack
The Honorable Jim Matheson
The Honorable Doris O. Matsui
The Honorable Tim Murphy
The Honorable Sue Wilkins Myrick
The Honorable Frank Pallone, Jr.
The Honorable Joseph R. Pitts
The Honorable John P. Sarbanes
The Honorable Steve Scalise
The Honorable Jan Schakowsky
The Honorable Zachary T. Space
The Honorable Cliff Stearns
The Honorable Bart Stupak
The Honorable John Sullivan
The Honorable Betty Sutton
The Honorable Lee Terry
The Honorable Anthony D. Weiner
The Honorable Ed Whitfield
The Honorable Joe Barton (ex officio)
The Honorable John D. Dingell (ex officio)
The Honorable Henry A. Waxman, CA (ex officio)

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes Mr. Pratt for 5 minutes for the purposes of an opening statement.

STATEMENT OF STUART K. PRATT

Mr. PRATT. Chairman Rush, Ranking Member Radanovich and members of the subcommittee, thank you for this opportunity to appear before you today. My name is Stuart Pratt, president and CEO of the Consumer Data Industry Association. Our 250 member companies provide our Nation's businesses with data tools necessary to manage risk and a wide range of consumer transactions, and these products include credit, mortgage reports, identity verification tools, law enforcement investigative products, fraud check transaction identification systems, decision sciences technologies, location services and collections. My comments today will focus exclusively on H.R. 2221, and we applaud its introduction.

CDIA's members agree that sensitive personal information should be protected. We also agree that consumers should receive breach notices when there is a significant risk of them becoming victims of identity theft. Our members agree with the Federal Trade Commission recommendations which embrace these two concepts. I would only add that if a federal law is to be enacted, it should be a true national standard.

We believe that data security and breach notification provisions in H.R. 2221 would be most effective if they were better aligned with requirements found in other current laws. Alignment is key to ensuring that all who are affected by the Act are successful in complying with new duties under DATA and also with their current duties found under other laws such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. Let me discuss some of the ways that 2221 interplays with existing duties found in current laws.

Section 56 defines the term "information broker." Absent aligning this definition with other current laws, our members' products will be affected. This bill would require information brokers to have reasonable procedures to verify the accuracy of personal information, provide consumers with access to these data and ensure a system by which consumers can dispute information. All of our members operate consumer reporting agencies as this term is defined in the Fair Credit Reporting Act. They produce data products defined as consumer reports. Consumer reports are used to make determinations of a consumer's eligibility for a service or a product and the FCRA establishes duties for accuracy, access and correction as it relates to these products. Our members agree that where data is used to make a decision regarding consumers' eligibility for a product or service, consumers should have these rights.

Since there are similar duties under the FCRA and DATA, we propose the definition of information broker should be amended to exclude the term "consumer reporting agency", and while we appreciate the inclusion of section C3C which attempts to address our concern, we believe that since the FCRA's duties are well understood and the FTC has direct enforcement powers, that we should have a complete exemption.

Regarding disclosure, section C3 allows an information broker under certain circumstances to not disclose personal information to a consumer. This section does not exempt an information broker's fraud prevention tool from the duty to verify accuracy. Fraud prevention tools are designed to identify the possibility of fraud and to apply an accuracy standard of fraud prevention tools is unworkable since these tools are designed to warn a lender or utility or other business about the possibility of fraud. Fraud prevention tools consider how data has been used in previous identified cases of fraud and employ many other relational strategies. We would urge the expansion of C3B to include fraud prevention tools so that they are completely exempted from the accuracy standard requirement, not because the tools are designed poorly but because these tools cannot line up with an accuracy standard in the first place.

Your bill also as indicated establishes both a requirement for data security and a requirement for security breach and we have absolutely no qualms about either of those requirements. Our member in fact comply with those types of requirements today and our only request is that where our member companies are already operating as a consumer reporting agency under the Fair Credit Reporting Act or where they are operating as a financial institution under the Gramm-Leach-Bliley Act, that they would be exempted from these data security and these security breach notification duties because they already have those duties under the Fair Credit Reporting Act and also under the Gramm-Leach-Bliley Act and in particular the safeguards rules which include breach notification.

So this process of alignment will make this bill more effective. If we can make this truly a national standard, you certainly will have filled some gaps along the way. I think that Mr. Sohn said it very well. In the meantime, we live with a range of State laws. We have worked constructively with many, many States in establishing those statutes and in establishing definitions of the crime of identity theft and we will continue to do that and we look forward concurrently to working with you in the committee. Thank you.

[The prepared statement of Mr. Pratt follows:]

STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

BEFORE THE

Energy and Commerce Committee

Subcommittee on Commerce, Trade and Consumer Protection

House of Representatives

ON

Legislative Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319,

the Informed P2P Act

Tuesday, May 5, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, thank you for this opportunity to appear before you today. My name is Stuart Pratt, president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify.

CDIA is an international trade association with more than 250 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it, ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

My comments will focus exclusively on H.R. 2221. H.R. 1319 focuses on issues relating to the practice of making "files from a protected computer available to another computer through a peer-to-peer file sharing program" and CDIA's members are not involved in these types of activities.

Scope of H.R. 2221

We applaud the introduction of H.R. 2221. Section 2 of H.R. 2221 proposes to require any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish policies and procedures for information security based on rules which would be promulgated by the Federal Trade Commission. Section 3 of H.R. 2221 requires these same persons to comply with specific requirements of the Act where they discover a breach of security relating to personal information. Section 2(c) of H.R. 2221 proposes to impose certain unique duties regarding "information brokers" as that term is defined in Section 5(6).

CDIA's members agree that sensitive personal information should be protected. They also agree that consumers should receive breach notices when there is a significant risk of them becoming victims of identity theft. Our members agree with the Federal Trade Commission recommendation offered in multiple testimonies on the Hill and via their joint Task Force report issued along with the Department of Justice that if a federal statute is to be enacted, it should be a true national standard and that it should focus on safeguarding sensitive personal information and notifying consumers when a breach has occurred which exposes the consumer to a significant risk of becoming a victim of identity theft. In the absence of a national standard, our members have worked constructively with state legislatures to create security breach notification laws, data security laws and laws which define the crime of identity theft.

We believe that in general the data security and breach notification provisions of H.R. 2221 would be most effective if they were better aligned with requirements found in other current federal laws. From our experience, statutory alignment is a key to ensuring that all who are affected by the Act are successful in complying with new duties under DATA and also with their current duties found in other laws such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. We also believe it is important to ensure that requirements do not harm the operation of products, which is a policy result none of us would wish to see.

Let me now discuss some of the ways in which duties under H.R. 2221 interplay with existing duties found in other laws.

Information Brokers & Consumer Reporting Agencies

In Section 5(6) of H.R. 2221, the term "information broker" is defined. It is a broad definition, and information brokers have specific, unique duties under the Act. Absent aligning this bill with other current laws, our members' products will be affected.

This bill would require information brokers to: have reasonable procedures to verify the accuracy of personal information; provide consumers with access to these data; and ensure a system by which a consumer can dispute information and to correct disputed information where it is found to be inaccurate.

All of our members operate consumer reporting agencies as this term is defined by the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) and produce data products defined as "consumer reports." Consumer reports are used to make determinations of a consumer's eligibility for a service or product. The FCRA establishes duties of accuracy, access and correction as it relates to consumer reports produced by consumer reporting agencies. Our members agree that where data is used to make a decision regarding a consumer's eligibility for a product or service, the consumer should have these rights, which have been available to all of us as consumers since 1970.

Since there are similar duties under the FCRA (consumer reporting agencies) and the DATA (information brokers), we propose that the definition of "information broker" should be amended to exclude a "consumer reporting agency" as that term is defined in the FCRA. We appreciate the inclusion of Section (c) (3) (C) which attempts to address our concern, but we believe that since the FCRA's duties are well understood and well established and the FTC already has direct enforcement powers under the FCRA with regard to the practices of consumer reporting agencies, that a clear exemption for consumer reporting agencies from the definition of information broker is the most effective approach.

Fraud Prevention Tools – Access and Correction Duties

Our members produce best-in-class fraud prevention tools and, due to the breadth of the definitions of "personal information" and "information broker," these products are

affected by the duty to provide access and correction. We appreciate the inclusion of Section 2(c)(3)(B)(iii)(I) & (II), which allows an information broker to limit access to information which otherwise must be disclosed. It is important to ensure that the "recipe" for fraud prevention tools is not disclosed. Unlike consumer reports regulated under the FCRA, fraud prevention tools are not used to stop a transaction or to make a decision about a consumer, but only to ensure that a consumer is properly identified in a transaction. We believe that Section (c)(3)(B)(iii)(II) would be less ambiguous if the decision to not disclose was not tied to an information broker having to decide whether or not disclosure would compromise the fraud prevention tool. We suggest that the phrase "that would be compromised by such access." be struck to ensure that fraud prevention tools are protected. Similarly, we believe that FTC Rulemaking in Section (c)(3)(B)(iv) could inhibit the development of these tools, as well.

Fraud Prevention/Investigative/Location Tools – Verification of Accuracy

While Section (c)(3)(B)(iii) allows an information broker, under certain circumstances, to not disclose personal information to a consumer, the section does exempt an information broker's fraud prevention tool from the duty to verify accuracy found in Section (c)(3)(A). Consumer reports are used to make decisions about a consumer's eligibility for a product or service. Because of this a consumer reporting agency must use "reasonable procedure to ensure maximum possible accuracy" standard when producing consumer reports. In contrast, a fraud prevention tool is not used to stop a transaction and in fact it is built based on the premise that fraud is not easily identified. Fraud tools are

designed to identify the possibility of fraud. To apply an accuracy standard to fraud prevention tools is unworkable since these tools are designed to warn a lender or utility for example, of the possibility of fraud. Fraud prevention tools consider how data has been used in previously identified cases of fraud and employ many other relational strategies. We urge Section (c)(3)(B)(iii) to be expanded to apply to Section (c)(3)(A) as well as to (B). We are also concerned about many investigative tools used by law enforcement and location tools used, for example, in the enforcement of child support. These investigative and location tools are build to help identify possible connections that will lead to the right person. As is the case with fraud prevention tools, imposing an accuracy standard is unworkable.

Data Security Requirements

Section 2 of H.R. 2111 establishes a requirement that all persons of a certain type which possess personal information must secure the data. Our members agree that data security is essential.

Our members operate consumer reporting agencies regulated by the FCRA and also operate financial institutions as defined by the Gramm-Leach-Bliley Act (Pub. L. 106-102). In addition to these specific statutes which impose data security requirements, every business in this country has to consider the implications of the Federal Trade Commission's enforcement efforts regarding data security where they have been successful in asserting that lax practices are likely unfair, or deceptive or both. Further,

data breaches have resulted in a range of private actions against companies that had inadequate security practices and thus this case law also informs the thinking of all companies which possess sensitive personal information.

Due to the extensive data security requirements already imposed on our members via both of these laws (and regulations therein) and the context of legal actions taken, we believe that consumer reporting agencies and financial institutions should be excluded from the requirements of Section 2 of H.R. 2111. We agree that because of the breadth of the application of H.R. 2111 that there is the need for the inclusion of Section 2(a)(3). This provision is important and helps to account for unanticipated results of the bill, but where we can identify specific instances where protections already exist as is the case for GLB and FCRA we do not believe an FTC determination is necessary and thus financial institutions and consumer reporting agencies should be specifically excluded from the requirements of Section 2.

Data Breach Notification Requirements

Section 3 of H.R. 2111 establishes requirements for notifying consumers where there is a breach of personal information. A notice is not required where "there is no reasonable risk of identity theft, fraud, or other unlawful conduct." There are also exceptions to the notification requirement if the data was encrypted or otherwise rendered unreadable or indecipherable.

CDIA agrees that there should be an effective risk-based trigger for the disclosure of notices is necessary and believes that the phrase "significant risk if identity theft" sets the right standard. We also agree that there should be specific exceptions for data which is encrypted or otherwise rendered unreadable or indecipherable.

Since CDIA members operate consumer reporting agencies defined by the FCRA and also often as financial institutions as defined by the Gramm-Leach-Bliley Act we proposed that these two entities be excluded from the data breach requirements of this bill since they are already required to comply with the breach notification requirements of other laws.

Content of Breach Notifications

Section (3)(d)(B) describes the content of notices which will be sent to consumers. With regard to the consumer's right to one free credit report on a quarterly basis, we appreciate inclusion of the language in Section 3(e) which makes it clear that the person who experienced the breach and who is notifying consumers is the one who pays for the credit reports to which the consumer is entitled.

3(d)(B)(iv) requires that the toll-free numbers for major credit reporting agencies be included in the notice. We request that the bill be amended to require those who are sending out breach notifications to more than 5,000 individuals to notify the consumer reporting agencies in advance. Further, all persons issuing notices must verify the

accuracy of the contact information included. Our members have at times discovered that breach notices issued by others had incorrect toll free numbers listed.

Definition of Personal Information

Section 5(7)(A) establishes a definition of the term "personal information." Having a definition is clearly necessary to ensure that all persons affected by the scope of the bill understand the type of data which must be protected, etc. Our members are concerned with the inclusion of Section 5(7)(B) which allows the FTC to alter this definition. We believe the definition as proposed is adequate. The FTC could make a determination that a new element of data is now included under the definition and in doing so unintentionally cause extraordinary expense for affected persons. As written the FTC is not required to validate their reasons for changing the definition, nor are they required to determine the financial or product impact such a change would have.

Enforcement

CDIA continues to believe that enforcement of the statute by state attorneys general should be comparable to the FCRA provision which allows them to sue for actual or statutory damages of $1,000 for each negligent or willful violation (see FCRA Section 621(c)(1)(B)). We believe a cap on damages is also appropriate and that compliance with the provisions of this Act should be tied to a "reasonable procedures" standard.

Uniform National Standard

CDIA applauds the inclusion of language in Section 6 which proposes to preempt additional state actions. Our members believe that absolute uniform standards are critical if this bill is to become law and we are happy to provide additional input on the current provision, which appears to be construed too narrowly.

Conclusion

Again, thank you very much for the opportunity to testify. I am happy to address any questions that you may have.

Mr. RUSH. The chair thanks the gentleman, and now the chair recognizes Mr. Rotenberg for 5 minutes.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Mr. Chairman, Mr. Radanovich, members of the committee, thank you very much for the opportunity to be here today. EPIC is a nonprofit research organization here in Washington.

We have a particular interest in this issue of security breach notification. EPIC was the organization that had urged the Federal Trade Commission to investigate the data practices of a company called ChoicePoint because we believed that that company was making the personal information of American consumers vulnerable to misuse. The FTC did not heed our warning and instead we all read in the newspapers when an investigation broke in Los Angeles that revealed that the records of 145,000 American consumers had been sold to a criminal ring engaged in the act of identity theft. I promise you, after that news story appeared, the FTC and many State attorneys general became very interested in this problem.

Now, we learned of the problem with ChoicePoint in part because of a good law that had been passed in the State of California which required companies that suffered from a security breach to notify people who are impacted, and as a result of the ChoicePoint notification, many other States began to understand the need for security breach notification. Now, this has been an evolving process. I think there are now 44 States in the United States that have security breach notification, and while we certainly support an effort to establish a high standard across the country, I do want to warn you that one of the consequences of this bill would be to effectively tie the hands of the State from further updating their laws or enforcing stronger laws, and I think this would be a mistake. I read recently, for example, that the California State Senate has just approved new changes to its notification law that would provide individuals with better information about the type of personal information that was improperly disclosed and how it might be misused. This need to be able to continue to update security breach notification I think should be a consideration as the committee looks at legislation to establish a national standard.

One of the other points I would like to make about the legislation concerns the relationship in the realm of notification between the individuals who are impacted and the role of the Federal Trade Commission, which is also notified under the bill. There is understandable concern that if individuals receive too many breach notices, they will serve no purpose, and so there is a need to set a standard so that people are not receiving lots and lots of these notices which they will come to ignore. But with respect to the role of the Federal Trade Commission, I think the bill could be strengthened by requiring companies in all circumstances to notify the Commission where substantive breaches have occurred, and moreover to put on the Commission an obligation to be more transparent about the information that it receives regarding the problems of breach notification in the United States. There is also a risk with the legislation as it is currently drafted that the FTC will

obtain information about security breaches, may choose not to act on the information it receives and that information will effectively remain secret both to the public and to this committee and the problem will continue to grow, so I hope that is an area that can be considered as well.

We talk also about the safe harbor provisions, essentially companies that have certain security practices such as encryption should be encouraged to put in place and maintain those practices but again we think that notification can be made to the Federal Trade Commission in those instances where security breaches occur even if it may not be necessary to notify the target population.

Finally, I would like to point out that since when the bill was originally introduced there have been significant changes both in the Internet and also in communications technology. Facebook, for example, now has 200 million users. Four years ago when this bill was first considered, there were many, many fewer people using these social network services. This has two implications. First of all, there is a new way to notify people online. It is no longer necessary to talk just about a website but also a social network presence. It also means that there is a new risk in data collection that needs to consider the growing significance of social network services. And finally, I might mention that text messaging has become a very effective way to notify people about things that might concern them regarding security. We propose in our testimony that where possible, text messaging be used as a supplement to the other notification procedures including mail and e-mail.

So thank you again for the chance to testify and I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act"

Before the

House Committee and Energy and Commerce
Subcommittee on Commerce, Trade,
and Consumer Protection

May 5, 2009
2123 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act. My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor at Georgetown University Law Center.

EPIC is a non-partisan research organization, focused on emerging privacy and civil liberties issues. We have worked for many years to draw attention to new privacy and security risks, such as data breaches, pretexting, and the commercial sale of personal data, as well as to make recommendations for both technical solutions and legislation that can help mitigate these risks. While there is no single solution, either in technology or law, that can prevent security breaches, there are a number of steps that can be taken to reduce the risk.

I have several specific suggestions for the legislation that is currently before the Committee today. But I would also like to make a preliminary comment about the relationship between legislation and the efforts that are underway to safeguard security and privacy. I think it would be a mistake to assign to the FTC, or to any agency, the central responsibility for information security. This is an area where technology is changing rapidly, and both new problems and new solutions arise almost daily. The federal rulemaking process is ill suited to respond in this environment, and there is a real danger that well intended regulation may in some circumstances frustrate more effective solutions either because the process is too cumbersome, too secretive, or simply unresponsive.

At the same time, there is a need to make clear fundamental obligations on the companies and organizations that collect and use personal data on consumers and Internet users. It is simply too easy for firms today to capture the benefits of data collection and ignore the risks. In the absence of security obligations and breach notification requirements, it is too easy for firms to continue bad practices. In fact, not only are there few incentives to change practices, without legislation, companies are likely to conceal rather than to correct problems.

This is why legislation is appropriate – to ensure that companies carry the responsibility for their data practices. But it is critical to ensure the legislation is effective, flexible, and responds to the rapidly changing environment. Congress should be wary of setting security standards through a rulemaking process. The better approach, in my opinion, is to focus on the broad obligations, to make clear the incentives, and to encourage the development of the best solutions. This does not diminish in any respect the need for robust security standards – it simply leaves the law to do what it does best: make clear the rights and responsibilities of the

various participants in the information exchange – and leaves to the technical experts the obligation to develop the best solutions.

The other key point to make at the outset is that almost all of the states have responded over the last few years to develop robust security breach notification legislation. Many of these laws can be traced back to the California notification law that was famously triggered in a matter that EPIC brought attention to involving the sale of data on American citizens to a criminal ring engaged in identity theft. That notification and the investigation that followed led to dramatic changes in the information broker practices in the United States. While there is clearly a lot more that needs to be done to safeguard personal data, you should not underestimate the enormous value of these breach notification statutes as well as the unintended problems that could result if the federal law preempts the more responsive state law. For reasons I will discuss in more detail below, I would recommend that you not adopt legislation that would preempt the ability of the states to develop more effective means to respond to these new problems

H.R. 2221, the Data Accountability and Trust Act

Mr. Chairman, although I have not seen the text of H.R. 2221, I understand that this bill is identical to H.R. 958, The Data Accountability and Trust Act that was introduced in the 110th Congress. My comments therefore are directed to the text of that bill. The main legislative development that has occurred since the introduction of H.R. 948 is the adoption of American Recovery and Reinvestment Act of 2009 (ARRA), which includes new provision for medical record privacy and new authorities for the FTC, including a rulemaking for security breach notification. It may be worth looking at those provisions to determine whether the current bill should be revised. There are also significant developments in technology, such as the rapid rise of social network services and the increasing use of text messages, which may be worth considering as the Committee reviews this legislation. Significantly, the new communications tools may also provide new opportunities for breach notification, and new analytic tools could provide better understanding of security challenges if the FTC data is made available to the public.

As currently drafted, H.R. 2221 attempts to address growing concerns about privacy protection and security breaches by granting the FTC new authority to regulate companies that collect and use personal data. The bill attempts to crack down on the information broker industry, limit pretexting, and sets out new notice obligations in the event of a security breach. Overall, this is an important and timely legislation that seeks to address several of the key concerns of American consumers and internet users – the failure to ensure that personal information is adequately protected, the unregulated market for personal data, and the inability of users to know when their data has been improperly disclosed.

EPIC would like to express its support for the legislation and the sponsors of this measure. We appreciate the willingness of the Committee to examine this issue and to develop a legislative response. My comments on the bill are intended to show areas where it may be possible to strengthen the legislation.

Method of Notification

The bill currently proposes the use of either written notification or email notification when an obligation to provide notification arises. Sect. 3(d)(1)(A). I would suggest that you include an additional obligation to provide a text message where possible. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But is a very effective technique for notification and it could help make people aware that they should look for a notice that might arrive in the mail or show up in the email box.

In a similar spirit, where the bill speaks of providing notification by means of a web site, it may be appropriate to add "or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

Public Record Defense

There is an odd provision, Section 4(c) of the Act, that would create an affirmative defense where all of the personal information disclosed as a result of a security breach in violation of the Act is "public record information" available from federal, state, or local government systems and was acquired by the company that suffered the breach for such purposes. The theory underlying this provision, I imagine, is that there could be no additional harm to the individual of the breach of this information if it is already available to the public. But this is the wrong way to understand the problem and the affirmative defense will undercut the purpose of the Act.

If an organization suffers a security breach of confidential information or of "public information" it has a problem that needs to be corrected. If no action is taken to correct the problem, it is quite likely the breach will occur again. That is why the security obligation should apply even when there is no immediate harm to the individual: The problem remains. Also, I would not assume the fact that personal

information may be found through public data sources that the information disclosed in a data breach is equivalent. It is quite likely, particularly in the information broker industry, that the "public" information contained in a particular data record is far more detailed than any record that would be available in a singe government record system.

Treatment of Personally Identifiable Information

One of the key provision of the Act is the definition of "Personal Information" set out in sect. 5(7). This definition is critical because, as with most privacy bills, this definition will determine when the obligations of the Act should be applied and when they can be pretty much ignored.

As currently drafted, the bill sets out a narrow definition for Personal Information, as compared with other privacy statutes. For example, the bill seems to suggest that a social security number would not be personally identifiable if it is possessed without the associated person's name. The bill also ignores other popular identifiers, such as a user ID for Facebook, which points as readily to a unique individual as would a driver's license or a social security number.

The definition is also narrow in light of the FTC report released earlier this year on Internet advertising that noted that there are many ways to track Internet users, including the use of "IP address" that can uniquely identify a user's computer, much as phone number will uniquely identify a cell phone. In many cases, this is also a form of personal information that should be subject to the bill's requirements.

The bill does provide for a rulemaking that could modify the definition of "personal information" but even this rulemaking seems unnecessarily narrow as it is limited to changes that are "necessary to accommodate changes in technology or practices."

I would suggest a construction that would define Personal Information as information that "identifies or could identify a particular person," followed by the examples cited in the bill as illustrations, with the qualifying phrase "including, but not limited to." This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

Preemption

Section 6 addresses preemption and the circumstances under which the federal law would overwrite possibly more effective state information security legislation. As currently drafted, H.R. 2221 preempts state laws that either have similar security obligations as well as state laws that provide for security breach

notification. The Act does leave in place state trespass, contract and tort law, as well as claims involving fraud.

My own view is that it would be a mistake to adopt a preemption provision of this type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues. President Obama made this point very directly in his recent remarks to the National Governors Association when he described the states as the "laboratories of democracy." This was a reference to a famous opinion by Justice Brandeis about the specific authority of the states to legislate in response to new problems. This view reflects the belief that there should be experimentation in regulatory approaches.

There is an additional reason that I believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California, which is widely credited for adopting the first breach notification statute, also found itself needing to update its own law to address the specific problems of medical information breach. It is very likely that the states will face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point."

While there is a clear need to strengthen security safeguards, I remain concerned about the ability of the FTC to develop a regulatory framework for information security in the United States, particularly when it is the only agency with authority to do so.

Private Right of Action

As the bill is currently drafted, a person whose personal data is improperly leaked by a company in possession of the data is signed up for two years for a credit card notification service. While this remedy may provide a nice revenue stream for those in the credit card monitoring service, it may not be very satisfying for consumers. Where a security breach has led to cases of identity theft, which was clearly the case in the Choicepoint incident, consumers are entitled to a real remedy.

I would strongly urge the Committee to add a private right of action to the bill with a stipulated damage award, as is found in many other privacy laws. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme which relies almost entirely on the

Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights.

If the law is passed without a private right of action, and the Commission fails to act, is reluctant to act, or simply doesn't understand a problem where it should act, individuals who are harmed by a security breach will be in a worse position then they6 were before the law was adopted because any rights that were previously available under state law, less those explicitly carved out, will no longer be available.

Safe Harbor

There are two different types of safe harbor provisions in the Act. Section 3(f)(1) essentially suspends the law if, following a breach of security, "such person determines that "there is no *reasonable risk* of identity theft, fraud, or other unlawful conduct." (Emphasis added). In other circumstances, a reasonableness standard might be appropriate. The problem here is that the company will decide itself, having suffered the breach, *whether there is reasonable risk of harm to others* and there will be no effective way to review this decision if the company guesses wrong. That is an approach that will invite greater secrecy and less accountability. The simple solution may be to remove the word "reasonable." If a company determines that there is "no risk of identity theft, fraud, or other unlawful conduct" then it would be reasonable to suspend the notification requirement.

The presumption in Section 3(f)(2) of the Act creates an important incentive to use strong security safeguards, including encryption and data minimization techniques, but also has the effect of preventing notification when security breaches occur. It is unclear, for example, how this presumption will be challenged if there is no notification to the party or to the FTC when a breach occurs. A partial solution would be to require the (a)(2) notification to the FTC with an explicit designation that the specified security standards were in place. This would fulfill several goals: provide some form of notification, create the appropriate presumption for the use of good security techniques, and enable the FTC to further investigate if necessary.

Transparency

On a related point, there is an unnecessary amount of secrecy surrounding the obligation to notify the Commission in Section 3(a)(2). As the bill is drafted, the companies will notify the Commission but the Commission will only make the information available to the public when it "would be in the public interest or for the protection of consumers." This leaves too much discretion with the agency, and will also make it difficult to evaluate long terms trends and key problems by preventing access to routine reporting about security breaches.

The better approach is to simply make information about security breaches available to the pubic. Section (a)(1) will still have the intended effect of ensuring the target population is affirmatively notified. Section (a)(2) will now ensure that the information about security breaches is generally available to the public.

Making data publicly accessible will have the additional benefit of providing information in ways that are compatible with the President's goals of making government information more accessible and useful to the public. It is conceivable, for example, that better tracking of security breach incidents, combined with other data sources, will make it easier for security researchers to detect problems and find solutions. "Mash-ups" could help identify related problems. Further, longitudinal data is always useful to determine long-term trends, such as the FTC's own findings about the growing problem of identity theft. But none of this will be possible if the data provided to the FTC in the event of a security breach is not made available to the public.

H.R. 1319, The Informed P2P User Act

Mr. Chairman, I would like to make a few remarks about H.R 1319, the Informed P2P User Act. The purpose of the bill is to make people aware, who might not otherwise be aware, of some of the risks of P2P file sharing. The bill as drafted would require a person who seeks to make another computer available for file sharing to inform that person and also to make known, before activation of the file sharing function, the files that will be made available for file sharing, The Act further prevents a person from trying to prevent the owner of the target computer from taking reasonable efforts to disable file sharing functionality.

P2P networks also have certain functionalities that are not found in the traditional client-server architecture of the Internet. For example, P2P networks make it possible to make more efficient use of bandwidth, as well as providing some protection against failure, as there is no single point of failure that would exist in a hierarchical network or one that relies on a central directory.

At the same time, recent vulnerabilities in P2P networks have raised understandable concerns about the reliability of some of the applications. The vulnerability of a poorly installed network is substantial as a user essentially leaves the files on his or her computer vulnerable to access by anyone on the file-sharing network. This matter was brought to the attention of the Committee in the recent exchange concerning Lime Wire.

In the consideration of this bill, it is important to understand that P2P programs are used for a wide variety of function from the sharing of music to Internet-based telephony as well as scientific research. Even the military makes use of P2P networks. The technique is also important in countries where Internet censorship is a threat,

In the most generic sense, a P2P network is a technical description, much like saying a telephone network or the Internet. It is no intrinsic application, other than architecture that allows nodes to exchange information equally with other nodes in the network. Some Internet scholars have observed that this architecture reflects the collaboration among individuals that has helped spur the growth of the Internet. Professor Yochai Benkler refers to this as "Commons Based Peer Production."

No doubt part of the bill aims to discourage the use of file sharing techniques that may infringe copyright as well as making users vulnerable to certain types of inadvertent file sharing. But there is some risk that the bill would also discourage the use of file sharing techniques that do not raise such concerns. More generally, it appears to be posting a warning sign on a very wide variety of applications that most likely have little to do with the sponsor's concern.

I do think that if legislation is adopted of this type for file sharing in P2P networks, it may also be appropriate to adopt legislation for the use of persistent cookies by advertising networks. These techniques also raise privacy concerns for individual users and at present there is no notice provision comparable to that proposed in H.R. 1319 for these particular tracking techniques. Moreover, the decision to place a persistent cookie on another user's computer without that user understanding the consequences or making an informed decision to accept the cookie raises several troubling privacy concerns, including the possibility of tracking the user's online activity. While there are many circumstances under which persistent cookies enable useful functionality, users should be given notice and full opportunity to consent, or to disable the tracking features if they so choose.

We would be pleased to work with the committee both to ensure that the key concern in the P2P file notification is addressed as well as to expand the bill's coverage to address the related problem of persistent cookies.

Conclusion

Data breaches remain one of the greatest concerns for Internet users in the United States. Many companies have poor security practices and collect far more information than they need or can safeguard. But since there are few consequences

for poor security practices, they can obtain all the value from the user data and leave it to others to deal with the consequences. This clearly needs to change.

Companies need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences. Legislation for information security and breach notification is needed, but it should not preempt stronger state measures and it should not rely solely on FTC rulemaking authority. My comments today suggest several steps that might ensure that the legislation is effective, takes advantage of new Internet-based services, and has the flexibility to evolve as new challenges arise.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

Mr. RUSH. The chair now recognizes Mr. Boback for 5 minutes.

STATEMENT OF ROBERT BOBACK

Mr. BOBACK. Chairman Rush, Ranking Member Radanovich and distinguished members of the committee, I thank you for giving us the opportunity to testify here today.

As many of you discussed in your opening statements the security risks associated with peer-to-peer, our company, Tiversa, which I am the CEO of, has unique insight on this in that Tiversa has the unique technology that allows us to span out globally to see all information that is occurring on all the peer-to-peer clients, so it is just a Lime Wire or a Kazaa or a BearShare, it is everyone, all encompassing, and we see it in real time. So therefore this provides us a great insight to provide information to the committee here today.

This information that we are finding is very sensitive. There are security measures. I commend the Honorable Ms. Bono Mack for bringing this here today. The reason why is that many security professionals around the world in high-ranking positions in corporations in the United States and abroad aren't even aware of this, so again, for her insight to bring this to the committee and bring 1319 forward, it is very important, because, again, the awareness is still not where it needs to be. For instance, in the last 60 days, despite the measures that have been taken by the peer-to-peer clients, despite which I also admit are improving, Lime Wire is improving its protocols to decrease the amount of breaches that have happened, but in the last 60 days Tiversa has downloaded breaches in the amount of 3,908,000 breaches, individual breaches in the last 60 days. I find it very important that 2221 and 1319 are actually discussed on the same day. The reason why is, this is where breaches are happening. As Mr. Gingrey of Georgia called out, obviously we all saw the Wall Street Journal article April 21st about the Joint Strike fighter. It wasn't reported in the Wall Street Journal, this was peer-to-peer. The information unfortunately is still on the peer-to-peer. This was discovered in January 2005. We discovered it. We reported it to the DOD. It is still here. It is still out there. It has never been remediated. Awareness is not where it needs to be. Oversight is not where it needs to be in order to address these problems. That is the type of national security ends.

Now, there are also the consumer ends. From Tiversa, we process 1.6 billion searches per day every day. Google is about 1.7 billion per day, so we were about nine times what Google is processing on a daily basis. In those searches we are able to see what the users are looking for around the world, and in those searches we see people searching for your financial records. They are not looking to apply for a credit card. They are not looking for health insurance. They are looking for your health insurance because they want to quickly go online and buy online pharmaceuticals using your medical insurance card as medical identity theft. No credit monitoring will stop that. They want to get your Social Security number filed with your tax return. We did a study with the Today show showing that in that instant 275,000 tax returns were found in one search on the peer-to-peer, so a minimum of 275,000 Social Security numbers on one time. Now, we have done other searches where it has

been over half a million on one time and yet I would also strongly urge the FTC that on the website where it would identify to users that this information is coming from the peer-to-peer, there is not one mention of peer-to-peer on where are they getting your information. Nine million victims every year of identity theft and the number one mention on the FTC's website is dumpster diving. It doesn't add up. The numbers don't add up to dumpster diving. Consumers are not aware of this problem, not from a national security standpoint. Executives don't know it. Security executives do not know this problem. Consumers aren't aware of this problem. They need to know that their information is out there and it is being sought after on an enormous scale such that even in our research in the last few months we have had a 60 percent increase in searches for information that will lead to identity theft and fraud. This is a serious growing problem that consumers again are not aware of, so we applaud 2221 for a national breach. I will tell you that as we find these breaches, these 3,900,000 breaches, as we can we return the information and alert the companies to the breach. Again, we do it out of our duty of care policy. There are no strings attached to that.

I will tell you that there are thousands of cases that our employees have provided to users, to companies nationwide that they completely disregard the breach. Many of those are actually cited in my written testimony, so you would think that you are safe if you do not use peer-to-peer. Well, I will show you in the written testimony there are users out there that all they did was go to the hospital and they provided their information there and now that is one of the things, so individuals need to have an identity theft protection service as well as a national breach notification such as 2121, and I thank you for the opportunity and welcome questions.

[The prepared statement of Mr. Boback follows:]

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009

TIVERSA

Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

As P2P file-sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer-to-peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer-to-peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

1 – Planned file sharing – its intended use.
2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads a P2P software program on his/her parents computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port-scanning, policies, etc, simply do no effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

> *"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."*

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previ-

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 credit card numbers
a&l credit card
aa credit card application
abbey credit cards
abbey national credit card
ad credit card authorization
april credit card information
athens mba credit card payment
atw 4m credit card application
austins credit card info
auth card credit
authorization credit card
authorization for credit card
authorize net credit card
bank and credit card informati
bank credit card
bank credit card information
bank credits cards passwords
bank numbers on credit cards
bank of america credit cards
bank of scotland credit card
bank staffs credit cards only
barnabys credit card personal
bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately $35. This is up from approximately $8-$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS's system as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

letter for medical bills
letter for medical bills dr
letter for medical bills etmc
letter re medical bills 10th
ltr client medical report
ltr hjh rosimah medical
ltr medical body4life
ltr medical maternity portland
ltr medical misc portland
ltr orange medical head center
ltr to valley medical
lytec medical billing
medical investigation
medical journals password
medical .txt

medical abuce records
medical abuse
medical abuse records
medical algoritms
medical authorization
medical authorization form
medical autorization
medical benefits
medical benefits plan chart
medical biliing
medical biling
medical bill
medical biller resume
medical billig software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at $1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

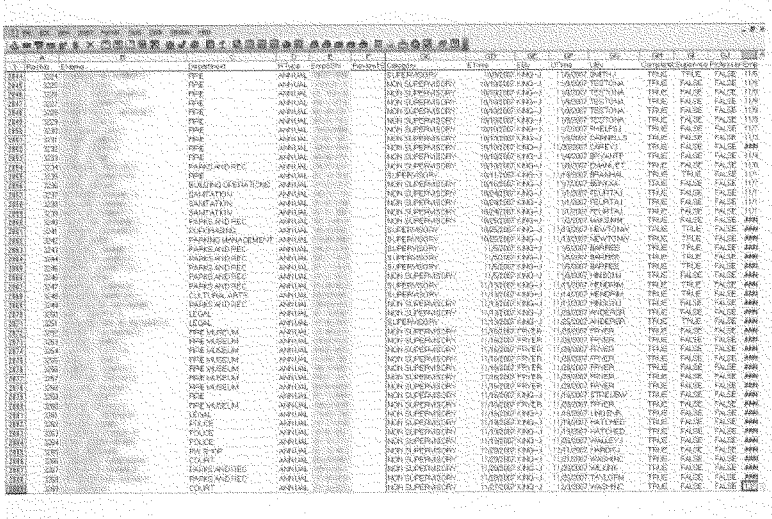
As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

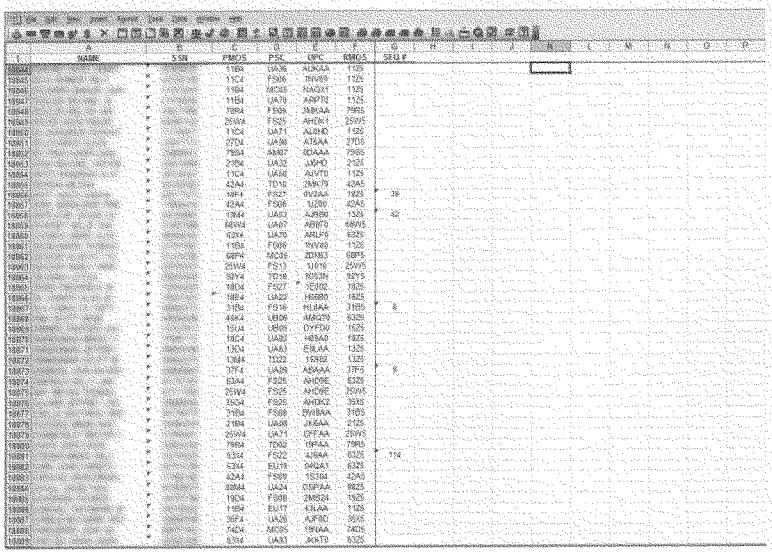
Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

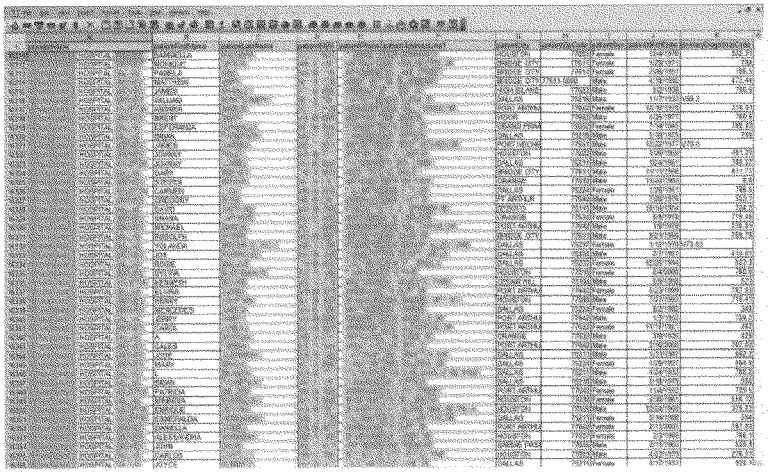
Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

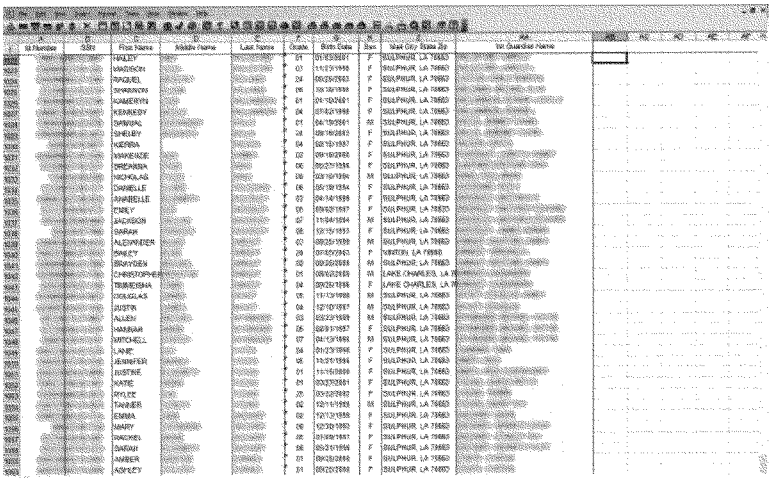
Examples to follow on subsequent pages...

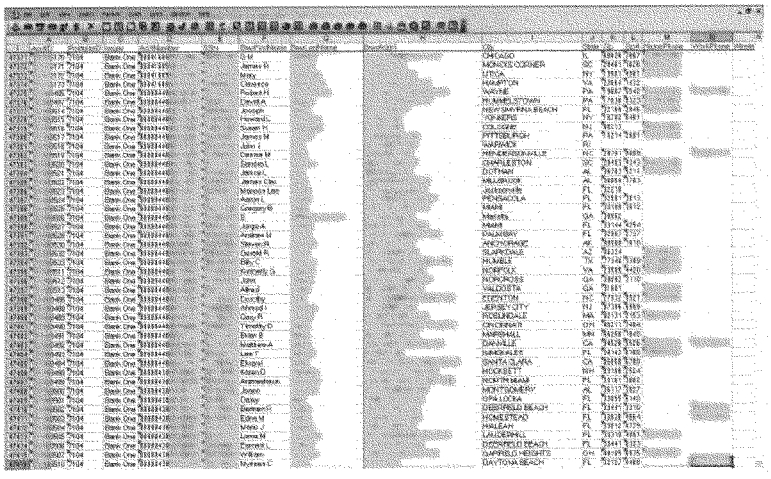


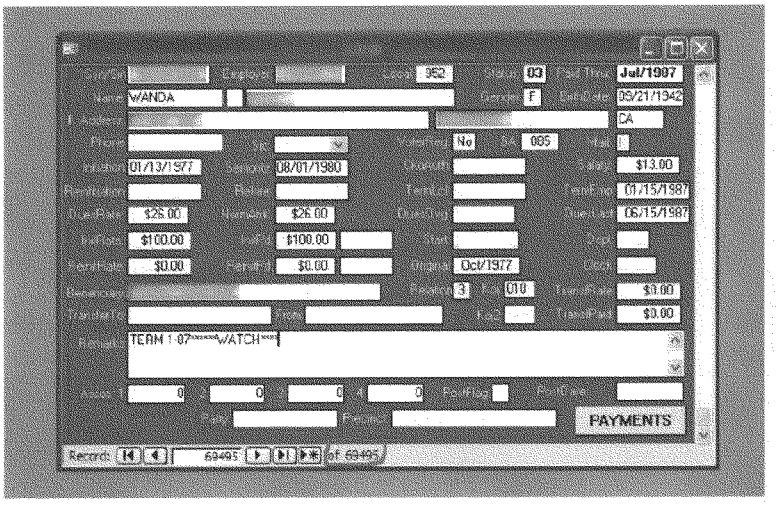




	A	B	C	D	E	F	G	H
4	Last	First	SSN	Taxable?	Degree	School	Major	Division
1000	[illegible]	John	[illegible]	N	Certificate	CFA Institute	CFA	Eastern
1001	[illegible]	Zishan	[illegible]	N	Graduate	NYIT	MBA	Western
1002	[illegible]	David	[illegible]	N	Certificate	CFA Institute	CFA	Western
1003	[illegible]	Anthony	[illegible]	N	Graduate	Stevens Institute	MIS	Eastern
1004	[illegible]	Melissa	[illegible]	N	Certificate	Dowling College	CFP	Eastern
1005	[illegible]	Thomas	[illegible]	N	Certificate	Pace	CFP	Eastern
1006	[illegible]	Mary Linley	[illegible]	N	Certificate	American College	CFP	Eastern
1007	[illegible]	Samuel	[illegible]	N	Certificate	Kaplan University	CFP	Eastern
1008	[illegible]	Sandeep	[illegible]	N	Graduate	Steven Institute	Info Mgmt sys	Eastern
1009	[illegible]	Emmee	[illegible]	N	Certificate	Kaplan	CFP	SouthWest
1010	[illegible]	Scott	[illegible]	N	Certificate	Kaplan	CFP	Western
1011	[illegible]	Darya	[illegible]	N	Undergrad	Montclair State University	Marketing	Eastern
1012	[illegible]	Isaac	[illegible]	N	Certificate	Pace University	CFP	Eastern
1013	[illegible]	Sotland	[illegible]	N	Certificate	Kaplan	CFP	Eastern
1014	[illegible]	James	[illegible]	N	Certificate	Kaplan	CFP	Eastern
1015	[illegible]	Steven	[illegible]	N	Graduate	University of Connecticut	MBA	Eastern
1016	[illegible]	Michael	[illegible]	N	Graduate	Stevens Ins	MIS	Eastern
1017	[illegible]	Alejandra	[illegible]	N	Degree	Pace University	BA	Eastern
1018	[illegible]	Hasan	[illegible]	N	Undergrad	NYU	International MBA	Eastern
1019	[illegible]	Snah	[illegible]	N	Undergrad	Stevens Institute	MIS	Eastern
1020	[illegible]	Luis	[illegible]	N	Undergrad	Axis College	BA	Eastern
1021	[illegible]	Jared	[illegible]	N	Certificate	Kaplan	CFP	Eastern
1022	[illegible]	Matthew	[illegible]	N	Undergrad	Brooklyn College	Finance	Eastern
1023	[illegible]	Francisco	[illegible]	N	Certificate	CFA Institute	CFA	Eastern
1024	[illegible]	Belinda	[illegible]	N	Undergrad	Universidad	Accounting	PR







Insurance Aging

INCORPORATED

JOHN J. Date of Birth: 8/29/1945 Insured: Self
Insurance: Primary ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
			05/01/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			12/17/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			04/30/2007	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Patient Total:				220.00	0.00	0.00	0.00	0.00	220.00	220.00
Insurance Total:				379.16	0.00	0.00	0.00	147.75	231.41	379.16

TIMOTHY L. Date of Birth: 02/21/1945 Insured: Self
Insurance: Primary Group Number: 00001922 ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
210464	02/17/2006	97086/97084	09/08/2006	41.00	0.00	0.00	0.00	0.00	41.00	41.00
			09/19/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			12/08/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Patient Total:				41.00	0.00	0.00	0.00	0.00	41.00	41.00

DANNY T. Date of Birth: 01/15/1946 Insured: Self
Insurance: Primary Group Number: 00000905 ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
203365	06/19/2006	97086/97084	09/08/2006	41.00	0.00	0.00	0.00	0.00	41.00	41.00
Patient Total:				41.00	0.00	0.00	0.00	0.00	41.00	41.00
Insurance Total:				82.00	0.00	0.00	0.00	0.00	82.00	82.00

BEN Date of Birth: 11/28/1935 Insured: Self
Insurance: Secondary ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25-4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the $300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and protection of those most affected, the consumers.
We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the file-name and meta-data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

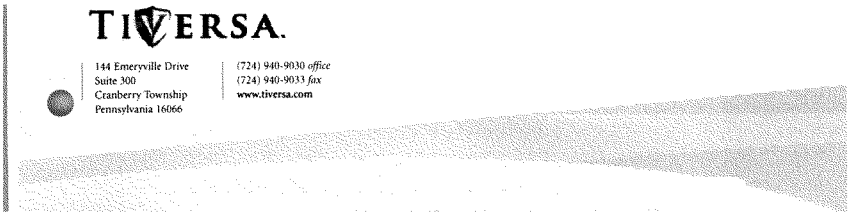
In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.


TIVERSA.
144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066
(724) 940-9030 office
(724) 940-9033 fax
www.tiversa.com

Mr. RUSH. Thank you very much. Now the chairman recognizes Mr. Sydnor. Mr. Sydnor, you are recognized for 5 minutes for opening statement.

STATEMENT OF THOMAS D. SYDNOR

Mr. SYDNOR. Thank you, Chairman Rush, Ranking Member Radanovich and members of the subcommittee. My name is Thomas Sydnor and I am a senior fellow at the Progress and Freedom Foundation. I am here speaking today on my own behalf, and I am also the author of two studies on the causes of inadvertent file sharing, File-Sharing Programs and Technological Features to Induce Users to Share, published by the United States Patent and Trademark Office, and Inadvertent File Sharing Revisited, published by the Progress and Freedom Foundation, and I am here today to testify in support of H.R. 1319, the Informed Peer-to-Peer User Act.

Mr. RUSH. Mr. Sydnor, would you please excuse me just for a moment? I want to alert the members that there is a little over 5 minutes for a vote, a three-series vote. There are three votes in the series, and that will be the last votes of the day. So if members want to leave to go and vote after this witness completes his opening statement, then the chair will recess the committee and reconvene at the conclusion of this series of votes. So we would ask that the members please return promptly so that we can complete the questioning of these witnesses and complete this hearing.

Mr. Sydnor, would you please continue?

Mr. SYDNOR. Thank you, Mr. Chairman.

I am testifying today in support of the bill because my written statement and my past published work on inadvertent sharing I think shows that in the past we have tried to rely on voluntary self-regulation and it has failed. Voluntary self-regulation should be an incredibly important part of our technology policy and for that reason it must be taken seriously. Unfortunately, in the context of distributors of filing sharing programs used mostly for unlawful purposes, it has been tried, voluntary self-regulation. It has failed miserably in the past, and I can report that it is failing again right now.

I want to consider just as an example the file-sharing program Lime Wire 5. The DCIA has hailed Lime Wire 5 as the gold standard for the implementation of its new voluntary best practices, and Lime Wire itself has a result of this hearing generated great publicity for itself by telling Congress that at long last Lime Wire 5 put the final nail in the coffin of inadvertent sharing of sensitive files, and the program is that last statement is not even arguably correct, and to show why, I want you to consider a hypothetical based upon the recent reports from Today Investigates showing that in New York State alone researchers could find over 150,000 inadvertently shared tax returns. The report also showed the real-world consequences of inadvertent sharing by profiling the Bucci family, who had their tax returns stolen by an identity thief because they had inadvertently shared their tax returns because their preteen daughters were using a file-sharing program reported to be Lime Wire. But the real problem in such a case is that a tax return is really only the tip of the iceberg. Such episodes usually

occurring mean that a family is sharing all of its personal data file stored on the family computer. All the parents' work and personal documents, scans of legal, medical and financial records, scanned documents providing identifying information about the family's children, all of the family's digital photos, all of its home videos, entire music collection, probably thousands of files.

Now, consider two families that have been affected by this type of catastrophic inadvertent file sharing, and just assume it was caused by an earlier version of Lime Wire. Consider what happens if they upgrade to Lime Wire 5. One family doesn't know they have a problem. They are unaware that a problem exists but they hear reports like Lime Wire 5 has ensured the complete lockdown of the safety and security of Lime Wire users and so they upgrade to Lime Wire 5. Will that correct their inadvertent sharing of sensitive documents problem? It will not. By default, simply by being installed, the family will continue to share documents that are by any a reasonable definition sensitive. They will continue to share the family photo collection. They will continue to share scanned legal, medical and financial records, perhaps even tax returns, continue to share data about their children. They will continue to share all their home videos. They will continue to share their entire music collection. So they will continue to be exposed to the full range of risks: identity theft, data on their children getting into the hands of the pedophiles that use their networks, and the risk of a lawsuit.

Now, the other family does know their problem. They detect it and they resolve it by uninstalling Lime Wire, remove it from their computer. So this family actually has put the final nail in the coffin of their inadvertent file-sharing problem but they hear about Lime Wire, they kids reinstall it because now it is completely secure. What will happen? By default, simply by being installed, that program will revive, will call back from the dead the family's inadvertent file-sharing problem. It will automatically begin re-sharing all the data files that were shared before except for some types simply by being installed. That is not acceptable behavior, it is not acceptable practice, and I think it indicates why the committee should be commended for its work on H.R. 1319. Thank you.

[The prepared statement of Mr. Sydnor follows:]

Prepared Statement of
Thomas D. Sydnor II,
Senior Fellow and Director for the Center for the Study of Digital Property,
Progress & Freedom Foundation

"Legislative Hearing on H.R. ___, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act"

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
United States House of Representatives
Washington, D.C.

May 5, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, I am Tom Sydnor, a Senior Fellow and the Director of the Center for the Study of Digital Property at the Progress & Freedom Foundation, a non-profit research foundation dedicated to studying the public-policy implications of technology. I am also the lead author of two empirical studies that focus on the causes of what has been called "inadvertent file-sharing." Both studies seek to answer one simple question: "Why do so many users of certain types of 'peer-to-peer' file-sharing programs end up 'sharing' types of files that no informed user would ever deliberately 'share'?"

I would like to thank the Subcommittee for holding this hearing, and I would like to thank the sponsors of H.R. 1319, The Informed P2P User Act, for proposing a thoughtful and moderate solution to the serious and protracted problem of inadvertent file-sharing. My support for the Act is based upon my analysis of three critical questions that it seems to raise.

First, should Congress legislate to deter inadvertent sharing, or can Congress assume that inadvertent sharing will be remediated because distributors of file-sharing programs like LimeWire can be trusted to abide by the Voluntary Best Practices developed in mid-2008 by the Distributed Computing Industry Association? Here, I think that the answer is clear: "No": This approach was tried in 2003; multiple distributors violated their own self-regulatory *Code of Conduct* repeatedly, and the consequences were disastrous for consumers, for commerce and for the country.

Second, could the Act's substantive requirements improve upon existing legal mechanisms for deterring inadvertent sharing? Here, I think that the answer is "yes": the Informed P2P User Act improves upon existing law because its substantive requirements can narrowly and rather gently target the critical problem: because *certain* file-sharing programs are used almost exclusively for unlawful purposes, we should ensure that their users—many of whom are preteen or teenage children—must *once again* act deliberately before they "share" files that might be dangerous for them to distribute.

Third, can the Act's requirements be targeted narrowly toward the appropriate subset of the technologists who have deployed peer-to-peer networking technologies? In other words, should legislators again try to devise some definition of "peer-to-peer" that will target problematic conduct without needlessly burdening legitimate, law-abiding uses of this particular networking technology? Here, I think that the answer is "yes, but...."

The Subcommittee should attempt such efforts. In the past, such efforts have not succeeded, but given the gravity of the stakes, and the lessons taught by the Supreme Court's decision in the *Grokster* conclude, I believe that another attempt would be worthwhile. In particular, I believe that a combination of both technological and result-focused constraints might enable the Subcommittee and the sponsors of H.R. 1319 to devise a broadly acceptable compromise.

But because such efforts might not succeed, I believe that the Subcommittee might also wish to consider a back-up strategy. The Informed P2P User Act improves upon existing law because it narrowly and rather gently targets critical root causes of inadvertent sharing. Nevertheless, Congress has long provided federal law-enforcement agencies with both criminal and civil enforcement authority that, while neither gentle nor narrowly targeted, can surely punish and deter the worst of the abuses that distributors of certain file-sharing programs have—for far too long—inflicted upon children, families, lawful commerce, national security and the rule of law.

The Informed P2P User Act seeks to end years of inexcusable conduct by devising a precision instrument that would narrowly target root causes of inadvertent sharing. But if a precision instrument cannot be made broadly acceptable to law-abiding technologists and thoughtful consumer advocates, then the Committee could, instead, urge federal law enforcement agencies to use their existing hammers to send a message. And should this back-up strategy be accepted, and resort to it required, the rest of my testimony may suggest why the message to be sent must be both forcefully delivered and unequivocal in content.

Given my background, I believe that I may best assist the Subcommittee's legislative efforts by focusing the rest of my written testimony on the first of the three questions that outlined above. Last year, the Distributed Computing Industry Association (DCIA) published a set of Voluntary Best Practices (VBPs) that were intended to help developers of programs and services that use peer-to-peer technologies avoid causing inadvertent sharing. In recent weeks, DCIA's member company, LimeWire LLC, has been telling both the public and Congress that its implementation of the DCIA VBPs in the most recent versions of its program, LimeWire 5 "put the final nail in the coffin of inadvertent sharing of sensitive files."

Such reports could suggest that the Committee should forego resort to legislation and rely, instead, upon further implementation of "voluntary self-regulation" by distributors of file-sharing programs like LimeWire 5. For the following reasons, I cannot advise any Committee of Congress to make *another* attempt to rely on voluntary self-regulation by distributors of certain types of file-sharing programs.

Voluntary Self-Regulation Has Been and Should Be a Critical "First-Resort" Component of Sound Technology Policy.

I believe that voluntary self-regulation should be the policy option of first resort when we encounter problems relating to computer, software, and internet technologies. Simply put, innovation is an inherently uncertain process in which missteps and mistakes are inevitable. Were Congress and regulators to react to each misstep by imposing stringent, prescriptive laws and regulations, the innovation that could drive our Information-Age economy toward recovery could be seriously impeded by constraints that could quickly become outdated, ineffectual, or market-distorting.

But precisely because voluntary self-regulation must be central to our innovation policy, entities who pledge to voluntarily self-regulate must take their self-imposed duties seriously. Consequently, voluntary self-regulation has three important components: 1) credible self-regulators; 2) meaningful self-regulations; and 3) reasonable implementations of the self-regulations.

When the circumstances of this situation are compared against the requirements for viable self-regulation, none appear to be clearly satisfied: 1) one critical self-regulator seems to have repeatedly proven itself to be untrustworthy; 2) in critical respects the VBPs provide only vague or inappropriate guidance; and 3) the implementation of the VBP's by the distributors of the LimeWire file-sharing program seem to reflect flaws so serious as to—again—raise questions about the integrity of its implementation process.

Under such circumstances, those of us who favor voluntary self-regulation should concede that the only question remaining is which branch of the government should act, and how. I will address each of these concerns—credibility, regulations, and implementation—in that order.

Few potential self-regulators are less credible than LimeWire LLC: generally, questions about voluntary self-regulation arise only *after* a problem has occurred. Consequently, sound public policy dictates that even entities and industries that have made serious errors should be able to qualify as potentially viable self-regulators. Nevertheless, at some point, misconduct can become so seemingly culpable, so egregious, or so frequent as to preclude further rational reliance on self-regulation.

Some cases may present fine questions about whether these lines have been crossed. But this is not one of them. The entity whose behavior is probably most critical to the efficacy of the DCIA VBPs is LimeWire LLC. I have described in detail aspects of LimeWire's previous conduct in my two prior papers on inadvertent sharing. Today, I only wish to highlight one episode to illustrate a larger pattern of conduct that should tend to discredit this potential self regulator. As a result, I want to describe the history of the deployment of a feature called a "search wizard" in the file-sharing programs KaZaA and LimeWire.

A "search wizard," as that term is used here, activates only the first time that a given program is installed on a given computer. When activated, it scans a computer's hard drive(s) and "recommends" that the new user recursively share certain folders identified by the distributors of the program as folders that a new user might want to share. Search-wizards actually deployed

tended to "recommend" that new users should share all, or almost all, of the files in their "My Documents" folder and all of its subfolders. Users accepting this "recommendation" would thus share almost all of their personal files—including their entire music collection: all of the audio files ripped from purchased CDs.

In retrospect, the existence of search wizards seems difficult to explain for two reasons. First, search wizards target new users—and new users of file-sharing programs will tend to be preteen and teenage children. Second, a search wizard that urges children to recursively share the "My Documents" folder of the family computer seems inexcusable. No one who understood the probable consequences should agree to share all the files in their *My Documents* folder and all of its subfolders. Consequently reasonable program developers should never have released programs that delivered such "recommendations" to their most vulnerable users.

But they did. Search wizards were deployed in many popular file-sharing programs, and some distributors of some file-sharing programs (like LimeWire) actually *began* deploying search-wizards *after* their self-evident consequences had been confirmed and condemned by computer-science research, by both Houses of Congress, and by the *Code of Conduct* developed by distributors of file-sharing programs including LimeWire LLC. The following search-wizard chronology makes this point:

> **June of 2002**: In *Usability and Privacy, A Study of KaZaA Peer-to-Peer Filesharing*, computer-science researchers from HP Labs conclude that two "features" in the KaZaA file-sharing program, including a search-wizard, were causing users to share so many sensitive files inadvertently that identity thieves had begun data-mining file-sharing networks for inadvertently shared credit-card numbers. Distributors responded by continuing to deploy search wizards.
>
> **June of 2003**: A year later, hearings on inadvertent sharing held by the House Committee on Oversight and Government Reform and the Senate Committee on the Judiciary caused the distributors of KaZaA., (who were members of DCIA), to belatedly recognize *Usability and Privacy* as "intelligent research," and to promise to remove both of the dangerous features it had criticized.
>
> **July of 2003**: The distributors of KaZaA did remove the dangerous features condemned by *Usability and Privacy* and the hearings, but they did so in an almost inexplicable way: both features, including the search wizard were removed in a way that *perpetuated* all of the consequences of the catastrophic inadvertent sharing that they had already caused.
>
> **September of 2003**: The distributors of LimeWire and other programs responded to the congressional hearings on *Usability and Privacy* by promulgating a self-regulatory *Code of Conduct* that should have precluded use of KaZaA-like search wizards. They declared, "[Our] software and associated user instructions … shall be designed to reasonably prevent the inadvertent designation of the content of the user's … principal data repository … as material available to other users."
>
> **Fall of 2003**: Copyright owners begin suing users of file-sharing programs "sharing" hundreds or thousands of infringing files. Published research found that such enforcement caused most users to drastically reduce the number of files that they shared, but oddly, a few kept on sharing hundreds of infringing files—almost as if they did not realize that they were sharing files at all.

January of 2004 (approximately): The distributors of LimeWire deployed a KaZaA-like search-wizard in their program. Like the KaZaA search wizard, it tended to recommend that new users should share their "My Documents" folder and all of its subfolders. Unlike the KaZaA search wizard, its "recommendations" appeared automatically during a default installation of LimeWire.

August of 2004: Predictably, LimeWire's more aggressive search wizard quickly caused catastrophic inadvertent sharing. Consequently, a reporter from the Boston Globe soon asked LimeWire LLC why its users were sharing classified military data. A LimeWire representative cited its search wizard: "One possible weakness in LimeWire is a feature that automatically scan the user's hard drive, looking for files to be shared over the network. [The representative] said this feature can make it easy to expose private information by mistake." Nevertheless, LimeWire kept on deploying the search wizard.

March of 2007: the United States Patent & Trademark Office published an empirical analysis of five popular file-sharing programs entitled *Filesharing Programs and Technological Features to Induce Users to Share*. It specifically criticized LimeWire for violating its own *Code of Conduct* by deploying a search wizard. LimeWire kept on deploying its search wizard.

June of 2007: The House Committee on Oversight and Government Reform, following up on its own 2003 hearing and the USPTO report, asked LimeWire to explain why it was it had, and was still, deploying a search wizard. LimeWire declined to explain, but it did—finally—remove the search-wizard feature from its program. But like KaZaA in 2003, LimeWire removed the search wizard in a way that happened to *perpetuate* all inadvertent sharing it had previously caused.

I do not purport to see how the conduct described above—which was part of a larger pattern—can be easily attributed to good faith or even repeated negligence. Some might argue that it could reflect mere repeated recklessness. Nevertheless, at least to an outsider like me, it seems difficult to deny the possibility that it reflects the results of *deliberation*: an intent to deploy a known means of directing absurdly dangerous guidance towards a program's most vulnerable users in order to cause them to share files inadvertently.

Fortunately, for present purposes, debates about repeated-recklessness versus deliberate-wrongdoing are irrelevant. In either case, history has discredited LimeWire LLC as a viable self regulator: we conducted that experiment, and the results were disastrous and unequivocal.

Critical components of the DCIA VBPs are necessarily vague or ill-suited when applied to particular programs: in theory, sufficiently prescriptive Voluntary Best Practices might reduce concerns about the character of the entities that must implement them. But in practice, the DCIA VBPs should not do so. For example, DCIA or others may criticize the Informed P2P User Act because its *initial* version prescribes a set of principles applicable to *all* uses of peer-to-peer networking—from the most inherently unobjectionable to the most inevitably unlawful. But if so, the same critique applies even more forcefully to the *final* version of the DCIA VBPs: they also try to prescribe rules of conduct for applications so diverse that critical components of the resulting "best practices" inevitably suffer from one of two limitations.

First, some "best practices" simply lack meaningful content because no specific "practice" could be "best" as applied to the whole range of applications governed by the VBPs. For example, perhaps the most critical provision of the VBPs requires developers to disable sharing of "sensitive" files by default. Yet no meaningful definition of "sensitive is provided and none could be: the set of files that would be "sensitive" to share using a given program could vary enormously. On a "closed" network that will distributed only authorized, authenticated files, no file types might be "sensitive." On a network like Gnutella, there would appear to be few file types that would not tend to be potentially harmful to share.

Second, and conversely, some "best practices" may make no sense as applied to some programs. For example, the VBPs presume that files downloaded by a user of any file-sharing program are never "sensitive" and thus inevitably safe to "share" by default. As applied to a program like LimeWire, I am aware of no evidence that would suggest that it would be safe for a user to "share" the types of files that users typically download.

Neither of these limitations suggest that the DCIA VBPs reflect a dishonest attempt to redress inadvertent file sharing. But they do suggest that the utility of the VBPs will depend heavily upon the good faith and common sense of the entities implementing them. To an entity trying to act responsibly, the VBPs could provide useful guidance. But to a negligent, reckless or willful entity, the VBPs could provide loopholes and excuses. Consequently, it is important to examine how the VBPs were implemented by LimeWire LLC in LimeWire 5.

The implementation of the VBPs in LimeWire 5 actually *perpetuates* some of the worst inadvertent sharing of sensitive files caused by previous versions: DCIA has praised LimeWire 5 as a "poster child for compliance" with its VBPs. But LimeWire's "compliance" seems rather cynical. In effect, LimeWire concluded that the VBPs let it remediate those consequences of inadvertent sharing that were clearly hurting both LimeWire users *and LimeWire LLC*—but *perpetuate* those consequences of inadvertent sharing that hurt users, but potentially benefited LimeWire LLC.

Moreover, those convenient results should have followed only if LimeWire could have reasonably concluded that a family's digital photos, its home movies, its entire music collection, and all of its scanned documents, like tax returns, are not "Sensitive File Types" when broadcast over a Gnutella file-sharing network known to be used by identity thieves and pedophiles. Because those conclusions do not seem *reasonable*, serious problems seem to affect the implementation of the VBPs in LimeWire 5.

LimeWire LLC began promoting the availability and advantages of LimeWire 5 after alert reporters documented the latest debacle that that distributors of file-sharing programs had inflicted upon the public: a report by Today Investigates revealed that the residents of New York state alone were inadvertently sharing over 150,000 tax returns. This report also profiled the Bucci family—identity theft victims who had inadvertently "shared" their tax return because their preteen daughters had downloaded and misconfigured LimeWire.

LimeWire responded by assuring its users that upgrading to LimeWire 5 would halt inadvertent sharing without resort to the rash delete-LimeWire-right-now strategy used by the Bucci family:

> "[a LimeWire spokesperson] said, 'Our newest version, LimeWire 5.0, by default cannot share sensitive file types such as spreadsheets or documents. In fact, the software can not share any file or directory without explicit permission from the user."
>
> "With LimeWire 5, the latest version of the software, 'LimeWire has ensured the complete lockdown of the safety and security of LimeWire users, said [Lime Group CEO] Gorton.'"

Unfortunately, widely repeated statements like these appear to be potentially misleading. And worse yet, LimeWire LLC may have known that.

For example, consider the claim that LimeWire made to LimeWire-using families who happened to be mere *constituents* of U.S. Representative Edolphus Towns: "[LimeWire 5] can not share any file or directory without explicit permission from the user." But when making claims to the Representative himself—who happens to be the Chairman of the House Committee on Oversight and Government Reform—LimeWire *added* a critical caveat: "for new LimeWire users, LimeWire 5 does not share *any* file of *any* type without explicit permission from the user."

The Chairman and his constituents were thus told different stories about how LimeWire 5 affects its users. Ordinary families who might have deleted LimeWire could have concluded that if they upgraded to LimeWire 5, then "the software can not share any file or directory without explicit permission from the user." But the Chairman was told that such benefits would accrue *only* to brand new users of LimeWire 5—not to users of previous versions of LimeWire who upgraded to LimeWire 5.

So it is *almost* déjà vu all over again: in 2003, a DCIA member-company distributing the file-sharing program KaZaA "remediated" catastrophic inadvertent sharing by perpetuating its effects. In 2009, a DCIA member-company distributing the file-sharing program LimeWire "remediated" catastrophic inadvertent sharing by perpetuating *some of its effects*—the subset that could materially benefit the Gnutella file-sharing network, albeit at the expense of common sense and user safety. Consequently, were a family like the one profiled by Today Investigates to try to resolve their inadvertent file-sharing problem by upgrading to LimeWire 5, that family would probably keep "sharing" many files that are clearly "sensitive" within any reasonable definition of that term—perhaps even their tax returns.

To understand what has happened, and why it might have happened, one need only understand a bit about the harm that catastrophic inadvertent sharing can inflict upon families, and the potential benefits that it could confer upon the distributor of a file-sharing program used mostly to download unlawful copies of popular music, popular movies, and "adult" images.

When inadvertent sharing affects people like the family profiled by Today Investigates, disclosure of a tax return is almost surely just one symptom of a much broader problem. It is very unlikely that families "share" a tax return because an adult decided to store it in the hard-to-access default "Shared" folder created by programs like LimeWire. Consequently, the over

150,000 tax returns being inadvertently shared *in one state alone* are probably being shared along with *all* files that a family has stored on its home computer in its *My Documents* folder and all of its subfolders. In my 2007 testimony to the House Committee on Oversight and Government Reform, I explained what could happen to my family were a cousin or babysitter to inadvertently and recursively share the *My Documents* of our family computer:

> I would end up sharing bank statements; tax returns; passwords for investment accounts; scans of legal, medical, and financial records; all my family photos; my children's names, addresses, and Social Security numbers; and a scan of the sign that designates the car authorized to pick up my daughter from preschool. And I would also share over 3,000 copyrighted audio files. With one mistake, I could be set up for identity theft, an infringement lawsuit, or far worse.

Ironically, the files that could inflict the worst harm if "shared," (the image files that could endanger my children and the document files that could end my career), seem to confer no real benefits upon a distributor of a file-sharing program. As LimeGroup CEO Mark Gorton testified in 2007, the only two "major use[s]" of his program are downloading music and downloading movies. And he might have added, *popular* music and videos, because, as a LimeWire developer has noted: "here's modern p2p's dirty little secret: it's actually horrible at rare stuff." Moreover, in addition to these two "major" uses, there is also a third potentially material use: downloading image files. Most are probably "adult" images, but infringing images of the "box" art on popular CDs and DVDs are also traded.

Interestingly, when existing LimeWire users upgrade to LimeWire 5, the program will *perpetuate* any inadvertent sharing of at least three categories of files: audio files, video files, and image files. Moreover, actually *using* LimeWire 5 to download a file can also cause inadvertent sharing: by default, LimeWire 5 shares most downloaded files without any "express permission from the user." So LimeWire did not misstate the behavior of its program when it told Chairman Towns that "for new LimeWire users, LimeWire 5 does not share *any* file of *any* type without explicit permission from the user." But it did fail to note that this happy state probably ends when the average user downloads a file.

One can easily see why the interests of the developer of a Gnutella-based file-sharing program that had caused widespread, catastrophic inadvertent sharing would be served by "remediation" efforts that perpetuated all previously caused inadvertent sharing of *existing* media files and could cause future inadvertent sharing of *downloaded* media files. But for the following reasons, it is difficult to see why those should be the results of remediation efforts driven by an informed and genuine concern for the interests of users, their families and employers, and the public.

Image Files: As my 2007 testimony indicated, users who have inadvertently shared sensitive personal files tend to "share" two types of image files. First, they tend to share all of their family photos, and it is certainly not safe or responsible to "share" these over a file-sharing network frequented by pedophiles. Second, consumer copiers and scanners often save scanned files in image-file formats like .tff and .jpg. As a result, were a family affected by inadvertent sharing to have *scanned* tax records stored on its home computer, an upgrade to LimeWire 5 would merely perpetuate its exposure to the identity thieves now data-mining the Gnutella file-sharing network.

Nor is identity theft the worst potential consequence of perpetuating inadvertent sharing of media files. I thought that I had made this clear enough in my 2007 testimony when I described the potential consequences of inadvertent sharing to my family and concluded that we could be "set up for identity theft, an infringement lawsuit, *or something far worse*." Unfortunately, some program distributors seem to have missed the point.

So I let me be even clearer: when I said "or something far worse," I meant that inadvertent sharing of files on my family computer, (including home movies and image files like digital photos and scanned documents), could disclose identifying information about my children to LimeWire-using pedophiles. *See, e.g., United States v. Park,* 2008 U.S. Dist. LEXIS 19688, (D. Neb. March 13, 2008) (a LimeWire user shared videos of an adult raping a little girl "bound with a rope and being choked with a belt"); *United States v. O'Rourke,* 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (a LimeWire user was held to be a "danger to the community" because he allegedly shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged"); *United States v. Postel,* 524 F. Supp.2d 1120, 1123 (N.D. Iowa 2006) (a LimeWire user used shared child pornography to "groom" the girl that he molested for four years).

Sadly, these are risks that LimeWire 5 can perpetuate. Nevertheless, Lime Group CEO Mark Gorton has told the public and Congress that "LimeWire 5 put the final nail in the coffin of inadvertent sharing of sensitive files."

Video Files: Increasingly inexpensive and sophisticated camcorders and video-editing software ensure that many people now archive family movies on their home computers—and these files are not "safe" to "share" for the reasons set forth above. Moreover, to the extent that users also have copies of popular commercial films, these will tend to be copyrighted, and thus not safe to "share" over the Gnutella file-sharing network.

Audio Files: As my 2007 testimony indicated, users who have inadvertently shared sensitive personal files will also tend to be sharing entire music collections—potentially thousands of copyrighted audio files of popular music. These files generally cannot be legally or safely shared, and it is particularly dangerous to share an entire music collection because users sharing hundreds or thousands of audio files are those most likely to be targeted by copyright enforcement actions.

Downloaded Files: At first, early Gnutella-based file-sharing programs had "symmetrical" downloading and uploading capabilities: in other words, just as a user then had to take—and must still take—a voluntary, deliberate act in order to *download* a given file, a user also had to take a voluntary, deliberate act in order to *upload* (or "share") a given file over the Gnutella file-sharing network. Unfortunately, computer-science researchers studied the results and concluded that there was not enough "voluntary cooperation between users" and that developers would have to rely, instead upon "technological features to induce users to share." One of the "features" suggested was automatic sharing of files that users download. As a result, one *knowing* act, a download, can then trigger an *unknowing* act, an upload that could distribute the downloaded file to others.

That default—share downloaded files automatically—is still the default setting for most file types in LimeWire 5. And the problem with that default setting is revealed in the following 2008 testimony given in federal court by a LimeWire developer. He testified, under oath, that "meaningful" default settings are those "set by the programmers" that "make sense and are in the user's best interest."

Hence the problem: programs like LimeWire are used primarily to download infringing copies of media files that are *illegal* to re-distribute. Consequently, a reasonable LimeWire developer should not conclude that a default re-distribution feature is actually in the average user's "best interest." As a practical matter, it simply is not.

Worse yet, because LimeWire 5 still "shares" media files by default, (without any "explicit permission"), and because it perpetuates all prior inadvertent sharing of media files—it seems sure to compromise interests even more important than the federal civil rights called "copyrights" that helped the United States become the world's most successful producer and net exporter of expressive works. Sadly, those interests may include the federal government's ability to protect children from pedophiles.

And this is not a hypothesis. It is not an abstract could-be threat. It is not arm-waving speculation about a theoretical parade-of-horribles. It is a statement about what has happened and what is increasingly likely to happen again. And worst of all, though the facts set forth below were known to LimeWire LLC long before they were known to me, their obvious implications do not seem to be reflected in the design of LimeWire 5.

The design of file-sharing programs like LimeWire and network protocols like Gnutella just so happen to make them attractive to teenage and preteen children who do not want to get caught illegally "sharing" popular music and movies. But for similar reasons, such programs and networks are also attractive to pedophiles who do not want to get caught "sharing" illegal child pornography. As a result, pedophiles have gravitated to the Gnutella network, and a wave of file-sharing-related child-pornography prosecutions is now moving through the federal courts.

Worse yet, some of these defendants are not just alleged viewers of child pornography—they are alleged child predators. When federal prosecutors catch such defendants, they can, of course, charge them with possession of child pornography. But because possession is a rare strict-liability criminal offense, long jail terms are generally not imposed for a conviction.

Consequently, if prosecutors bring criminal charges against a LimeWire user who appears to be, as one court found, "a danger to the community," they may also charge a more serious crime: *knowing distribution* of child pornography. A knowing-distribution conviction can sequester dangerous predators from their potential victims for a long time—*but only if the prosecutor can prove beyond a reasonable doubt that the defendant knew that he was distributing media files containing child pornography.*

Predictably, the task of defending most file-sharers charged with knowing distribution of child pornography falls upon the federal public defenders who serve an essential role in our justice

system and have both a legal and ethical duty to vigorously defend their clients. And those public defenders have realized that inadvertent file-sharing provides a potential complete defense to a defendant charged with knowing distribution of child pornography.

As a result, LimeWire developers are no longer just writing code, they are also testifying in criminal child-pornography cases. Unfortunately, as the following testimony from a March 2008 trial shows, the design of the LimeWire program has ensured that the testimony of LimeWire employees can be as valuable to the defendant as to the prosecution:

> PROSECUTOR: Your Honor, I don't believe it is possible to share files inadvertently.
>
> ***
>
> THE COURT: ... [D]oes your software make it possible make it possible for people to accidentally share personal files or sensitive data?
>
> LIMEWIRE DEVELOPER: Accidentally?
>
> THE COURT: Yes.
>
> LIMEWIRE DEVELOPER. Yes.

While such testimony did not prevent a conviction in this particular case, the difficulty of proving scienter in file-sharing child-pornography cases has already had consequences. For example, in *United States v. Park,* 2008 U.S. Dist. LEXIS 19688 (D. Neb. March 13, 2008), a defendant had used LimeWire to share, *inter alia,* a three-hour video depicting a little girl "bound with a rope and being choked with a belt by what appeared to be an adult male.'" Nevertheless, that defendant secured a reduced sentence because he "lacked an understanding of the software and thus ... the knowledge to distribute the illegal wares that he possessed."

Consequently, for over 14 months, LimeWire LLC has known that unless LimeWire 5 comprehensively foreclosed *any* potential inadvertent sharing *even of mere media files*, it could compromise the ability of prosecutors to sequester dangerous pedophiles from their potential victims. Nevertheless, LimeWire LLC *chose* to design LimeWire 5 so that it would *perpetuate* all inadvertent sharing of all previously shared media files and *continue* to automatically "share" all media files that a user might download.

To conclude, I must note an important point: I do agree that the implementation of the DCIA VBPs reflected in at least *non-beta* versions of LimeWire 5 does seem to make *some* consequential changes that should significantly reduce *some types* of inadvertent file-sharing, including some long known to be very dangerous. These are improvements. Nevertheless, I cannot conclude that these improvements really do signal an overdue-but-now-genuine commitment to "user-safety-first" file sharing. Indeed, in some cases, they seem to reflect little more than the belated admission of the long obvious.

For example, in a May 1, 2009 letter to Chairman Towns of the House Committee on Oversight and Government Reform, Lime Wire LLC heaped glowing praise upon itself because LimeWire 5 now disallows sharing of document file-types by default. But this change can only be welcomed—not praised. After years of countless disasters, Lime Wire LLC has now belatedly conceded that which was obvious to *responsible* developers of file-sharing programs in the year 2000 and that which was *made obvious* to all others in 2002.

In 2000, lawyers who had misread the Supreme Court's famous *Sony* decision began giving developers of file-sharing programs the sort of bad advice later offered in the Electronic Frontier Foundation's infamous "whitepaper": "If your product is intended to work solely as a mechanism for copyright piracy, you're asking for legal trouble.... For example, if you're developing a file-sharing system or distributed search engine, support all file types, not just MP3 or Divx files."

Nevertheless such advice was rejected by the developers of the first popular file-sharing program, Napster. Its developers examined other services that had followed such advice and "often turned up documents from computers whose owners didn't realize that the material could be seen by others." This empirical research convinced Napster's developers that sharing document files by default would be "a big mistake." Joseph Mein, All the Rave 239 (2003). In 2002, computer-science research later praised by a DCIA member-company derived similar conclusions from more formal empirical analysis. *See* Nathaniel Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA Peer-to-Peer File Sharing,* (2003).

Consequently, Lime Wire's 2009 decision to stop sharing document files by default is welcome—and troubling. Tomorrow, a *new* security problem with file-sharing programs may arise—a problem whose deadly serious consequences and simple solution would be obvious to both responsible program distributors and computer scientists. Should this happen, would we again need to endure nine years of needless, recurring security disasters before LimeWire LLC grasped the problem, perceived its long-published solution, and implemented it?

Possibilities like this—combined with the other factors discussed above—require me to conclude that I would only undermine and discredit the cause of voluntary self-regulation were I to advise this Committee that it remains a viable option in this case.

I thank the Subcommittee and the sponsors of H.R. 1319 for their careful attention to these important issues, and I look forward to providing any further assistance that might be useful to the Subcommittee and the sponsors of H.R. 1319.

Mr. RUSH. The chair thanks this witness and all the witnesses. Now the chair will ask that this committee stand in recess until such time as we return from a series of three votes. I would ask the witnesses if you please would wait so that the members can come back and ask questions. Thank you so much. The committee is in recess.

[Recess.]

Mr. RUSH. The hearing will now come to order. The chair recognizes himself for 5 minutes for the purposes of questioning the witnesses.

I would like to start out with some very simple questions to get on the record how the witness may view the legislation we are contemplating today. I will ask each and every one of you if you would just answer with a yes or no if you can, and if not, give me a very brief explanation of your answer. So my first question is with regard to H.R. 1319, do you support the legislation in its current form? If not, do you support the intent of the bill with revisions? And my second question, do support H.R. 2221 as it is currently drafted? If not, do you support the intent of the bill with some revisions? I will start with Mrs. Harrington.

Ms. HARRINGTON. The Federal Trade Commission strongly supports the intent of both bills. We would like to continue working with committee staff on revisions to each but we are very—and we are particularly supportive of the enforcement authority and tools that both bills give the FTC of civil penalty authority.

Mr. RUSH. Thank you.

Mr. Sohn?

Mr. SOHN. CDT has significant reservations about H.R. 1319 as drafted but we certainly support the intent. We do think it may be tricky to figure out the drafting details but we are certainly happy to work with the committee on that. On H.R. 2221, we generally do support the bill as drafted. There are some modifications we have suggested and we absolutely support the intent.

Mr. RUSH. Thank you.

Mr. Holleyman?

Mr. HOLLEYMAN. I actually agree fully with Mr. Sohn's comment that we support the intent of both bills. We have some recommendations in our written testimony. I believe strongly that action is needed. I think it may be more difficult to make some of the definitions in 1319 but are certainly eager to work with the committee to ensure the intent is fulfilled.

Mr. RUSH. Mr. Lafferty?

Mr. LAFFERTY. I will just speak to 1319. We absolutely support the intent of the bill, the clear, conspicuous notice and the informed consent for very important file-sharing modalities that could have major impact on consumers. We just don't think it can be legislated. We have worked hard to try to come up with suggestions for a redraft and it is very difficult to get the language not to reach out and touch other kinds of technologies and future software applications that would be impacted and disadvantage U.S. firms from overseas competitors. So we support the intent but not the language.

Mr. RUSH. Mr. Pratt?

Mr. PRATT. The CDIA has no position on H.R. 1319. With regard to H.R. 2221, we certainly support the intent. We have outlined in our written testimony the range of suggestions about how we could align the bills with other federal laws and if we could accomplish that goal, I think we would feel more comfortable with the final work product. Thank you.

Mr. RUSH. Thank you.

Mr. ROTENBERG. Mr. Chairman, we do support the intent of H.R. 2221 and generally support the legislation as drafted. We have a number of suggestions in our testimony for how to strengthen it.

With respect to 1319, we don't have a position for or against the bill. With respect to the intent behind 1319, we think it may be possible to get to some of the concerns regarding security through other legislation but we would certainly be happy to work with the committee to see how it can be accomplished.

Mr. RUSH. Mr. Boback?

Mr. BOBACK. Mr. Chairman, we strongly support both 2221 as well as 1319 in clearly raising awareness and providing some responsibility and structure to a very needed process both on the peer-to-peer as well as just federal data breach notification.

Mr. SYDNOR. Mr. Chairman, I will confine my comments to H.R. 1319. Yes, absolutely strongly support the intent of the bill. I am aware that there are legitimate concerns about making sure that we don't necessarily sweep in entirely—potentially entirely legitimate uses of peer-to-peer technology and would be happy to continue to work with the committee and anyone else to try to get to a place where everyone is comfortable.

Mr. RUSH. The chair thanks the witnesses. The chair's time is concluded. The chair now recognizes Ms. Bono Mack from California for 5 minutes for questioning.

Ms. BONO MACK. I thank the chairman and our panelists also for your time today.

Mr. Lafferty, I would like to read to you a bolded warning in the user guide on the Lime Wire website entitled "Using Lime Wire and P2P software safely." The warning states, and I quote, "Please ensure that any folder on your computer that contains personal information is not included in your Lime Wire library." So tell me, Mr. Lafferty, if I were to complete a default installation of Lime Wire 5.1.2, what files and folders will the mere installation of the program included in my Lime Wire library?

Mr. LAFFERTY. With Lime Wire 5 and later versions of Lime Wire, sensitive file types, which are a large number of extensions of files to protect your spreadsheets, your Word documents, PDFs, things that might have sensitive data, are unshared by default. So I would completely refute the testimony of Tom Sydnor earlier. It just isn't true. When you—neither example that he gave with the family that kept—just upgraded the version or the one that uninstalled it and reinstalled it, in both cases all the sensitive file types are unshared by default. It is over. They are no longer accessed or shared. To re-share any of those files, you would have to individually take the file and go through—ignore several warnings to put those individual files into the mode where they could be shared and then be asked whether you want to share that with specific friends or the network at large. So Lime Wire 5 has done

away with the concept of shared folders really and now it is a file-by-file—

Ms. BONO MACK. There are specific warnings? What do they say? And it is not—it is still actually sort of an inherent default. You have little boxes that come up. I believe there are four different boxes that are there. And one does say my documents, so you just that that could be an Excel spreadsheet which in fact would probably be saved under a my documents folder, would it not?

Mr. LAFFERTY. If you chose to put the my documents folder into a shared mode, it would still—

Ms. BONO MACK. Is that the default for an Excel spreadsheet for the standard user?

Mr. LAFFERTY. I don't understand the question.

Ms. BONO MACK. Where is a default Excel spreadsheet saved on your computer, on your hard drive? Is it not necessarily defaulted to my documents?

Mr. LAFFERTY. It is probably different for every person, but the point is—

Ms. BONO MACK. Probably different? What is the default? Where does—Mr. Sydnor, perhaps you have the answer to that.

Mr. LAFFERTY. It doesn't really matter where it is that. That file type won't be shared.

Ms. BONO MACK. How could it not matter? With all due respect, how could it not matter where it is? That is the root of the whole problem here.

Mr. LAFFERTY. Because it won't be shared.

Ms. BONO MACK. Unless you check simply one of the four—

Mr. LAFFERTY. Unless you choose that individual file if it has that Excel spreadsheet.

Ms. BONO MACK. That individual file?

Mr. LAFFERTY. Individual file, correct.

Ms. BONO MACK. Mr. Sydnor, do you care to comment on that?

Mr. SYDNOR. Yes. That is not quite an accurate statement about how the Lime Wire my library feature works. My library in Lime Wire 5 basically are the set documents that are going to be managed in Lime Wire and thereby that set of documents is going to be much easier to share because they are going to be in the library and there will be a button to click to share them, and that is why Lime Wire users' guide has the warning that you read, please ensure that any folder in your computer that contains personal information is not included in your Lime Wire library. Now, by default when you install Lime Wire 5.1, and I did it last night again, the default option is to have Lime Wire put all the files stored in your my documents folder and all of its subfolders into the Lime Wire library. That alone will not share them but it will make them available for sharing and much easier to share and therefore the behavior of the program simply not consistent with the advice in the users' guide. As to my testimony earlier, it was quite correct. The difference—the reason I think we are getting confused is, when I say sensitive files, I mean files that would actually be sensitive to share over a network like Gnutella so you have, for example, scans of your family medical records and tax returns, those can be stored in image file formats often and those will be shared by default, and if you upgrade to Lime Wire 5, it will continue to share

those file types if you were sharing them before, and if you install Lime Wire 5 on your computer and a previous version of Lime Wire has ever been there, then it will automatically begin re-sharing files that were shared previously. So simply installing the program can indeed resume sharing of files even if you are installing on a computer where there is no version of Lime Wire currently installed. I am correct about that. I reran the test again this morning before the hearing.

Ms. BONO MACK. Thank you. I know my time is expired and I hope we have a second round. Thank you, Mr. Chairman.

Mr. RUSH. The chair intends to have a second round. The chair now recognizes the gentleman from Georgia, Mr. Barrow, for 5 minutes.

Mr. BARROW. I thank the chair. I want to try and get my arms around the inadequacy of the current situation and talk about what it is this legislation proposes to do in order to try and alter the situation for the better.

Ms. Harrington, am I correct in understanding that there are very limited tools available to the FTC right now to deal with this issue, that basically the only option you have under current law is to initiate a specific enforcement action against somebody, a fact-specific action based on a specific instance and that basically you are pretty much limited to, is it adjunctive proceedings? Is that about the extent of it?

Ms. HARRINGTON. That is right.

Mr. BARROW. No civil penalties whatsoever?

Ms. HARRINGTON. No civil penalties.

Mr. BARROW. No rulemaking authority, no prescribing of proper procedures or best practices, you just have to go after individual cases and all you can do is tell folks to stop doing what they are doing when you prove that they have done it?

Ms. HARRINGTON. The rulemaking authority available to the Commission is under the Magnusson-Moss amendments to the FTC Act and those are laborious and take a very long time, the procedures to use.

Mr. BARROW. So what we are proposing to give the FTC under 1319 would give you all some authority you don't have right now. Are the civil penalties helpful to you all in trying to bring some order to this situation?

Ms. HARRINGTON. There are two things that are helpful. Civil penalty authority is very helpful, and also to the extent that some practices in these very fact-specific situations might be injurious but neither deceptive nor unfair, then having additional statutory authority is very helpful.

Mr. BARROW. Earlier on in the testimony, we heard some folks raise some issues about the international end of things. We all know we are connected to a worldwide web and that any effective regulation of this marketplace in our country is going to involve dealings with folks who can cross the boundaries in cyberspace pretty much at will. What was your concern, if not the extraterritoriality of the law, the extraterritorial effect of us being able to regulate this? How do you think we can address that supposed shortcoming of us attempting to regulate this on our own shores?

Ms. HARRINGTON. Well, first of all, the subcommittee was instrumental in giving the Commission additional authority under the U.S. Safe Web Act, which we used to get information about overseas targets and to enlist help from other governments and that is very useful. But that said, if there are overseas software providers who are making available file-sharing software that is injurious to U.S. consumers, we can certainly assert our jurisdiction over those practices that occur within the United States but we may not be able to reach the purveyors if they are in other countries and particularly in countries that aren't particularly interested in helping out.

One of the things that we are very concerned about is that the dominant players in this industry, which are in the United States, do the best thing and the right thing and we think that setting some legislative standards such as the ones that are set forth in the bill would really help. We want the U.S. players to be the best players so that they continue to be the dominant players and the ones that consumers can use with some confidence.

Mr. BARROW. The impression I get from what you are saying, this is how I hear what you are saying, is that if we police the marketplace where everybody shops, we don't have to worry about the marketplace where few very people shop or hardly anybody goes. Is that a fair way of putting it?

Ms. HARRINGTON. Well, we certainly should police the marketplace where everybody stops if that marketplace is subject to our jurisdiction.

Mr. BARROW. But the high-volume users, the ones that have the lion's share of the market, if we can make sure that what they are doing is right and appropriate and folks who trade at these places will not have to worry about losing their stuff, we don't have to worry quite so much about those areas that might be hard to reach. Why strain at a gnat and swallow an elephant in the process.

Ms. HARRINGTON. You know, that is certainly the intention. There is always a risk that overseas operators can gain in market share in the United States by doing—you know, by gaining some sort of competitive advantage over the regulated entities in our marketplace but, you know, that is not a worry right now that is keeping me awake at night.

Mr. BARROW. I will wait for a second round, Mr. Chairman. Thank you, ma'am.

Mr. RUSH. Thank you.

The chair now recognizes the gentleman from Louisiana, Mr. Scalise, for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. Really I can open this up to the whole panel on H.R. 1319. Do you think this will help prevent a legal use of peer-to-peer software including stealing personal records, copyright violations and things like sharing child pornography?

Ms. HARRINGTON. I think it will help under some circumstances and under others we need more. The data security bill actually could be very helpful here too because, as I mentioned in my oral statement, there are really three scenarios where sensitive information is shared. One is when consumers don't know, don't understand, and this bill will hopefully go a long way I think there. It

is not going to help when the problem is malware, and it is not going to help when the problem is a business that has not prohibited and barred from its system and its computers file-sharing software and it is not going to help if the problem is that an employee of a company takes sensitive information home and puts it on his or her computer and that computer has file-sharing software or malware on it that extracts that, so it is going to go a long way to help in scenario one.

Mr. SCALISE. Anybody else want to touch on that?

Mr. SOHN. I will just say I do think the intent and the focus of the bill is certainly on the inadvertent disclosure so that the privacy-related concerns, I think that would be the main impact and is the main thrust of the bill.

Mr. SCALISE. Let me ask about the data breaches that have occurred, I think FTC had dealt with it, the largest one I have seen, the TJX, which I think initial estimates were about 45 million Visa/MasterCard records were breached. Ultimately it turned out somewhere close to 100 million were breached, and you all had brought charges against them, and subsequently other companies. Is there now an industry standard for data protection? What is your feeling on where we are today versus some of those cases a few years ago?

Ms. HARRINGTON. Well, there are certainly well-established good practices that in the cases that we have brought were not followed. For example, you know, downloading available patches, preventing against well-known attacks and kinds of attacks are well-settled, you know, necessary practices. They are not even best practices. They are necessary. And those companies did not follow those practices.

Mr. SCALISE. Anybody else want to add anything to that? We are getting into now an area of moving towards electronic medical records. There was some funding language in the stimulus bill to start going down that road more as people's health information gets put on the Web more and more. What kind of protections are there today, what kind do we need, whether it is in either these two bills or another vehicle to protect people's health records as they become available on the Internet so that they are only available to the doctors who need to be reviewing them?

Ms. HARRINGTON. Well, the Recovery Act also directed both the FTC and the Department of Health and Human Services to do rulemaking to set standards for breach notification when consumers' sensitive health information is placed at risk. The FTC, as I mentioned, has just issued a proposed rule dealing with personal health records and other non-HIPAA-covered entities that may have this sensitive information to set breach notification standards and we are continuing also to work with HHS to do a report that is due back to Congress in a year on these issues.

Mr. SCALISE. Any of you all doing any work on that issue? Mr. Boback?

Mr. BOBACK. I would like to also comment on that. There are no standards as far as peer-to-peer notifications. There are no standards as far as peer-to-peer security measures. In fact, most companies don't even have any standards on peer-to-peer. When asked, most corporations, large and scale, what information they are doing

about peer-to-peer, most people, if they respond at all will say that they are blocking peer-to-peer and that they have a policy against it. That is the extent of it. And I will tell you that—or they will say that they have a firewall or an encryption of which nothing—firewall does not stop peer-to-peer, encryption does not stop peer-to-peer. Intrusion prevention detection and all the standard security measures do not peer-to-peer disclosures from happening, which is why in the past 60 days we have had, you know, almost 4 million disclosures of this type via peer-to-peer because there is just no standards.

Mr. SCALISE. And finally Mr. Holleyman.

Mr. HOLLEYMAN. Mr. Scalise, we believe that the incentives that are in Chairman Rush's bill that would encourage a marketplace to grow for companies who hold sensitive data to use proper security technologies to make that information inaccessible to anyone who might actually breach it, that those market-based incentives is a great supplement to the enforcement authority that the bill would give. So we think the two together can be effective.

Mr. SCALISE. Thanks. I yield back, Mr. Chairman.

Mr. RUSH. The chair intends to engage the members of the committee in a second round of questioning and we will allow each member an additional 2 minutes for the second round of questioning. The chair recognizes himself now for the second round and allocates 2 minutes for the purposes of questioning.

Mr. Rotenberg and Mr. Sohn, is the definition of personal information under H.R. 2221, is it adequate in terms of data security? The bill only addresses financial information. Should we also consider requiring companies to secure sensitive information such as medical information or password numbers or et cetera? I mean, should we expand the definition of personal information?

Mr. SOHN. Well, the bill has several different components, and I think for purposes of the breach notification component, the definition there is fairly close to what has been done in a lot of the States and it reflects a lot of what has been common in the data breach notification area. I think for purposes of something like security standards, asking companies to have reasonable procedures in place to protect data, there is no reason to restrict it to the rather narrow set of data that is in the definition of personal information now because what is currently in the bill only applies—it is not just name and address and some other information. There actually has to be either a Social Security number or a financial account number plus password or a driver's license number, something like that. So I do think that the bill might consider using a broader definition of personal information for some purposes and the narrower definition for others.

Mr. ROTENBERG. Mr. Chairman, in my written statement I made a suggestion on this issue of personal information. I do think it is appropriate to have a broader standard and also to recognize that some of the personal identifiers nowadays aren't just limited, for example, to a Social Security number or driver's license number. There are other types of personal identifiers like a Facebook member number or even the IP address associated with your computer that needs to be incorporated as well. So I think those changes can

be made both to get to more circumstances where the bill should reach and also new types of identifiers.

Mr. RUSH. The chair thanks the witnesses. Now the chair recognizes the gentlelady from California for 2 minutes for additional questions.

Ms. BONO MACK. I thank the chair for the second round.

Mr. Holleyman, you testified that the P2P bill would cover more than just the illegitimate purpose software. You identified a number of legitimate uses of P2P software such as bicoastal collaboration on projects. I think you actually mentioned Palm Springs to Chicago airports collaborating. So this is of course when used correctly beneficial use of P2P software. So we all agree that this technology can be extremely helpful but if such programs are covered by H.R. 1319, what is the harm? How is notice and consent an issue? Back to the Palm Springs-Chicago, yes, I can see them collaborating on plans but I don't think they necessarily want to collaborate on payroll numbers and the like. So how is notice and consent an issue in this case?

Mr. HOLLEYMAN. Ms. Bono Mack, our sense is that there is a rapid growth in the legitimate uses of P2P, and that it will become a de facto part of how we use technology that most people will want to use. So our sense is as that part of the market grows, we want to ensure that the legislation doesn't overreach to get into things which all of us would generally agree would not necessarily need—an initial notice that that is there is fine but the process of how you would then disable that needs to be clarified.

Ms. BONO MACK. Which is growing faster, illegitimate or legitimate uses?

Mr. HOLLEYMAN. I think our sense as technologists is—and I am not a technologist, I play one on TV, but not as technologists but our engineers and our companies believe that legitimate purposes of peer-to-peer in the next 10 years will certainly grow much faster than the illegitimate ones.

Ms. BONO MACK. In the next 10 years, quickly in 10 seconds, Mr. Boback, which has grown faster, legitimate or illegitimate uses?

Mr. BOBACK. I will tell you that legitimate uses are now emerging so while there is still a growth at this point because the awareness is still decreased and there is not enough awareness as to the problem, the legitimate uses and the distribution content is an absolute must going forward. So I am a supporter of peer-to-peer, however, the security measures just as in the early stages of the World Wide Web need to be addressed as in your bill 1319.

Ms. BONO MACK. Thank you.

Mr. RUSH. The chair now recognizes the gentleman from Georgia.

Mr. BARROW. I thank the chair. I think Ms. Bono Mack is getting to the heart of the issue on the peer-to-peer legislation. If I could reframe the issue, we want to fix what is broke with this system. There is stuff out there that is inside this legislation's definition of peer-to-peer file-sharing program that is malicious. There is stuff out there that is inside this definition that is perfectly benign.

Mr. Holleyman and Mr. Sohn, I am going to pitch this one in you all's direction. How would you all define what we are getting at in such a way as to stop the bad stuff and allow all the other stuff to continue without having to have a proliferation of warnings and

opt-outs that basically hobble this technology before it can even get started? Take a shot at how you would define this in order to be able to reach the stuff you want to reach.

Mr. HOLLEYMAN. I will start on that, Mr. Barrow. In our testimony, we have actually listed five ways in which we would modify the definition in the bill and believe that if those types of changes are made, that that would be useful and would help preserve the intent of the bill including looking at the type of purposes that peer-to-peer file-sharing program is typically used for, going at many of those things like copyright infringements, which are a huge source of concern to—

Mr. BARROW. Is that an effective way of defining it though so that the regulators can get at what is going on?

Mr. HOLLEYMAN. We actually think that the regulators would—their hand would be strengthened by more precision in the definition rather than the breadth that is in there currently.

Mr. BARROW. Mr. Sohn, what do you think?

Mr. SOHN. I also set forth in my testimony some ideas on that point of how you might make this more narrow and apply to what we think of as file-sharing software. I agree with Mr. Lafferty's testimony that the key here really isn't peer-to-peer. Peer-to-peer is a kind of architecture. It is really about file-sharing functions that could enable documents and other kinds of files on a user's local computer to be made available to third parties, you know, in bulk and third parties that haven't been selected or aren't even known to the user and so we propose four bullet points of items that we think could be in the definition but it tends to focus on that, the ability to share files with unknown parties with no intervening action or knowledge or selection by the user in terms of who that file will be shared with.

Mr. BARROW. Mr. Chairman, my time is expired but I would like to ask the witnesses to go beyond that and actually be prepared to work with counsel and us to see if we can actually come up with some concrete language to accomplish this. Thank you. I yield the mic.

Mr. RUSH. The chair now recognizes the gentleman from Louisiana for an additional 2 minutes.

Mr. SCALISE. Thank you again, Mr. Chairman.

These two bills might not necessarily be the vehicles for it but they might. It has been a problem for years, especially with identity theft getting worse with so many documents and authenticators that use Social Security numbers that require Social Security numbers to be used or documents that are public record that still require people to use Social Security numbers. A number of States have gone on their own and tried to ferret those out and prohibit Social Security numbers on public documents but it is not universal. There is no real standard still. I think there as standalone legislation, it might have been in the last Congress, that really didn't go anywhere but there is a way that we can have some kind of standard to protect people's Social Security numbers so that they are not required for certain documents or authenticators so that they are not so easily obtainable by third parties that are trying to take them for bad purposes? I will start it off with Ms. Harrington and anybody else that wants to take a shot.

Ms. HARRINGTON. Well, as part of the President's identity theft task force work that we have been engaged in, there are couple of important initiatives that we are supporting. One, the task force brought about a government-wide examination of government uses of Social Security numbers with the goal of minimizing to circumstances where the number is absolutely essential, federal government agencies' use of Social Security numbers, and I think a lot of progress has been made in the government on that. Number two, the FTC as part of the identity theft task force work convened a workshop and has continued to work on the question of authentication and how better authentication procedures and technologies can be developed so that something like the ubiquitous Social Security number is no longer needed. But there are lots of commercial settings right now where both consumers and businesses benefit from the use of Social Security numbers and may need them, and until we have much better authentication measures available, it is a very tough question to answer what to use instead of Social Security numbers. For example, consumers have really benefited in many instances from being able to quickly get a loan to get a car. That whole credit reporting system depends on Social Security numbers, and you know, we need a replacement but we don't have one yet.

Mr. SCALISE. And at least in the government sector where we can set up a mechanism where people aren't required to have it on a document that is public record because—

Ms. HARRINGTON. Right.

Mr. SCALISE. —clearly in the government arena, there are records that are public and some of those records require a Social Security number, which obviously poses big, big security breach problems that have been documented. In this legislation, if there a way to maybe try to address that, I don't want to interfere with the chairman or Ms. Bono Mack's bill but if there is a way we can do something that doesn't necessarily cause other problems on the other side we can try to address a narrow part of that problem.

Mr. RUSH. The gentleman's time is expired.

Mr. SCALISE. Thank you.

Mr. RUSH. The chair really just wants to again thank the witnesses. We have imposed on your time pretty significantly this afternoon and we certainly are appreciative of the fact that you have allowed us to do that and you have been a great panel. If you would be so kind, we want to keep the record open for at least 72 hours until there might be members of the subcommittee who will in writing ask questions and if you would respond in writing within 72 hours, the chair would certainly appreciate that.

So thank you so very much again and you have really done this subcommittee quite a great service. The hearing now stands adjourned.

[Whereupon, at 4:45 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Statement of the Honorable Marsha Blackburn (TN-07)
The Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection
Legislative Hearing: "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act"
May 5, 2009

Mr. Chairman, I want applaud your leadership and thank the subcommittee for calling Members' attention to the legislation under consideration today. As we all know, the challenge of protecting consumer data in our digital age continues to perplex private sector leaders, consumer advocates and government officials alike. We must all work together to solve this problem, and I hope the expert testimony offered by our panel of witnesses today will contribute to that effort.

In particular, I rise in strong support of H.R. 1319, legislation offered by my friend and colleague, Rep. Bono-Mack, and the gentleman from Georgia, Rep. Barrow. The Informed P2P User Act takes a series of commonsense steps towards ensuring a safe and secure Internet experience not only for users of peer-to-peer software, but also for family members who don't use peer to peer software but nevertheless may be adversely impacted by breaches in data security.

Primarily, the legislation prohibits Peer-to-Peer (P2P) software purveyors from improperly disclosing personal information without a consumer's notice and consent. This simple tool creates a legal obstacle to prevent an inadvertent breach in a P2P user's sensitive data. After all, many users are simply not aware that tax, medical or other private documents lurking in an insecure hard drive folder are likely at risk when a they log-in to use a P2P service on the market today.

This provision creates piece of mind for consumers, but also for parents who want to know their families' most sensitive information remains secure when children use the Internet.

The legislation also provides legal security for digital entertainment enthusiasts who abide by the letter of the law and refuse to obtain digital media illegally. When peer to peer users log on to use a service for legitimate purposes, they have a right to know that legal, pure digital content downloaded for personal use will remain pristine, and not subject to impermissible dissemination or degradation without their knowledge or consent. H.R. 1319 takes critical steps to ensure this data remains under lock and key.

Mr. Chairman, Rep. Bono-Mack and Rep. Barrow are to be commended for bringing forward the legislation under consideration today. I humbly offer my full support as a cosponsor of H.R. 1319, and yield back the balance of my time.

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6115

MAJORITY (202) 225-2927
FACSIMILE (202) 225-2525
MINORITY (202) 225-3641

energycommerce.house.gov

June 25, 2009

Eileen Harrington
Acting Director
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Ms. Harrington:

Thank you for appearing before the Subcommittee on Commerce, Trade, and Consumer Protection on May 5, 2009, at the hearing entitled "Legislative Hearing on H.R. __, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by July, 9, 2009, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

Response to Questions from the Honorable Bobby Rush
Following Up on May 5, 2009 Hearing on HR 2221:
Data Accountability and Protection Act

1. **The definition of personal information in the Data Accountability and Trust Act is very narrow. It covers a person's name or address or phone number in combination with any one or more of: Social Security number; Driver's License number or other State ID number; financial account number or credit or debit card number and any code necessary to access that account. That definition applies to both the information security requirements and the data breach notification requirements. While such a narrow definition of personal information may be appropriate for the data breach provisions to avoid over-notification, it may be too narrow for information security requirements. Do you believe that it would be appropriate to expand the definition of personal information for the security provisions of the Act? What should the definition of personal information be for that provision? Would it be appropriate to provide the FTC with rulemaking authority to modify or expand the definition of personal information for the information security provisions beyond the limited rulemaking authority already in the bill?**

As you note, HR 2221 imposes data security requirements on entities that maintain "personal information." The definition of "personal information" in HR 2221 as introduced covered only information that included Social Security numbers, other identifying numbers, or account numbers. Thus, for example, a company that owned a database containing only consumers' names, along with their sensitive health information, would not have been required to maintain the security of its database. Indeed, such a company may not have been subject to *any* federal requirement to maintain the security of the sensitive health information it held.[1]

Rather than expanding the definition of "personal information" in the bill itself to address specific scenarios, the Commission staff had recommended to Congressional staff that the Commission be given authority to conduct a rulemaking to expand the definition. A rulemaking proceeding would allow the Commission to seek input about what types of personal information

[1] The security requirements of the Health Insurance Portability and Accountability Act ("HIPAA") would not necessarily apply to such a company; they apply only to health care providers that conduct certain transactions in electronic form, health care clearinghouses (which provide certain data processing services for health information), health plans, or business associates of such entities.

companies collect, and the costs and benefits associated with maintaining the security of such information. We are extremely pleased that your Subcommittee adopted this suggested change.

On a related issue, staff suggests not limiting breach notification to situations in which there is a "reasonable risk of identity theft, fraud, or other unlawful conduct" as is currently proposed in HR 2221. This formulation does not capture other harms associated with unauthorized disclosure of information, such as the embarrassment associated with the release of sensitive health information. Thus, staff suggests that the breach notification provisions should apply when there is a "reasonable risk of identity theft, fraud, or other harmful conduct," and that the bill should require the FTC to conduct a rulemaking to determine what constitutes "harmful" conduct.

2. **Section 4(c) of H.R. 2221 provides that it will be an affirmative defense to a law enforcement action brought under the Act's data breach notification provisions that all of the information that was subject to the breach was information acquired from public records. Thus, if a database is compromised that is made up exclusively of public records such as bankruptcy documents, criminal histories, property records, court filings, and other documents with sensitive personal information consumers will not be notified. If the same or even less information is in another database, consumer would receive notice. Does this distinction based on the original source of the information make sense? What are the benefits of this affirmative defense?**

The Commission staff does not support an affirmative defense for breaches of public record databases. In many cases, information brokers compile detailed dossiers on individuals, consisting solely of public record information. This information may be extremely sensitive and, when collected and compiled together in one place, could do significant harm to consumers if breached.[2] For example, such dossiers may contain Social Security numbers (which are not always redacted in public records) and/or enough detailed history about the consumer that an unauthorized person could perpetrate identity theft, thus posing substantial harm to the consumer.[3] An unauthorized user also could gain enough information to engage in "pretexting," the practice of posing as another person in order to obtain financial records or other private information. Finally, unauthorized users

[2] Although public record data is already accessible in public files elsewhere, it is scattered among many different places, and thus difficult for any one person to find on his or her own. Information brokers compile this data together, thus making it a treasure trove for those seeking to do harm.

[3] For example, for authentication purposes, businesses often ask consumers personal questions that presumably only the consumers themselves know the answers to. An identity thief may be able to gather enough information about a particular consumer to answer these questions.

could use information in these records to blackmail, stalk, harass, or otherwise threaten consumers.

If an unauthorized user accesses these dossiers about individual consumers, staff believes that the consumers would want to know. In addition, notice would allow the consumers to take steps, when possible, to limit the harm from the disclosure. For these reasons, Commission staff suggests deleting this affirmative defense.

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6115

MAJORITY (202) 225–2927
FACSIMILE (202) 225–2525
MINORITY (202) 225–3641

energycommerce.house.gov

June 25, 2009

David M. Sohn
Senior Policy Counsel
Director, Project on Intellectual Property and Technology
Center for Democracy and Technology
1634 I Street, NW #1100
Washington, DC 20006

Dear Mr. Sohn:

Thank you for appearing before the Subcommittee on Commerce, Trade, and Consumer Protection on May 5, 2009, at the hearing entitled "Legislative Hearing on H.R. __, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by July, 9, 2009, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

July 8, 2009

Committee on Energy and Commerce,
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Legislative Hearing on H.R. 2221 and H.R. 1319:
Response of Center for Democracy and Technology (CDT)
to Written Questions for the Record

CDT is pleased to submit the following responses to written questions for the record in connection with the May 5, 2009 hearing entitled "Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act."

Questions from The Honorable Bobby Rush

1. The definition of personal information in the Data Accountability and Trust Act is very narrow. It covers a person's name or address or phone number in combination with any one or more of: Social Security Number; Driver's License number or other State ID number; financial account number or credit or debit card number and any code necessary to access that account. That definition applies to both the information security requirements and the data breach notification requirements. While such a narrow definition of personal information may be appropriate for the data breach provisions to avoid over-notification, it may be too narrow for information security requirements. Do you believe that it would be appropriate to expand the definition of personal information for the security provisions of the Act? What should the definition of personal information be for that provision? Would it be appropriate to provide the FTC with rulemaking authority to modify or expand the definition of personal information for the information security provisions beyond the limited rulemaking authority already in the bill?

Answer: Yes, CDT believes that the information security requirements in H.R. 2221 should reach beyond the relatively narrow class of data defined as "personal information" for purposes of the bill's breach notification provisions. The bill's current definition closely tracks that found in state breach notification statutes. Presumably, the states have used this type of narrow definition in order to avoid over-notification. If notices become too routine, they may cease to provide useful warnings to consumers and may needlessly impose costs on the entities required to send them.

In contrast, sound data security practices should be encouraged for all personal data. That does not mean one-size-fits-all rules; the particular security safeguards

that may be warranted in a given circumstance will vary depending on factors such as the sensitivity of the data in question. But the general concept of evaluating possible privacy and security risks to personal data and adopting safeguards appropriate to those risks should apply across-the-board.

CDT would suggest a legislative approach based on the FTC's implementation of the security safeguards requirements in the Gramm-Leach-Bliley Act (GLB). GLB calls for financial institutions to protect the security and confidentiality of customers' "nonpublic personal information" and requires appropriate security safeguards for "customer records and information." (See 15 USC 6801(a) and (b).) The FTC rules implementing these provisions apply to "customer information," defined as "any record containing nonpublic personal information . . . that is handled or maintained by or on behalf of you or your affiliates" (16 CFR 314.2(b)). "Nonpublic personal information" excludes information that is publicly available but otherwise includes essentially any personally identifiable information a financial institution has obtained from or about a customer. (See 16 CFR 313(n)-(o).)

To follow this approach, the Committee could modify the information security provisions (section 2) of H.R. 2221 by replacing the term "personal information" with the term "non-public information" – a term already defined in section 5(9) of the bill. In addition, for the reasons discussed in the answer to the next question, CDT would also recommend that the Committee consider going a step further and extending coverage to data that is "public record information" but that would be difficult, costly, or time consuming for a third party to obtain or compile independently.

An alternative approach, as the question notes, would be to authorize the FTC to expand the definition of "personal information" for purposes of the bill's information security provisions. Section 5(7)(B) of H.R. 2221 already authorizes the FTC to modify the definition of "personal information," but it is not clear whether this would empower the agency to modify the definition for some parts of the statute but not others. The agency might well conclude that if it modifies the definition, it must do so for all parts of the Act. Therefore, if the Committee wishes to rely on the FTC to expand the scope of the data to which bill's information security provisions will apply, it should include a specific provision in section 2 directing the FTC to consider such an expansion as part of the rulemaking required under section 2(a)(1).

In connection with either approach to expanding the reach of the information security provisions, CDT believes that two further changes to section 2 would be warranted. First, to clarify that not all nonpublic data raises the same level of security concerns, a new section 2(a)(1)(D) should be added, reading: "(D) the sensitivity of the nonpublic information at issue." Second, to avoid requiring individuals with very small amounts of data to file formal written security plans, the Committee should consider a de minimis exception for persons that own or possess data in connection with purely personal, family, or noncommercial activities.

2. Section 4(c) of H.R. 2221 provides that it will be an affirmative defense to a law enforcement action brought under the Act's data breach notification provisions that all of the information that was subject to the breach was information acquired from public records. Thus, if a database is compromised that is made up exclusively of public records such as bankruptcy documents, criminal histories, property records, court filings, and other documents with sensitive personal information consumers will not be notified. If the same or even less information is in another database, consumers would receive notice. Does this distinction based on the original source of the information make sense? What are the benefits of this affirmative defense?

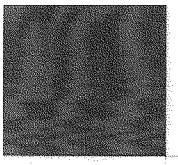
Answer: The apparent rationale for the affirmative defense set forth in section 4(c) is that when information is available from public records, a breach of a private database containing that information poses little if any additional security threat to the individual; after all, if thieves or scammers wanted to use the information, they could go and get it from public records. Therefore, notification would serve little purpose and the entity suffering the breach should not be required to bear the costs associated with notification.

The problem with this rationale, however, is that there is a great deal of public record information that is "practically obscure" – that is, publicly available in theory but difficult to access in practice. For example, certain records exist in paper form and can be obtained only by digging through dusty files in a county courthouse. When companies gather this data and compile it in convenient electronic form, they effectively transform scattered bits of difficult-to-access information into highly usable, large-scale databases. If those databases are later breached, individuals are put at risk – much greater risk than if the information had remained in scattered public records.

For this reason, CDT believes that entities compiling personal data from public records should be required to notify individuals when hackers have accessed that data. The mere fact that an identity thief in theory could have obtained a person's data from another source would be little comfort to the individual victim in a scenario where the identity thief took advantage of a company's convenient electronic compilation and the company, relying on section 4(c), elected not to provide notice of the breach. In short, CDT does not support the affirmative defense set forth in section 4(c).

CDT appreciates the opportunity to provide this additional input. Thank you.

David M. Sohn
Senior Policy Counsel
Center for Democracy and Technology



BSA
BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202.872.5500
f. 202.872.5501

July 14, 2009

The Honorable Bobby Rush
U.S. House of Representatives
2416 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Rush:

Thank you for your interest in the views of the Business Software Alliance (BSA)* on H.R. 2221, the Data Accountability and Trust Act. As I indicated in my testimony before your Subcommittee on May 5, we believe your bill would make a substantial contribution to improving security and trust online.

Per the letter of Chairman Waxman of June 25, below are BSA's answers to your questions for the record. We remain at your disposal should you have further questions and look forward to working with you as the bill moves to the Full Committee.

Sincerely,

Robert Holleyman

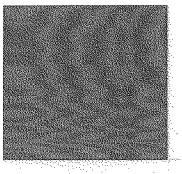
*The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cadence, Cisco Systems, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, and The MathWorks.

1. *"The definition of personal information in the Data Accountability and Trust Act is very narrow. It covers a person's name or address or phone number in combination with any one or more of: Social Security Number; Driver's License Number or other State ID number; financial account number or credit or debit card number and any code necessary to access that account. That definition applies to both the information security requirements and the data breach notification requirements. While such a narrow definition of personal information may be appropriate for the data breach provisions to avoid over-notification, it may be too narrow for information security requirements. Do you believe that it would be appropriate to expand the definition of personal information for the security provisions of the Act? What should the definition of personal information be for that provision? Would it be appropriate to provide the FTC with rulemaking authority to modify or expand the definition of personal information for the information security provisions beyond the limited rulemaking authority already in the bill?"*

BSA does not believe that the definition should be expanded for the security provisions of the Act, for two reasons.

First, the definition is appropriately based on the concept that data should be protected on the basis of its value, specifically that it can be used to commit identity theft, fraud and other unlawful conduct. As the information security provisions of the bill are rightly demanding, we believe it is appropriate to ensure they apply to personal information that genuinely needs this high level of protection.

Second, as I indicated in my testimony, we are concerned about the risk of making data custody – an activity that most companies, whether large or small, engage in and yet is only incidental to their core business – a regulated activity. We increase this risk every time we unnecessarily expand the scope of data security requirements, and thus increase compliance burdens, without commensurate improvements in data security. Compliance challenges and confusion would only increase if a law provided two different definitions of the same notion.



2. *"Section 4(c) of H.R. 2221 provides that it will be an affirmative defense to a law enforcement action brought under the Acts data breach notification provisions that all of the information that was subject to the breach was information acquired from public records. Thus, if a database is compromised that is made up exclusively of public records such as bankruptcy documents, criminal histories, property records, court filings, and other documents with sensitive personal information consumers will not be notified. If the same or even less information is in another database, consumers would receive notice. Does this distinction based on the original source of the information make sense? What are the benefits of this affirmative defense?"*

BSA members have not formed a position on the specific issue of notification of breaches of publicly available data within the context of the broader provisions of H.R. 2221.

June 25, 2009

Stuart K. Pratt
President and CEO
Consumer Data Industry Association
1090 Vermont Avenue, NW, Suite 200
Washington, DC 20005-4905

Dear Mr. Pratt:

Thank you for appearing before the Subcommittee on Commerce, Trade, and Consumer Protection on May 5, 2009, at the hearing entitled "Legislative Hearing on H.R. __, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by July, 9, 2009, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

July 8, 2009

The Honorable Henry A. Waxman
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

RE: The Data Accountability and Protection Act

Dear Chairman Waxman:

Thank you for the opportunity to respond to your questions regarding the Data Accountability and Protection Act. Following are our responses:

Question 1

The definition of personal information in the Data Accountability and Trust Act is very narrow. It covers a person's name or address or phone number in combination with any one or more of: Social Security number; Driver's License number or other State ID number; financial account number or credit or debit card number and any code necessary to access that account. That definition applies to both the information security requirements and the data breach notification requirements. While such a narrow definition of personal information may be appropriate for the data breach provisions to avoid over-notification, it may be too narrow for information security requirements. Do you believe that it would be appropriate to expand the definition of personal information for the security provisions of the Act? What should the definition of personal information be for that provision? Would it be appropriate to provide the FTC with rulemaking authority to modify or expand the definition of personal information for the information security provisions beyond the limited rulemaking authority already in the bill?

Response to Question 1

We do not feel it is appropriate to expand the definition of "personal information" as it applies to the data security provisions in the Act. The focus should remain on those data elements whose misuse is most commonly associated with identity theft or fraud. The data elements specified in Act are the most sensitive and are those most commonly used to commit identity theft and fraud. Further, the Act already provides the FTC with rulemaking authority to modify the definition of "personal information," therefore, no expansion of the definition in the Act is necessary.

Question 2

Section 4(c) of H.R. 2221 provides that it will be an affirmative defense to a law enforcement action brought under the Act's data breach notification provisions that all of the information that was subject to the breach was information acquired from public records. Thus, if a database is compromised that is made up exclusively of public records such as bankruptcy documents, criminal histories, property records, court filings, and other documents with sensitive personal information consumers will not be notified. If the same or even less information is in another database, consumers would receive notice. Does this distinction based on the original source of the information make sense? What are the benefits of this affirmative defense?

Response to Question 2

We commend the committee for recognizing the need to address the issue of information obtained from public records. It simply makes no sense to require companies to notify individuals of security breaches involving public record information or to implement additional security requirements for such information, since the information already is widely available and in the public domain.

However, we do not believe that the bill's affirmative defense provision is the best way to address this issue. We are concerned that this approach will lead to unnecessary litigation and significant, unnecessary expense. A defendant typically cannot raise an affirmative defense until a case has been brought and significant resources are consumed both by the regulators and the defendant.

A recommended alternative to the affirmative defense approach would be to include an exception for public record information in the definition of personal information. This is the approach taken by all of the states that have included a public record exception in their data security laws. To date, 40 states, including Illinois, have enacted data security laws that included exceptions for public record information.[1]

This also is the approach that Congress took with the sensitive financial information protected by the data privacy and security provisions of the Gramm-Leach-Bliley Act, which exclude publicly available information, including public record information, from their scope. Consequently, the FTC and the functional regulators exclude publicly available information from the types of information that must be protected under the GLB Safeguards Rule and that trigger consumer notifications under the jointly-issued security breach notification guidance. Thus, we recommend that the definition of "personal information" be amended to exclude from its scope information obtained from public record and publicly available sources.

Sincerely,

Stuart K. Pratt
President & CEO

[1] The forty states are: AZ, CA, CO, CT, DE, FL, GA, HI, IA, ID, IL, IN, KS, LA, ME, MA, MD, MI, MN, NC, ND, NE, NH, NJ, NY, NV, OH, OK, OR*, PA, SC, TN, TX, UT, VA, VT, WA, WI, WV, WY.

June 25, 2009

Marc Rotenberg
Executive Director
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

Dear Mr. Rotenberg:

Thank you for appearing before the Subcommittee on Commerce, Trade, and Consumer Protection on May 5, 2009, at the hearing entitled "Legislative Hearing on H.R. __, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by July, 9, 2009, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

July 9, 2009

Chairman Henry Waxman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Waxman,

This letter responds to your letter of June 25, 2009 regarding the May 5, 2009 hearing entitled "Legislative Hearing on H.R. ___, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act."

Congressman Rush asked:

The definition of personal information in the Data Accountability and Trust Act is very narrow. It covers a person's name or address or phone number in combination with any one or more of: Social Security Number; Driver's License number or other State ID number; financial account number or credit or debit card number and any code necessary to access that account. That definition applies to both the information security requirements and the data breach notification requirements. While such a narrow definition of personal information may be appropriate for the data breach provisions to avoid over-notification, it may be too narrow for information security requirements. Do you believe that it would be appropriate to expand the definition of personal information for the security provisions of the Act? What should the definition of personal information be for that provision? Would it be appropriate to provide the FTC with rulemaking authority to modify or expand the definition of personal information for the information security provisions beyond the limited rulemaking authority already in the bill?

The current definition of personal information is too limited—not only for the bill's information security provisions, but also for its data breach notification provisions. The Internet makes reconstruction of identity from a single identifier quite a simple matter. Yet, under the current definition, unauthorized access to or acquisition of each and every piece of information listed in sections 5(7)(A)(i)-(iii) would not trigger the Act's notification or security requirements unless linked with the individual's name, address, or phone number. However, armed with a driver's license number, passport number, military identification number, and financial account or credit card number plus the associated security code or password, an identity thief could inflict a tremendous amount of damage.

For example, under the definition of personal information currently in the bill, a company in possession of a phone number without further other information could claim that it does not possess personal information. But of course, it is trivial with most phone

numbers to conduct a reverse look-up on the Internet and determine the actual person associated with the phone number. It would be absurd for the company to claim that it had no actual knowledge of who the person might be because if a breach would occur and the number released, it would be easy for the person who obtains the phone number to conduct the reverse look-up.

Since the current definition excludes such a breach, the bill not only fails to protect consumers in cases that carry equivalent risk of identity theft, but also undermines the goals of the bill.

A second scenario also demonstrates how easily data brokers can rely on this definition of personal information to avoid their obligations under the bill. A data broker could maintain unencrypted name, phone number, and address records in one file, and unencrypted social security number, financial account number, and driver's license number records in another file. If the first file were breached in one instance, and the second in a separate instance, according to the current definition, no personal information has been breached. Yet this scenario poses an extreme risk of identity theft, fraud, or other unlawful conduct, and should trigger both the information security and breach notification provisions of the bill.

We have proposed a revised definition for "personal information" that is based on the simple concept that personal information means "information that identifies or could reasonably identify a particular when joined with other publically available information." Several examples could be included in the act to make clear the types of data that make it possible to identify individuals.

Congressman Rush asked:

Section 4(c) of H.R. 2221 provides that it will be an affirmative defense to a law enforcement action brought under the Act's data breach notification provisions that all of the information that was subject to the breach was information acquired from public records. Thus, if a database is compromised that is made up exclusively of public records such as bankruptcy documents, criminal histories, property records, court filings, and other documents with sensitive personal information consumers will not be notified. If the same or even less information is in another database, consumers would receive notice. Does this distinction based on the original source of the information make sense? What are the benefits of this affirmative defense?

The distinction between public and non-public records does not make sense in the context of this bill, and, for at least three reasons, there should be no affirmative defense for a data breach irrespective of the source of the data.

First, a data breach—*any* data breach—signals a failure in the data broker's information security system, and it makes no sense to allow the data broker to evade the bill's obligations simply because the information was acquired from public records.

Instead, any time a data broker experiences a data breach, that information should be communicated both to the individuals whose information was acquired or accessed without authorization, and to the public pursuant to section 3(g)'s provision regarding publication on the FTC Web site.

Second, personal information contained in public records can still be highly sensitive, particularly when compiled from many sources. If a data broker combines information from multiple public sources in a single database, a breach would pose the same risk of identity theft, fraud, or other unlawful conduct as a breach of information that was not in the public record.

Third, it is not clear that inclusion of this affirmative defense confers any benefits other than to corporations that maintain inadequate security safeguards. This bill is about protecting consumers, not the data brokers who lose their information. Because this affirmative defense does not advance that goal, but in fact works against it, the provision should be removed from the bill.

The overarching goal of this bill is to protect consumers, and from a consumer's standpoint, it makes no difference whatsoever how a data broker acquired his or her personal information; what matters is that the information was accessed or acquired without authorization.

Thank you for the opportunity to participate in the hearing and to provide additional information for the Committee.

Sincerely,

Marc Rotenberg
Executive Director

○