DATA RETENTION AS A TOOL FOR INVESTIGATING INTERNET CHILD PORNOGRAPHY AND OTHER INTERNET CRIMES

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JANUARY 25, 2011

Serial No. 112–3

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
63–873 PDF WASHINGTON : 2011

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

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM REED, New York
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
DEBBIE WASSERMAN SCHULTZ, Florida

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
DEBBIE WASSERMAN SCHULTZ, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

JANUARY 25, 2011

DATA RETENTION AS A TOOL FOR INVESTIGATING INTERNET CHILD PORNOGRAPHY AND OTHER INTERNET CRIMES

TUESDAY, JANUARY 25, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Smith, Gohmert, Goodlatte, Lungren, Poe, Griffin, Marino, Adams, Quayle, Scott, Conyers, Johnson, Chu, Deutch, Wasserman Schultz, and Quigley.

Staff Present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Arthur Radford Baker, Counsel; Sam Ramer, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Liliana Coronado, Counsel; Ron LeGrand, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will come to order. Welcome to the first hearing in the 112th Congress of the Subcommittee on Crime, Terrorism and Homeland Security.

I would especially like to welcome our witnesses and thank you for joining us today.

I am joined today by my colleague from Virginia, the distinguished Ranking Member of the Subcommittee, Bobby Scott; by the Chairman of the full Committee, Lamar Smith from Texas; and the Chairman emeritus, John Conyers of Michigan.

Today's hearing examines the role of data retention as a law enforcement tool to investigate the distribution of child pornography on the Internet and other online crimes. Many Internet Service Providers, ISPs currently retain data that can be used to identify the operator or user of an illegal Web site. But not all ISPs retain this important data, and the length of time such data is retained often varies from one provider to the next.

The issue of data retention is not new. In 1999, then Deputy Attorney General Eric Holder said that certain data must be retained by ISPs for reasonable periods of time so that it can be accessible to law enforcement. In the 12 years since Mr. Holder's endorsement of data retention by ISPs, the size, scope and accessibility of the Internet has increased exponentially. The criminals can now use

the Internet to facilitate almost any crime, including illegal gambling, cigarette and prescription drug distribution, and child exploitation. These criminals have the luxury of cloaking themselves in the anonymity that the Internet provides, making their apprehension significantly more difficult.

When law enforcement officers begin an investigation and develop information that will assist in identifying an offender, they are often frustrated to find that information relating describer information or information that would otherwise identify the perpetrator is not retained in a uniform manner. Current law already requires providers to preserve such data upon the request of law enforcement, but the preservation of data only works if the data has been retained.

Internet crimes are often complex, multi-jurisdictional and international. This can result in protracted investigations before law enforcement officers are in a position to request data from the providers. When the information is developed sufficiently to point investigators to the records they need, it may be too late. Without uniform retention, the records that are desperately needed to attribute communications to a certain person or computer may be lost forever.

This issue not only impacts Federal investigations of online crimes and national security matters but State and local law enforcement investigations as well.

The International Association of Chiefs of Police adopted a resolution in 2006 expressing its support for data retention to aid in the investigation of crimes facilitated or committed through the use of the Internet and telephony-based communication services. Providing law enforcement officers with an expectation that certain data will be available ensures that our very limited police resources are properly assigned and are not sent on wild goose chases for information that no longer exists.

Simply put, no matter what type of investigation it is, investigators ultimately have to identify the person at the keyboard. The service providers hold the key to identifying the person behind the screen name, an e-mail address or an Internet protocol address. Retention of their records is paramount to fighting crime in an Internet age.

It is now my pleasure to recognize for his opening statement, the Ranking Member of the Subcommittee, the gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman, and I look forward to working with you, as the new Chairman of the Subcommittee. Today's hearing is meant to be an informational and fact-finding proceeding to help us begin the conversation about the desirability, feasibility and consequences of retaining data regarding a consumer's Internet use.

No one disputes that mandated data retention can help the identification and prosecution of those who engage in trafficking of child pornography on the Internet. The question is whether we—the question we should seek to answer however is how we can best investigate such crimes, consistent with the rights and liberties of all in society and consistent with the cost-benefits of such a policy.

While we want to ensure the legitimate needs of law enforcement are met to allow to investigate and prosecute offenders who use the Internet to commit crimes, particularly those who use it to commit sex crimes against children, it is critical to understand the nature and scope of any problem under current law before we purport to fix it.

Currently many companies already retained significant amounts of subscriber data, some up to 12 months. Nonetheless there is lack of empirical research about law enforcement's requests under current law and the instances in which data is not available.

We should also review what law enforcement is doing with information that they presently have. I have been informed that the private industry already forwards over 100,000 leads a year to law enforcement, and less than 10,000 prosecutions have been brought in the last 3 years. If we are looking for the proverbial needle in a haystack, the last thing we need is more hay.

As we review the current situation, we should also recognize that there is a lack of clarity about the types requests that law enforcement is presently making and whether much of the desired information is already available.

For these reasons, we should consider whether we need a comprehensive study of data retention, including current practices and the costs associated with the various proposals of data retention policy, among other questions. Some of the questions are, what kind of data we are talking about retaining, whether it is all the content or just the site information? This way we will ensure that the public policy ultimately adopted will be an evidence-based, cost-effective policy.

But apart from technological and practical issues that must be addressed, if we are to consider such policy, there are other costs, societal costs, associated with data retention. There are approximately 230 million Americans who use the Internet, and there are serious privacy and First Amendment concerns that are implicated in this discussion. We must ask ourselves whether it is prudent to require telecommunications companies to retain large amounts of personal and sensitive information, which would be attractive targets for computer hackers, about millions of Internet users in order to get a miniscule number of users who engage in crimes against children online. We need to consider alternative policies that specifically target those suspected of wrongdoing without requiring that innocent consumers compromise their rights to privacy and free speech when they choose to use the Internet.

The notion of preserving large amounts of what amounts to be virtual potential crime scenes is a backward and possibly ineffective way to go about going about the important business of protecting our children. This is particularly true when the unintended collateral consequences of such a policy on industry, private interests, and on free speech may be substantial, as some of the witnesses will explain today.

And when we consider the rights of privacy about retained data, we should also consider—we should also take the opportunity to consider retaining information on gun purchases by those enjoying their Second Amendment rights.

Final point to keep in mind in our discussion is that several aspects of the mandated data retention policy run counter to the idea that we should always consider the cost-benefit implications of any new regulations. Data retention policy can be expensive. This is a huge government expense. And just to get a sense of the possible costs, Congress appropriated $500 million to implement the Communications Assistance Law Enforcement Act a few years ago. This did not involve ongoing costs such that data retention will. Should the industry be expected to absorb some of the costs, we should be clear about what the costs are and what the benefits will be.

So I look forward to hearing testimony from our witnesses and hope we can have a productive conversation about the complexities of data retention policies.

Thank you, Mr. Chairman, for holding the hearing today.

Mr. SENSENBRENNER. Thank you, Mr. Scott.

The Chair now recognizes the distinguished Chairman of the Committee, the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, like you, I thank our witnesses for being here today, and it is nice to be on the same side as the Administration, or maybe I should say, I am glad they are on our side, but it works well regardless.

Also I want to mention, Mr. Chairman, that I heard Mr. Scott's remarks right now, and I am absolutely confident that we will be able to find that balance between protecting privacy and also protecting children. Mr. Scott mentioned having a productive conversation on that subject, and I look forward to that as well.

Mr. Chairman, it may be difficult to believe, but according to the U.S. Justice Department, trafficking of child pornography images was almost completely eradicated in America by the mid-1980's. Purchasing or trading child pornography images was risky and almost impossible to undertake.

The advent of the Internet reversed this accomplishment. Today child pornography images litter the Internet, and pedophiles can purchase, view or exchange this disgusting material with virtual anonymity.

Parents who once relied on the four walls of their homes to keep their children safe are now faced with a new challenge. The Internet has unlocked the doors and opened windows into our homes. FBI Director Robert Mueller told this Committee in April 2008 that, "Just about every crime has gravitated to the Internet, and in certain cases the Internet has provided the vehicle for expansion that otherwise would not be there, and this is certainly true with child pornography."

The statistics reflect just how serious the problem of child exploitation has become. Since the National Center for Missing & Exploited Children, NCMEC, created the cyber tip line 12 years ago, electronic service providers have reported almost 8 million images and videos of sexually exploited children. According to that organization, child porn images increased 1,500 percent between 1995 and 2005, an average increase of over 100 percent a year. The number of reports to a cyber tip line of child pornography, child prostitution, child sex tourism, child sexual molestation, and online

sex enticement of children increased from 4,500 in 1998 to 102,000 in 2008. An average increase of over 200 percent per year.

As many as one in three kids have received unsolicited sexual content online, and one in seven children has been solicited for sex online. More robust data retention will certainly assist law enforcement investigators on a wide array of criminal activity, but such a requirement would be especially helpful in the investigation of child pornography and other child exploitation matters. The investigation of these types of cases has become increasingly more complicated, and perpetrators have become increasingly more sophisticated in their methods of concealing their activities.

When law enforcement officers do develop leads that might ultimately result in saving a child or apprehending a pornographer, their efforts should not be frustrated because vital records were destroyed simply because there was no requirement to retain them. Every piece of discarded information could be the footprint of a child predator.

Last Congress I introduced the Internet Stopping Adults Facilitating the Exploitation of Today's Youth, SAFETY, Act of 2009. Among other things, the bill required providers to retain records pertaining to the identity of an IP address user for at least 2 years. It ensures that the online footprints of predators are not erased.

Data retention preserves critical evidence from the online crime scene so that investigators can apprehend the predator and potentially save a child from further exploitation.

The Internet has proved to be of great value in many aspects of our lives, but it has also evolved into a virtual playground for sex predators and pedophiles, and facilitated nearly effortless trafficking of child pornography. The loss of a child's innocence or, even worse, their life is simply too high a price to pay for not retaining certain data for a reasonable amount of time.

I look forward to hearing from our witnesses and working with them to combat one of fastest growing crimes in America.

Thank you, Mr. Chairman, I yield back.

Mr. SENSENBRENNER. The Chair now recognizes the distinguished new Chairman emeritus of the full Committee, the speaker being the old Chairman emeritus, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thanks, Chairman Sensenbrenner.

It is with some reluctance that I join the rank of ex-Chairmen like you, but here we are all together, working.

This bipartisan thing is really getting frightening because we are all waiting with anticipation tonight at 8 o'clock to find out just how far the 44th is carrying this thing.

Already Chairman Smith and the Department of Justice have hooked up people like the Constitution Project, ACLU, and David Cole; I won't mention myself, because I will be sitting next to a Republican tonight, and I don't want to get any flack. But I suppose this hearing is very necessary, but I am impressed with what the Center for Democracy and Technology is doing, along with the other dissidents that I have listed.

I am worried about privacy rights. And data retention creates, as Bobby Scott has said, it creates some big problems, including iden-

tity theft. I think the Internet industry ought to be concerned about this, and let's see where we can go on it.

Now if this cooperation continues in the Committee, this Subcommittee, we have got to look at the Federal prison system. There are a number of other projects that perhaps the Department of Justice and the Subcommittee on Crime can be working on. I look forward to working with all of you on this subject.

Thanks, Chairman Sensenbrenner.

Mr. SENSENBRENNER. Thank you very much.

Without objection, other Members' statements will be made a part of the record.

And without objection, the Chair will be authorized to declare recesses during votes in the House.

It is now my pleasure to introduce today's witnesses.

Jason Weinstein serves as deputy assistant attorney general with the Department of Justice. He has also served as a special investigative counsel in the Justice Department's Office of the Inspector General and as assistant U.S. attorney in the southern district of New York. Mr. Weinstein previously served as chief of the Violent Crime Section in the U.S. Attorney's Office in Baltimore where he developed Project Exile, a multi-agency effort to curb violent crime in that state. He received has Bachelors of degree in politics from Princeton and his J.D. From George Washington University Law School in 1994.

Without objection, Mr. Weinstein's statement and the other witness's statements will appear in the record.

Each witness will be recognized for 5 minutes to summarize their written statement, and the Chair recognizes Mr. Weinstein.

TESTIMONY OF JASON WEINSTEIN, DEPUTY ASSISTANT ATTORNEY GENERAL, UNITED STATES DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. WEINSTEIN. Good morning, Chairman Sensenbrenner, Chairman Smith, Chairman Emeritus Conyers, and Ranking Member Scott, and Members of the Subcommittee.

And Mr. Chairman, although I was rooting for the Bears, let me congratulate you on the Packers making the Super Bowl.

Mr. SENSENBRENNER. You are forgiven.

Mr. WEINSTEIN. As we all know, the explosive growth of the Internet and other modern forms of communication has revolutionized nearly every aspect of our lives, but at the same time, it has also revolutionized crime.

Increasingly the Internet and other forms of electronic communication are exploited by criminals to commit a staggering array of crimes, from hackers who steal tens of millions of bank card numbers to gang members who issue orders to murder their rivals to predators who sexually abuse children and post images of that abuse online and, of course, to terrorists.

These criminals take advantage of the Internet because of its global nature and because of the speed with which it allows them to operate. Unfortunately, as an added benefit to them, the Internet also affords them a kind of anonymity.

Federal, State and local law enforcement officers who investigate and prosecute these crimes need to have certain information about

the identities and the activities of these criminals who commit them in order to identify and arrest the perpetrators. That information is noncontent data; that is, it is data about the criminals and their communications with others as opposed to the content of those communications.

The government, under current law, is allowed to use lawful process, which is typically a subpoena, a court order or search warrant, to require providers to furnish that data. But those authorities are only useful if the data is still in existence at the time the government seeks to obtain it. And for that reason, data retention by companies that provide the public with Internet and other communication services is fundamental to our ability to protect public safety.

Currently, despite the diligent and efficient work by law enforcement officers at all levels, critical data has too often been deleted by providers before law enforcement can obtain that lawful process. This gap between providers' retention practices and the needs of law enforcement can be extremely harmful to investigations that are critical to protecting the public from predators and other criminals.

And the problem is exacerbated by the complexity of investigating crimes committed using online means. These crimes are difficult to detect, and they may not be discovered or reported to law enforcement until months and months have gone by.

And they are even more difficult to investigate. They often involve the time-consuming process of obtaining evidence from overseas. They often require months and months of work obtaining records from a series of providers as agents attempt to follow the trail of steps used by criminals to try to cover their tracks and render themselves anonymous.

Unfortunately, when providers have not retained the data that is needed for a sufficient period of time, important investigations of serious crimes may come to a dead end. To be sure, most providers are cooperative with law enforcement, and for that, we are appreciative. Many providers, in fact, already collect the types of data that we need to solve crimes, because they use that data to operate their networks or for other commercial purposes. The problem is often simply that that data is not retained long enough to meet the needs of public safety.

However, some providers simply don't retain the needed data at all. Provider retention policies that are in place vary widely across the industry, and they are subject to change at will. In short, the lack of adequate, uniform and consistent data retention policies threatens our ability to use the legal tools Congress has provided to law enforcement to protect public safety.

Now, in setting the retention policies and practices, companies are often motivated by a completely understandable desire to control costs and to protect the privacy of their users. But those factors must be balanced against the cost to public safety of allowing criminals to go free. And truly protecting privacy requires not only that we keep personal information from the criminals who seek to steel it but also that we ensure that law enforcement has the data that it needs to catch and prosecute those same criminals.

Developing an appropriate and effective data retention requirement will mean balancing all of the interests involved: balancing the impact on privacy, the provider costs associated with retaining data for longer periods, and the cost to public safety when critical data noncontent data has been deleted. Congress has a critical role to play in fostering that discussion and in balancing those interests, and today's hearing is an important step in that process.

As we embark on this discussion, it is important to be clear that this debate is not about giving the government, not about giving law enforcement new authorities. It is simply about making sure that data is available when law enforcement seeks to use the authorities that Congress has already provided.

My primary goal here today is to explain the nature of the public safety interest in data retention. Today I am not in a position to propose a particular solution, but the Justice Department looks forward to working with Congress, with industry, and with other interested groups as we seek to develop just such a solution.

I thank you for the opportunity to discuss this important issue with you this morning, and I would be pleased to answer your questions at the appropriate time.

[The prepared statement of Mr. Weinstein follows:]

PREPARED STATEMENT OF JASON WEINSTEIN

Department of Justice

STATEMENT OF

JASON WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED

"DATA RETENTION AS A TOOL FOR INVESTIGATING INTERNET CHILD PORNOGRAPHY AND OTHER INTERNET CRIMES"

PRESENTED

JANUARY 25, 2011

TESTIMONY OF DEPUTY ASSISTANT ATTORNEY GENERAL JASON WEINSTEIN

Good afternoon, Subcommittee Chairman Sensenbrenner, Committee Chairman Smith, Ranking Member Scott, and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice. We welcome this opportunity to provide our views about data retention by companies that provide the public with Internet and cell phone services. I am particularly pleased to be able to speak with you about data retention, because data retention is fundamental to the Department's work in investigating and prosecuting almost every type of crime.

In offering this testimony, our goal is explain the nature of the public safety interest in data retention by providers. We do not attempt to discuss appropriate solutions, evaluate cross-cutting considerations, or evaluate the proper balance between data retention and other concerns. We look forward to continuing the dialog on these important issues with Congress, industry, and other interested organizations.

The harm from a lack of retention

Our modern system of communications is run by private companies that provide communications services. These providers include the companies that sell us cell phone service, the companies that bring Internet connectivity to our homes, and the companies that run online services, such as e-mail. These providers often keep records about who is using their services, and how. They keep these non-content records for business purposes; the records can be useful for billing, to resolve customer disputes, and for business analytics. Some records are kept for weeks or months; others are stored very briefly before being purged. In many cases, these records are the only available evidence that allows us to investigate who committed crimes on the Internet. They may be the only way to learn, for example, that a certain Internet address was used by a particular human being to engage in or facilitate a criminal offense.

All of us rely on the government to protect our lives and safety by thwarting threats to national security and the integrity of our computer networks and punishing and deterring dangerous criminals. That protection often requires the government to obtain a range of information about those who would do us harm.

In discharging its duty to the American people, the Department increasingly finds that Internet and cell phone companies' records are crucial evidence in cases involving a wide array of crimes, including child exploitation, violent crime, fraud, terrorism, public corruption, drug trafficking, online piracy, computer hacking and other privacy crimes. What's more, these records are important not only in federal investigations, but also in investigations by state and local law enforcement officers.

Through compulsory process obtained by law enforcement officials satisfying the requirements of law, the government can obtain access to such non-content data, which is essential to pursue investigations and secure convictions that thwart cyber intrusions, protect children from sexual exploitation and neutralize terrorist threats – but only if the data is still in existence by the time law enforcement gets there.

There is no doubt among public safety officials that the gaps between providers' retention policies and law enforcement agencies' needs can be extremely harmful to the agencies' investigations. In 2006, forty-nine Attorneys General wrote to Congress to express "grave concern" about "the problem of insufficient data retention policies by Internet Service Providers." They wrote that child exploitation investigations "often tragically dead-end at the door of Internet Service Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location." The International Association of Chiefs of Police adopted a formal resolution stating that "the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations." In 2008 testimony before this Committee, FBI Director Robert Mueller reported that "from the perspective of an investigator, having that backlog of records would be tremendously important," and that where information is retained for only short periods of time, "you may lose the information you need to be able to bring the person to justice." Former Attorney General Gonzales similarly testified about "investigations where the evidence is no longer available because there's no requirement to retain the data."

In a 2006 hearing before another committee in this House, an agent of the Wyoming Division of Criminal Investigation gave a heart-wrenching example of the harm that a lack of data retention can cause. He described how an undercover operation discovered a movie, depicting the rape of a two-year-old child that was being traded on a peer-to-peer file sharing network. Investigators were able to determine that the movie had first been traded four months earlier. So, investigators promptly sent a subpoena to the ISP that had first transmitted the video, asking for the name and address of the customer who had sent the video. The ISP reported that it didn't have the records. Despite considerable effort, the child was not rescued and the criminals involved were not apprehended.

In some ways, the problem of investigations being stymied by a lack of data retention is growing worse. One mid-size cell phone company does not retain any records, and others are moving in that direction. A cable Internet provider does not keep track of the Internet protocol addresses it assigns to customers, at all. Another keeps them for only seven days—often, citizens don't even bring an Internet crime to law enforcement's attention that quickly. These practices thwart law enforcement's ability to protect the public. When investigators need records to investigate a drug dealer's communications, or to investigate a harassing phone call, records are simply unavailable.

These decisions by providers to delete records are rarely done out of a lack of desire to cooperate with law enforcement; rather, they are usually done out of an understandable desire to cut costs. Some providers also seem to delete records out of a concern for customer privacy.

Yet, as a result of short or even non-existent retention periods, criminal investigations are being frustrated. In one ongoing case being investigated by the Criminal Division's Child Exploitation and Obscenity Section working with the Federal Bureau of Investigation and Immigration and Customs Enforcement, we are seeking to identify members of online groups using social networking sites to upload and trade images of the sexual abuse of children. One U.S. target of this investigation uploaded child sexual abuse images hundreds of times to several different groups of like-minded offenders – including one group that had thousands of members. Investigators sent legal process to Internet service providers seeking to identify the distributors based on IP addresses that were six months old or less. Of the 172 requests, they received 33 separate responses noting that the requested information was no longer retained by the company because it was out of their data retention period. In other words, 19 percent of these requests resulted in no information about these offenders being provided due to lack of data retention. Indeed, lack of data retention has to date prevented us from identifying the investigation's chief U.S. target.

In October 2008, a federal arrest warrant was issued for a fugitive drug dealer. Law enforcement officers later identified a social networking account used by an associate of the drug dealer. Logins to the social networking account were traced back to IP addresses assigned by a particular cellular provider, revealing that the social networking account was being accessed through that cellular provider's network. A subpoena was sought for data identifying the particular cellular phone number to which the IP addresses were assigned, but the cellular provider was unable to isolate the device by the IP addresses identified, because the data was not there. The inability to identify the specific cellular phone being used to access the social networking account stymied the effort to get the drug dealer off the street.

In many cases, investigations simply end once investigators recognize that, pursuant to provider policy, the necessary records have almost certainly been deleted. This occurs, for example, when a victim of a hacking crime discovers an attack too late, or when evidence of criminal conduct involving the Internet comes to light only after lengthy and complex forensic examination. Unlike burglaries, murders, and arsons, online crimes can be difficult to detect, and even more difficult to investigate. A business that has been hacked may not realize that its customers' identifying information has been stolen until months after the theft. Moreover, investigating online crimes can require obtaining many different records from many different providers in order to pierce the veil of anonymity provided by the Internet. The reason why the government may need access to records months or years after they were made is not because the government is slow or lazy in investigating those crimes, but because gathering the evidence in compliance with federal law – including meeting the statutory thresholds to obtain orders and warrants – takes time.

The current preservation regime

These unfortunate incidents arose under a legal regime that does not require providers to retain non-content data for any period of time, but instead relies upon investigators, on a case-by-case basis, to request that providers preserve data.

Federal law permits the government only to request that providers preserve particular records relevant to a particular case while investigators work on getting the proper court order, subpoena, or search warrant to obtain those records.

This approach has had its limitations. The investigator must realize he needs the records before the provider deletes them, but providers are free to delete records after a short period of time, or to destroy them immediately. If, as has sometimes been the case, a provider deletes the relevant records after just a few seconds or a few days, a preservation request can come too late. For example, suppose agents investigating a terrorist seize a computer and analyze it for evidence of who communicated with the target. If the terrorist has communicated over the Internet with co-conspirators, but those communications are older than the ISPs' retention periods, then investigators lose the ability to use information about the source and destination of those communications to trace the identity of other terrorists. With respect to those communications, provider practices thwart the government's legal authority to preserve evidence.

The current preservation regime also suffers from inconsistent responses from providers. In some cases, providers have been affirmatively uncooperative. In these instances, providers have failed to provide law enforcement agencies with reliable contact information, have ignored preservation requests, and have undermined the confidentiality of investigations by informing customers about preservation requests.

Many of the larger providers have established policies about how long they retain this data. For obvious reasons, I will not testify about how long those periods are for specific providers. I will say that, in general, those periods are rarely longer than a few months, and in some cases are considerably shorter.

Privacy and costs

Data retention implicates several concerns. These include not just the needs of public safety, but also privacy interests and the burden on providers. Imposing greater retention requirements would raise legitimate concerns about privacy, and these concerns should be considered. However, the absence of strong data retention requirements introduces different privacy risks, as the government may be less effective at targeting malicious activities that threaten citizens' private data. Moreover, any privacy concerns about data retention should be balanced against the needs of law enforcement to keep the public safe. In considering those factors, it is important to be clear what data retention is *not* about.

Data retention is not primarily about collecting additional data that is not already collected. Most responsible providers are already collecting the data that is most relevant to criminal and national security-related investigations. In many cases, they have to collect it in order to provide service to begin with. In other cases, they collect it for the company's security, or to research how their service is being used. They simply do not retain that data for periods that are sufficient to meet the needs of public safety.

To be sure, the presence of large databases, by itself, poses privacy concerns. Those databases exist today, but data retention requirements could make them more common. Privacy concerns about those databases might be addressed by tailoring the information that is retained and clarifying the time period for which it is retained. Although we do not have a position on what information should be retained or for how long, the Department would welcome such a discussion.

A discussion about data retention is also not about whether the government should have the ability to obtain retained data. Retained data is held by the provider, not the government. Federal law controls when providers can disclose information related to communications, and it requires investigators to obtain legal process, such as a subpoena or court order and in some cases with a search warrant, in order to compel providers to disclose it.

As members of the Committee may be aware, there is an ongoing discussion about whether those laws strike a proper balance between privacy protection and public safety. I do not address that discussion in these remarks. Yet, whatever one's position in that discussion might be, data retention concerns a different question: Whether, in cases where law enforcement needs to obtain certain types of non-content data to protect public safety, and satisfies the legal standard for obtaining that data, the data will be available for that discrete purpose at all.

Short or non-existent data retention periods mean the data will not be available. Denying law enforcement that evidence prevents law enforcement from identifying those who victimize others online, whether by the production and trade of sexually abusive images of children, or by other online crimes, such as stealing private personal information.

It also can disserve the cause of privacy. Americans today face a wide range of threats to their privacy interests. In particular, foreign actors, including cyber criminals, routinely and unlawfully access data in the United States pertaining to individuals that most people would regard as highly personal and private. Data retention can help mitigate those threats by enabling effective prosecution of those crimes. Cyber criminals, often anonymously, hack into computer networks of retailers and financial institutions, stealing millions of credit and debit card numbers and other personal information. In addition, many Americans' computers are, unbeknownst to them, part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal or foreign adversary. Criminals and other malicious actors can extensively monitor these computers, capturing every keystroke, mouse click, password, credit card number, and e-mail. Unfortunately, because many Americans are using such infected computers, they are suffering from an extensive, pervasive, and entirely unlawful invasion of

privacy at the hands of these actors. Making extensive use of data retained by providers, the Department has successfully investigated and prosecuted criminals who use these techniques to invade the public's privacy.

Unlike the Department of Justice – which must comply with the Constitution and laws of the United States and is accountable to Congress and other oversight bodies – malicious cyber actors do not respect our laws or our privacy. The government has an obligation to prevent, disrupt, deter, and defeat such intrusions. The protection of privacy requires that we keep information from those who do not respect it — from criminals and others who would abuse that information and cause harm. Investigating and stopping this type of criminal activity is a high priority for the Department, and investigations of this type require that law enforcement be able to utilize lawful process to obtain data about the activities of identity thieves and other online criminals. Privacy interests can be undercut when data is not retained for a reasonable period of time, thereby preventing law enforcement officers from obtaining the information they need to catch and prosecute those criminals. Short or non-existent data retention periods harm those efforts.

Providers incur some costs in retaining that data, and although storage costs have been dropping exponentially, it is possible that longer retention periods would impose higher costs. However, when data retention is purely a business decision, it seems likely that the public safety interest in data retention is not being given sufficient weight. There is a role for Congress in striking a more appropriate balance.

Thus, I welcome a discussion about the balance among public safety, providers' needs, and privacy interests. Legitimate debates about privacy protection should not be resolved solely through the "delete" key.

Conclusion

I very much appreciate the opportunity to discuss with you the important role of data retention in helping law enforcement fight crime, improve public safety, and defend the national security while protecting privacy. We look forward to continuing to work with Congress as it considers whether legal changes are needed in this area. I also wish to emphasize that the Administration is in the process of developing comprehensive views on both cybersecurity legislation and potential amendments to the Electronic Communications Privacy Act. Nothing in my testimony should be interpreted to pre-judge the outcome of those discussions.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Committee.

Mr. SENSENBRENNER. Thank you, Mr. Weinstein.

John M. Douglass serves as the chief of police for the Overland Park Police Department in Kansas. He began his law enforcement career with the Overland Park Police Department in 1973. He currently serves as cochair of the National Advisory Committee for the Regional Computer Forensic Lab System. He has served in numerous positions during his tenure with the Overland Park Police Department as well as other various professional positions, including the past president of the Kansas Association of Chiefs of Police.

Chief Douglass has received numerous awards, including the Clarence M. Kelly Award For Excellence in Criminal Justice Administration in 2000, the Evelyn Wasserstrom Award and Clarence Barrow Peacekeeper Award. Chief Douglass received his Bachelor's degree from the University of Kansas and his Masters degree in public administration also from the University of Kansas.

Mr. Douglass.

TESTIMONY OF JOHN M. DOUGLASS, CHIEF OF POLICE, OVERLAND PARK, KS; INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, ALEXANDRIA, VA

Chief DOUGLASS. Thank you, Mr. Chairman, Members of the Subcommittee.

As stated, my name is John Douglass, and I serve as the chief of police in Overland Park, Kansas, a suburb of Kansas City. I am here today on behalf of the International Association of Chiefs of Police, representing over 20,000 law enforcement executives in over 100 countries throughout the world.

I am pleased to be here this morning to discuss the challenges currently confronting the U.S. law enforcement community and our need for further clarity on data retention issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our State highways and streets of our communities each and every day.——

Mr. SCOTT. Could you pull your microphone?

Chief DOUGLASS. Yes, sir, I am sorry.

A great number of these officers also survey the Internet, phone and data logs, and other electronic communication as they investigate crimes. Each day Federal, State, and local tribal law enforcement agencies are investigating cybercrime cases, ranging from bank intrusions, to fraud, intellectual property, terrorism, economic espionage and, unfortunately, innocent images or child pornography crimes.

Data preservation is a key component in any investigation. When criminals access the Internet through an ISP or Internet Service Provider or they send text messages, e-mails and other data, it creates important records and other information. In every case where criminal or civil action is envisioned, there is a clear need to preserve third-party logs and business records related to these connections which specifically demonstrate that a suspect's service provider is connecting with a victim's service provider or through another infrastructure en route.

When law enforcement suspects that a crime has been committed, we request a subpoena, court order or search warrant to obtain critical evidence from the service provider, such as customer records, connection information or stored data.

Take, for example, a case from southern California which would not have been solved without the cell phone data from Verizon Wireless. On July 26th, 2006, 22-year old Tori Vienneau and her 10-month infant son, Dean, were murdered in their two-bedroom apartment in San Diego. Tori was found strangled in her living room, and Baby Dean was found strangled and hung from his crib in one of the adjoining bedrooms.

This horrifying crime scene triggered an exhaustive 18-month investigation. The case was ultimately solved exclusively by the circumstantial evidence, including cell text message content and cell tower data from Verizon Wireless. The defendant denied any involvement in the killings and provided an intricate and extensive alibi.

Investigators focused their attention on Dennis Potts almost immediately because he was rumored to have had dinner plans with Tori on the night of her murder. Mr. Potts denied these rumors of dinner plans, and the victim's cell phone was examined for any text messages between the two of them supporting or refuting such rumors.

In a most interesting twist, all incoming and outgoing text messages prior to 6:30 p.m. on the night of the killings had been deleted. The victim's cell phone provider was contacted, but the text message content was not stored by the cell provider and, therefore, could not be recovered that way.

Over the ensuing months, the victim's phone was subjected to be extensive forensic analysis in the hopes of recovering some of these message. The defendant's cell phone carrier, Verizon Wireless, was also contacted, and investigators were told incoming text message content, victim-to-defendant text only, was preserved for only 3 to 5 days. But in a stroke of good luck, this incoming data still existed and was preserved.

And it later proved to be pivotal in proving the defendant's guilt. The text message content proved not only that the defendant lied to investigators and that the two did in fact have plans to meet that evening, but also that the defendant was checking to see if the victim and her son were alone in the apartment.

Verizon also provided the cell tower data from the defendant's phone. This data, coupled with some additional testing, showed the defendant's alibi was false, and he was not where he said he was. Furthermore, at the time of the killings, his cell phone pinged off a cell tower only 500 yards from the victim's apartment. This became the single most important piece of evidence in linking the defendant to the killings.

Clearly, preserving digital evidence is crucial in any modern day criminal investigation. While law enforcement does have success obtaining evidence through the appropriate legal process, because we are extremely aware of spoliation concerns, we are not always successful. Many times we face obstacles in our investigations, from the differing locations of victims to their locations of the perpetrators.

In closing, Federal, State, tribal and local law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism both online and in our streets, but we cannot do it alone. We need the full support and the assistance of the Federal Government and clear guidance and regulations on data retention to aid us in successfully investigating and prosecuting the most dangerous of criminals.

[The prepared statement of Chief Douglass follows:]

PREPARED STATEMENT OF JOHN M. DOUGLASS

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief John M. Douglass

Chair, Mid-Sized Cities Section
International Association of Chiefs of Police

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

United States House of Representatives

January 25, 2011

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning Mr. Chairman and Members of the Subcommittee,

My name is John Douglass and I serve as the Chief of Police in Overland Park, Kansas, a suburb of Kansas City. I am here today on behalf of the International Association of Chiefs of Police representing over 20,000 law enforcement executives in over 100 countries throughout the world. I am pleased to be here this morning to discuss the challenges currently confronting the U.S. law enforcement community and our need for further clarity on data retention issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our state highways and the streets of our communities each and every day. A great number of those officers also survey the Internet, phone and data logs and other electronic communication as they investigate crimes. Each day, federal, state, local and tribal law enforcement agencies are investigating cyber crime cases ranging from bank intrusions to fraud, intellectual property, terrorism and economic espionage, and, unfortunately "innocent images," or child pornography crimes.

Data preservation is a key component in any investigation. When criminals access the Internet through an ISP (or Internet Service Provider), send text messages, emails and other data, it creates important records and other information. In every case where criminal or civil action is envisioned, there is a clear need to preserve third party logs and business records related to connections which specifically demonstrate that a suspect's service provider is connecting with a victim's service provider or through another infrastructure en route.

When law enforcement suspects that a crime has been committed, we request a subpoena, court order, and search warrant etc. to obtain critical evidence from a service provider such as, customer records, connection information and stored data.

Take, for example, a case from Southern California which would not have been solved without the cell phone data from Verizon Wireless:

On July 26, 2006 22 year old Tori Vienneau and her 10 month infant son, Dean were murdered in their 2 bedroom apartment in San Diego. Tori was found strangled in her living room and baby Dean was found strangled and hung from his crib in one of the adjoining bedrooms. This horrifying crime scene triggered an exhaustive 18 month investigation.

The case was ultimately solved exclusively by the circumstantial evidence, including cell text message content and cell tower data from Verizon Wireless. The defendant denied any involvement in the killings and provided an intricate and extensive alibi.

Investigators focused their attention on Dennis Potts almost immediately because he was rumored to have had dinner plans with Tori on the night of her murder. Mr. Potts denied these rumors of dinner plans and the victim's cell phone was examined for any text messages between the two of them supporting/refuting such rumors. In a most interesting twist, all incoming and outgoing text messages prior to 6:30 pm on the night of the killings had been deleted. The victim's cell phone provider was contacted, but the text message content was not stored by the cell provider and therefore could not be recovered that way. Over the ensuing months, the victim's phone was subjected to extensive forensic analysis in the hopes of recovering some of these messages.

The defendant's cell phone carrier (Verizon Wireless) was also contacted and investigators were told incoming text message content (victim to defendant texts only) was preserved only for 3-5 days. In a stroke of good luck, this incoming data still existed and was preserved. It later proved to be pivotal in proving the defendant's guilt. The text message content proved not only that the defendant lied to investigators and that the two did, in fact, have plans to meet that evening, but also that the defendant was checking to see if the victim and her son were alone in the apartment.

Verizon also provided the cell tower data for the defendant's phone. This data, coupled with some additional testing, showed that the defendant's alibi was false and he was not

where he said he was. Furthermore, at the time of the killings, his cell phone "pinged" off of a cell tower only 500 yards from the victim's apartment. This became the single most important piece of evidence linking the defendant to the killings and to is ultimate conviction in September, 2009.

Clearly, preserving digital evidence is crucial in any modern-day criminal investigation.

While law enforcement does have success obtaining evidence through the appropriate legal process—because we are extremely aware of spoliation concerns—we are not always successful.

Many times we face obstacles in our investigations—from the differing locations of victims vs. perpetrators to the time when we request the information. Additionally, there are cases where we are not able to work quickly enough—mostly because a "lead" is discovered after the logs have expired or we are unaware of the specific service provider's protocols concerning data retention time periods.

For example, while most service providers save data for 30 days, there is no national standard and not all providers follow the 30 day rule. We are aware of specific ISPs who only save data for 15 days. 30 days is cutting it close many times depending upon when a victim reports a crime or when we discover a crime has been committed. So, as you can imagine, data preserved for a small window of time anything less than that can translate into a headache for law enforcement.

Also troublesome is that, when we are dealing with crimes committed online, often we have difficulty locating the ISP, as their servers can be located anywhere in the world. These days, online criminals operate internationally and electronic evidence can be virtually untraceable. Additionally, because laws differ internationally, obtaining information from foreign ISPs can often be difficult due to another country's retention practices.

Here are a few examples of cases where we have needed information from several different service providers located in many countries:

In a recent case, an international suspect hacked into United States based systems through systems in the United Kingdom. In this instance, data logs were located at the suspect's location in Europe, in the server's location in the UK, as well as victim locations in the US. Because all of these logs are essential to prosecution, search warrants were immediately issued for all parties in order to secure evidence which could spoil long before the arrest of a suspect.

In another case, an IP—or Internet Protocol— was stolen from a fortune 500 corporation and attempted to be sold to competitors—the suspect was in the Middle East and the victim company was in the US. Data logs and business records for connections, email accounts, online payment processors, etc. are all critical evidence. In this case, subtle nuances were important—when a web mail account was created versus the IP accessing the account are normally only established through log and related data has a lifecycle for retention and can easily spoil.

In both of these cases, we were lucky—had there been insufficient data retention to allow normal law enforcement efforts to legally obtain logs, the cases would not have been possible to successfully investigate or prosecute.

In closing, federal, state, tribal and local law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism—both online and in our streets, but we cannot do it alone. We need the full support and assistance of the federal government and clear guidance and regulations on data retention to aid us in successfully investigating and prosecuting the most dangerous of criminals.

Thank you.

Mr. SENSENBRENNER. Thank you very much, Chief.

Kate Dean serves as the executive director of the United States Internet Service Provider Association. Ms. Dean has been active in telecommunications and Internet policy in Washington, D.C., for more than 10 years and is a member of the International Academy

of Digital Arts and Sciences. She started her own firm in 2006, where, in addition to continuing to work with US ISPA, she volunteers with an organization in Singapore that brings healthy sanitation solutions to underserved villages in the developing world. And he received her bachelor degree in 2000 from American University.

Ms. Dean.

TESTIMONY OF KATE DEAN, EXECUTIVE DIRECTOR, UNITED STATES INTERNET SERVICE PROVIDER ASSOCIATION, WASHINGTON, DC

Ms. DEAN. Chairman Sensenbrenner. Ranking Member Scott.

Mr. SENSENBRENNER. Could you pull the mike a little closer to you?

Ms. DEAN. I sure can.

Mr. SENSENBRENNER. Thank you.

Ms. DEAN. My name is Kate Dean, and I am the executive director of the United States Internet Service Provider Association or US ISPA. Since January 2002, our members major Internet service, network and portal providers, have focused on policy and legal concerns related to law enforcement compliance and security matters, including ECPA, CALEA, cyber security and notably the fight against online child exploitation. For years US ISPA and our members have participated in efforts to examine the issue of data retention, particularly in a content of child exploitation, including past dialogues with the Department of Justice and with State and local law enforcement.

We welcome the opportunity to continue the discussion today. Before addressing data retention, I would like to tell you about our efforts in the child protection arena. In 2005, we published "Sound Practices for Reporting Child Pornography," a joint project between US ISPA and the National Center for Missing & Exploited Children.

We updated those practices to reflect new requirements put in place by the 2008 passage of the Protect Our Children Act, a bill US ISPA strongly supported.

Last year we developed sound practices for subpoena compliance with the National Association of Attorneys General. We also supported the Online Safety and Technology Working Group, which reported to Congress in June with their examination of industry reporting practices and data retention.

US ISPA members have been active in various internet safety task forces, including the Technology Coalition and the Financial Coalition Against Child Pornography. Members maintain 24-by-7 response capabilities, offer law enforcement guides, frequently interact with the ICAC and conduct training for investigators and prosecutors.

As I hope our actions demonstrate, US ISPA is committed to the fight against online child exploitation. And we support law enforcement efforts to bring online criminals to justice, especially those who harm children. We fully appreciate the critical role that electronic evidence plays in those efforts.

Service providers report tens of thousands of incidents of apparent child pornography each year to NCMEC. And because of the Protect Our Children Act, all providers are now required to sent ro-

bust reports, including subscriber information, historical and geographic data, and the images themselves through NCMEC's cyber tip line.

At the time of receipt, providers automatically preserve the account and hold onto data for 90 days, awaiting legal process. The novel approach to preservation adopted in the reporting statute was derived from preservation authority that has long existed in the Electronic Communications Privacy Act. ECPA gives law enforcement the authority to require providers to preserve evidence needed for investigations for up to 180 days without issuing legal process. We believe that effective use of preservation, a targeted, valuable tool, is key to addressing law enforcement's needs.

US ISPA has carefully examined past data retention proposals and each time has concluded that a uniform retention mandate is certain to present significant challenges to the communications industry, as well as myriad unintended consequences. These challenges include the potential conflict of new obligations and regulatory burdens; new questions about user privacy and the standards for law enforcement access to stored data; technical and security risks; and delay when retrieving data, all which could negatively effect law enforcement investigations.

Many of these challenges have plagued the European Union's attempt at implementation of its data retention directive. As we discuss the issue here today, a similar dialogue is taking place within the EU as they reassess their approach and consider alternatives, like preservation.

Unlike preservation, data retention raises tough questions about breadth, scope, duration, liability and costs, costs that go well beyond mere dollars. These are all critical considerations that require close examination by industry and by Congress.

In closing, US ISPA remains committed to an open dialogue, but we have concerns about the effectiveness and implementation of mandatory data retention. We worry about the indirect costs to innovation, privacy and the speed and accuracy of investigations. Based on our experiences, we continue to believe that targeted approaches like preservation are the best and most effective use of available resources. We appreciate this opportunity to present our views on this topic and look forward to working with you and your staff.

[The prepared statement of Ms. Dean follows:]

PREPARED STATEMENT OF KATE DEAN

Written Testimony

of

Kate Dean

United States Internet Service Provider Association

Before the

U.S. House of Representatives

Committee on the Judiciary

Subcommittee on Crime, Terrorism and Homeland Security

"Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes"

January 25, 2011

My name is Kate Dean and I am appearing here today to represent the United States Internet Service Provider Association ("US ISPA") where I am the executive director. US ISPA is a unique-member driven organization that was founded in January 2002 based on successful collaboration by service provider attorneys on the first USA PATRIOT Act. The association was established to focus on a discrete set of policy and legal concerns common to major Internet service, network and portal providers. US ISPA works primarily on law enforcement compliance and security matters – including ECPA, CALEA, and cybersecurity – and notably, in the fight against online child exploitation.

With our focus on law enforcement compliance issues, it is only natural that US ISPA members are interested in participating in discussions regarding data retention. In fact, our members and US ISPA itself have participated in many efforts seeking to address data retention, including past dialogues between industry and the Department of Justice and with state and local law enforcement through the Internet Crimes against Children ("ICAC") Taskforces and the National Association of Attorneys General. We welcome the opportunity to continue the dialogue today.

We are interested in hearing from fellow panelists about the challenges that law enforcement face when conducting investigations that may rely on data from our member companies. We hope that through open discussion of these issues, we may be able to develop solutions that can address law enforcement's needs without any unnecessary negative impact on business interests or the privacy of our customers.

Over the years US ISPA has carefully examined data retention proposals, and has come to the understanding that a blanket legal requirement to retain Internet usage data for established time periods is certain to present significant challenges to the communications industry, both for well-established companies and newer online media enterprises, as well as unintended consequences which are incapable of precise identification. Nevertheless, US ISPA has achieved success in connection with targeted legislative directives aimed at a specific law enforcement challenges. Once such recent success grew out of US ISPA and its members' efforts to help law enforcement and other constituencies battle crimes against children.

It is safe to say that US ISPA and its members are industry leaders in the fight against online child exploitation. In 2005, the organization led the way by developing and publishing Sound Practices for Reporting Child Pornography, created through a joint project between US ISPA and the National Center for Missing and Exploited Children ("NCMEC") to educate the Internet Service Provider ("ISP") community on its obligations to report incidents of apparent child pornography. US ISPA recently updated its Sound Practices to reflect the changes to reporting and preservation procedures introduced by the PROTECT Our Children Act, passed by Congress in 2008. US ISPA strongly supported that Act and its legislative acknowledgment of US ISPA's long recommended practices for child pornography reporting. US ISPA and its members provided draft language, brainstormed ideas, and testified in hearings to support the efforts to clarify provider child pornography reporting obligations.

Our members were also active in the Online Safety and Technology Working Group ("OSTWG") created by Congress that same year. The OSTWG was tasked with examining the state of online safety education, parental controls, industry reporting mechanisms and data retention. The OSTWG report was presented to Congress in June 2010 and is available online at the National Telecommunications and Information Administration website. US ISPA members have also been active in efforts such as the Internet Safety Technical Task Force, the Technology Coalition, the Virginia Attorney General's Internet Safety Task Force, and the Financial Coalition against Child Pornography.

US ISPA has also worked on these issues directly with state and local law enforcement. Members frequently interact with the ICAC Taskforces, conducting training and attending meetings and conferences. In addition, US ISPA was instrumental in working with the National Association of Attorneys General to develop ISP Sound Practices for Subpoena Compliance. The ISP Sound Practices for Subpoena Compliance provides the ISP community with guidance regarding how companies can respond to law enforcement requests in a manner that assists law enforcement within the framework of the Electronic Communications Privacy Act ("ECPA").

US ISPA member companies continually demonstrate their commitment and leadership through industry efforts to promote cooperation with law enforcement. Members maintain 24x7 response capabilities, offer law enforcement guides to lawful data disclosures under ECPA, conduct training for investigators and prosecutors, and maintain an open dialogue with all levels of federal, state and local law enforcement.

As this long history of contribution and cooperation makes clear, among industry associations, US ISPA is exceptionally committed to supporting law enforcement efforts to bring to justice those who use the Internet for criminal benefit, and most of all, those who harm children. And we fully recognize and appreciate the critical role that electronic evidence plays in those efforts.

It is our hope that by discussing the challenges associated with generalized data retention proposals, we can further a productive dialogue about how industry and law enforcement can continue to work together to increase the chances of successful investigations and prosecutions.

Indeed, beginning the discussion with uniform mandatory data retention proposals may be counter-productive. Every time industry has seriously examined how it might operationalize broad data retention mandates, it has concluded that such an undertaking is dramatically overbroad and fraught with legal, technical and practical challenges. I would like to highlight a few of those challenges.

Mandatory data retention presents complex challenges and risk

First, I would like to address the issue of over breadth. Mandatory data retention requirements potentially require an entire industry to retain billions of discrete electronic records due to the possibility that a tiny percentage of them might contain evidence related to a crime. While we certainly agree that the potential criminal activity could be serious and should be investigated, we think that it is important to weigh that potential value against the impact on the millions of innocent Internet users' privacy. The privacy issues that will be raised by a data retention proposal could include questions regarding the legal standard by which law enforcement and other parties could subpoena such data and whether retention obligations would create new needs for additional privacy and security regulation. Indeed, retention could bring with a whole new rash of complex regulatory and legal requirements that go far beyond simply saving data.

Potential legal considerations aside, from a practical perspective the sheer volume of data alone makes the task of gathering and storing such data daunting. Many providers have hundreds of thousands of users, some millions, and others hundreds of millions. There are more than 250 million Internet users in North America alone. These users access and use their networks all day, every day of the year. As the technology industry innovates, new devices, such as e-readers, tablets and game devices, continue to multiply the number of ways that each of these users can access the Internet. Today, it is not uncommon for a user to use Internet-based services through multiple devices simultaneously. Access options are multiplying as well. Wired or wireless, network providers now include hotels, airlines, municipalities, libraries, universities, and the family-owned coffee shop on the corner. Imagine how many log-ins a top-tier service provider sees over a 24-hour span today. Now imagine how many log-ins they'll see in a 24-hour span in 6 months. The growth could be exponential.

Maintaining exponentially-increasing volumes of data, in a searchable format that would enable companies to quickly locate a targeted user's data amidst exabytes of information, would be extremely complicated, and burdensome. While storing huge volumes of data may be possible, providers have concerns about ensuring the integrity and availability of that data to respond to legal demands. The sheer complexity of systems required to perform these tasks increases the probability of crashes, failures, and delays. Thus, despite a provider's efforts to comply with the data retention obligation, the data, through no fault of the provider, may still not be available to law enforcement.

Perhaps the biggest concern for both providers and law enforcement may be the risk impairing provider response times for ordinary legal requests and, more importantly, that their ability to respond promptly in true emergencies could suffer. Those who work day-to-day with law enforcement know how important it is that a provider be able to call up data in seconds in cases involving an emergency where time is of the essence. Data from ISPs can be critical in emergencies, such as child abductions, and providers know that in such cases hours, even minutes, could mean the difference between a child returned home safely and one who never makes it home. For this reason, the longer search times that are likely to result from a data retention mandate are a grave concern.

Finally, we would like to note that many of these challenges have plagued the European Union's attempted implementation of its Data Retention Directive (Directive 2006/24/EC). Legislation implementing the Directive has been the subject of much litigation and, in March of last year, Germany's national data retention law was declared unconstitutional by its Federal Constitutional Court. The EU's Article 29 Data Protection Working Party not long ago issued a report describing the difficulties companies face interpreting and attempting to comply with the varying data retention requirements in each EU country. As we discuss this issue here today, a similar dialogue is taking place within the EU as they re-assess their approach to data retention. Not only are shorter time periods under consideration, but they are also re-examining whether they should abandon broad-based retention in favor of the targeted preservation system used here in the U.S.

Data preservation is a powerful tool for law enforcement that exists today

U.S. law enforcement has long had mechanisms at its disposal to preserve electronic evidence that might be useful for criminal or civil investigations.

The preservation authority in the Stored Communications Act (18 U.S.C. § 2701 *et seq.*) was enacted into law in 1996 and has been used in a wide range of criminal investigations over the past 15 years. Section 2703(f) allows law enforcement, by letter, fax, or email to direct service providers to preserve records and other electronic evidence in their possession pending the issuance of a court order or other legal process. Providers must retain the records requested for 90 days, and this initial period can easily be extended for an additional 90 days upon a renewed request by law enforcement. Thus, today, information and evidence believed to be important to a law enforcement investigation can be preserved with little or no burden on the government to issue formal legal process or even demonstrate relevance.

Preservation authority is a powerful, targeted tool available to law enforcement today that, from the perspective of US ISPA's members, strikes the appropriate balance between the government's need to preserve evidence for a pending investigation and the avoidance of undue burden on ISPs by compelling data retention well beyond the time periods necessary to meet their business needs.

Let me return to the recent success that I alluded to at the beginning of my testimony: a targeted legislative solution that USISPA and its member companies were instrumental in achieving in the context of crimes against children. As this Subcommittee is well aware, Congress recently further refined investigative data preservation authority in this area tool in the PROTECT Our Children Act (18 U.S.C. § 2258(h)). Now, whenever a provider makes a report to the CyberTipline, the report itself will include the basic digital data that law enforcement considers critical to identifying the perpetrator of child pornography crimes.[1]

[1] This data includes identifying information concerning the individual who appears to have committed the crime (such as email address, Internet Protocol address, and any self-reported

Law enforcement need not issue a preservation request in connection with each provider report of apparent child pornography to NCMEC's CyberTipline in order to ensure that important investigative data is preserved. In addition, the statute requires providers to automatically preserve for 90 days both the data contained in the CyberTipline report and additional data that Congress determined to be key to solving crimes against children. Upon notice of NCMEC's receipt of its report, providers must preserve any images or digital files commingled among the images of apparent child pornography within a particular communication or user-created folder or directory.

When the CyberTipline report is made, this electronic evidence is delivered to NCMEC and forwarded to law enforcement, and almost simultaneously preserved by the service provider, without a law enforcement preservation request and even *before* any criminal investigation has begun. Mandatory data retention is therefore assured with respect to all of the evidence accompanying CyberTipline reports, plus all of the associated evidence preserved by the provider in the user's account.

US ISPA recommends that Congress carefully assess the effectiveness of automatic data preservation under section 2258A, once law enforcement has accumulated substantial first-hand experience using the preserved data in prosecuting crimes against children. Only if data preservation proves ineffective in this context should Congress consider a much broader scheme of mandatory data retention which would apply more than 99 percent of the time to records of lawful conduct having nothing at all to with child pornography.

Examining data retention.

Before the Members of this Subcommittee consider imposing a broad mandate on American businesses that abandons the targeted approach of data preservation, we think that a great deal of further discussion is needed. We think that the topics that are critical to address in such discussions are covered entities, scope and duration, liability and cost.

1) Covered Entities

Congress must consider which types of service providers would be subject to any mandate to retain data. A comprehensive mandate would extend to all "electronic communication service" and "remote computing service" providers, as those terms are defined in ECPA. It would encompass a wide spectrum of businesses, from the nation's largest telecommunications companies down to the neighborhood coffee shop offering free WiFi access. It would also include organizations such as employers, universities and

---

identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

government agencies that offer Internet access to their employees or students. Organizations that diverse probably could not fit under a "one size fits all" data retention mandate without adversely impacting small businesses or even larger enterprises that lack the technology resources, surplus revenue, and technical expertise required to comply with the mandate. Yet at the same time, any data retention scheme that does not apply to all these different types of entities would likely fail because it would be so easy for those bent on engaging in criminal activity to avoid creating electronic trails simply by choosing which "on ramp" to the Internet to use.

2) Scope and Duration

Congress must also consider how to define the specific types of data that companies subject to the mandate must retain. Companies generally retain data that they need for business purposes and discard data that is of no commercial value to them. Many providers of online access services require their users to present credentials (such as a username and password) to securely identify themselves. If authentication is successful, the provider assigns a temporary IP address that enables the user to access the Internet or other online resources. Most providers retain this authentication data for billing or security purposes. Some providers, for example, free municipal WiFi systems, do not require authentication at all and thus have no authentication data to retain.

Duration of mandated data retention, like scope, is critical to assessing technical feasibility and cost. Data preservation under the Stored Communications Act and the PROTECT Our Children Act works well because no re-engineering of storage technology or redesign of search techniques has been necessary. Providers are able simply to store limited sets of data, already in their possession, that law enforcement has identified specifically in the preservation request. By contrast, retention of all data subject to mandate for all users of the providers' service gives rise to an entirely different class of technical challenges, creating resource, compliance and cost burdens that increase exponentially the longer the retention period is.

3) Liability and Privacy Concerns

Providers have well-founded concerns over the increased risks of liability associated with a broad legal obligation to retain data. Apart from the risks of data corruption, technical failures and delays engendered by the need to warehouse and manipulate vast quantities of data, the twin concerns of data privacy and security will likely bring additional obligations and risks on top of a data retention mandate. US ISPA is concerned that a data retention mandate would thus bring with it a complex regulatory framework that would impose new, and as of now unforeseen, costs, legal risks, and burdens.

With regard to data privacy and security, we would like to note that there is on-going discussion on both of these issues that could result in new requirements for industry. The recent Federal Trade Commission Staff Report on privacy recommended minimization and rapid deletion of IP address and other data that might reasonably identify Internet users. Similarly, a draft privacy bill circulating in the Senate Commerce Committee would limit the

retention of IP address and other data tied to IP addresses for only so long as necessary for service delivery or fraud prevention. Others urge congressional action to impose federal cybersecurity requirements on providers, to be enforced by private lawsuits for breach of contract or by civil enforcement actions by government agencies. US ISPA is concerned that a data retention mandate would create a "Catch-22" situation involving conflicting requirements, or a cumbersome regulatory framework that would impose new legal risks, burdens and cost to online businesses.

For providers, it will be critical that Congressional action in these areas take into account liability concerns, as well as the interaction of new legal requirements imposed on providers with existing and future legal obligations at the federal, state, and international levels.

4) Cost

Each decision made with respect to coverage, scope, duration and liability will impact the costs associated with data retention. Because the data that industry would be required to maintain is not needed for business purposes – otherwise providers would maintain it without a legal mandate to so do – all costs incurred would be exclusively to satisfy the data retention requirement.

There is no doubt that a data retention mandate will be expensive, but the costs go well beyond mere dollars. Members of the Subcommittee should consider whether providers, especially small and medium-sized companies, can absorb the costs of storing exabytes of data, of no commercial value to them, without undermining their ability to raise capital, serve their existing customers and acquire new ones, and deliver innovative products and services in a rapidly changing environment. Even under the narrowest of mandates, expert technical resources would be diverted from business innovation in order to build, maintain and secure massive data storage and retrieval systems. Cost recovery could address some of the potential negative impact of a data retention requirement, but in many ways reimbursement falls short of compensating industry for the opportunity costs of having their experts diverted away from focus on innovating the next generation of Internet-based services. Nevertheless, effective cost recovery mechanisms are an important part of the conversation.

A Potential Better Way

As Congress considers this complex issue, we suggest an alternative approach that would build on progress in data preservation and voluntary industry efforts on data retention. From our experience working with the data preservation provisions in the PROTECT Our Children Act, we think that there are further opportunities to innovate around the preservation model to address law enforcement needs. In addition, further coordination between industry and law enforcement could help ensure that these methodologies are being used to the their full potential. Finally, we believe that law enforcement continues to need further resources to support child exploitation investigations.

We believe that these approaches hold the greatest promise for improving evidence-gathering and prosecution in child pornography prosecutions, while avoiding many of the difficulties and complexities raised by data retention mandates.

In closing, US ISPA remains committed to continuing the dialogue with law enforcement about how we can contribute to the fight against child exploitation. We do not think that data retention is the best place to focus our energies. Based on our recent experience with the innovative new approach to preservation in the Protect Our Children Act, we believe that preservation is still the best approach to ensuring data is available for law enforcement investigations. We have important questions that would need to be answered by any data retention proposal, including who would be covered, what types of data would have to be saved and for how long, and what types of protections, additional obligations, and costs would come with a retention mandate. We also have serious concerns about the identifiable costs to innovation, privacy, and speed of investigations, and fears about the unknown and unanticipated collateral damage that could be caused by such an obligation.

We thank you for this opportunity to present US ISPA's views on this topic and look forward to continuing to work with the Subcommittee Members and your staff on these issues.

Mr. SENSENBRENNER. Thank you, Ms. Dean.

John B. Morris, Jr., serves as general counsel at the Center for Democracy and Technology in Washington, D.C. He is director of the Internet Standards Technology and Policy Project. He is also involved in the Center for Democracy and Technology's work on cyber security, privacy and neutrality. Prior to joining the center, Mr. Morris was a partner in the law firm of Jenner & Block. Addi-

tionally, Morris has served as director of CDT's Broadband Access Project. He received his Bachelors degree from Yale and his J.D. From Yale Law School. Mr. Morris.

TESTIMONY OF JOHN B. MORRIS, JR., GENERAL COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC

Mr. MORRIS. Thank you very much, Chairman Sensenbrenner, Ranking Member Scott, Chairman Smith and Chairman Emeritus Conyers and the Members of the Committee.

On behalf of the Center for Democracy and Technology, I would like to thank you for the opportunity to testify today. Child pornography is a horrific crime, and we applaud the efforts by this Congress and this Subcommittee to increase the resources available to prosecute this crime.

A data retention mandate would raise a number of serious privacy and free speech concerns. At a time when there is a growing concern about privacy and identify theft, a growing concern about the commercial misuse of personal data and a growing concern about the intrusion of the Federal Government into the personal lives of American citizens, Congress should be very hesitant to require service providers create databases to track the Internet activities of 230 million innocent Americans.

This morning I would like to set aside briefly the privacy and free speech concerns that I addressed in my written testimony and instead focus on the fact that a data retention mandate would harm innovation and competition on the Internet and harm the ability of the American Internet industry to compete in the global online marketplace, which in turn directly effects the ability of users to be able to participate and speak on the online market.

Ms. Dean addressed the data retention concerns that the Internet Service Providers have. Let me look at the other end of the communication and then address proposals by law enforcement that source data be retained by any online services that allow users to communicate with each other. And the proposal that has been made to have services like Yahoo or Google or Facebook retain data is truly breathtaking and would be devastating to the Internet services, both to existing services and certainly to new innovators and startup services.

The reach of the proposal cannot be underestimated. The proposed mandate that would reach most Web sites and online services, including all Web 2.0 sites, all social networking sites, all blogs, all sites that allow political or other commentary, the great majority of e-commerce sites and almost all modern news sites, like the NewYorkTimes.com or FoxNews.com.

And the scale of what law enforcement is proposing is also astounding. Looking just at Facebook as an example, Facebook users post in the neighborhood of 2 billion chat messages every single day. When combined with other postings, Facebook alone would have to create and maintain a data retention database containing more than 1 trillion new records every single year. The size of Facebook's data retention database alone would be larger than all of the content that the Library of Congress has put online to date.

Looking beyond Facebook, in 2009, there were 247 billion e-mail messages sent every single day. And law enforcement is asking Congress to order that every single one of these messages be recorded and tracked. Over the course of a year, this mandate would require a database of more than 90 trillion records. And this does not even include chat or instant messaging, which is supplanting e-mail as a preferred method of person-to-person communications.

Who would pay for this? Internet users would pay for this. And what would the impact of this burden be on online services? Some larger companies might survive, but smaller companies would likely be run out of business. Imposing an unfunded Federal mandate on anyone who allows users to communicate online can only have one result: There will be fewer businesses able to compete in the online marketplace, this will entrench the large providers, harm competition, harm innovation and ultimately harm users. Congress should not mandate the creation of an Orwellian tracking database with hundreds of trillions of records tracking innocent citizens wherever they go online.

As a final critical point addressing the child pornography context, I have worked in this space a fair amount over the last 10 years, and every task force I serve on, every working group I serve on, I learned that law enforcement is overwhelmed with these cases. They don't have enough prosecutorial resources to prosecute all of the cases that they have. And so I really urge the Congress to look at the question as to whether adding more data and more data retention will in fact lead to more prosecutions of this horrific type of crime.

The voluntary retention and data preservation orders allow law enforcement to target suspected criminals, and we urge the Subcommittee not to go down the path of imposing data retention mandates on this entire industry.

[The prepared statement of Mr. Morris follows:]

PREPARED STATEMENT OF JOHN B. MORRIS, JR.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

Statement of **John B. Morris, Jr.**
General Counsel

Center for Democracy & Technology

before the House Committee on the Judiciary,
Subcommittee on Crime, Terrorism and Homeland Security

Hearing on "DATA RETENTION AS A TOOL FOR INVESTIGATING INTERNET CHILD PORNOGRAPHY AND OTHER INTERNET CRIMES"

January 25, 2011

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT),[1] I thank you for the opportunity to testify today on data retention in the context of child pornography investigations.

CDT strongly agrees with the Subcommittee that child pornography is a horrific crime, and we have long supported increasing the resources available for its prosecution. The organization has spent extensive time examining the challenges raised by child pornography and seeking ways to fight this crime that are consistent civil liberties, and with openness, competition, and innovation on the Internet.

Mandatory data retention raises serious privacy and free speech concerns, and would also harm innovation and competition in the online context. We urge this Subcommittee to carefully consider the significant risks posed by a data retention mandate. Congress has already enacted strong data *preservation* requirements, which have proven to be effective tools for combating child pornography, without the panoply of problems raised by data *retention*. Mandatory data retention would cause significant harms and would, at the same time, not likely increase the number of child pornographers that this country is able to prosecute and put in prison.

As detailed below, we believe that mandatory data retention:

- Would harm Americans' privacy rights, both vis-à-vis the government as well as private actors. Beyond inappropriate invasion of privacy, data retention would also aggravate the problem of identity theft.

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. We have long worked to protect children in the online environment while at the same time also protecting online users' privacy and civil liberties. CDT has offices in Washington, D.C., and San Francisco.

- Would harm Americans' free speech rights and would chill Americans from accessing sensitive content online; and
- Would seriously damage competition and innovation in the Internet industry, and would harm the American industry's ability to compete in the global online market.

A vital alternative to data retention is data preservation, which avoids the risks inherent in data retention. It is, in any event, very unclear that adding a data retention regime would in fact lead to more prosecutions of child pornographers. We urge Congress to fully investigate questions about child pornography investigations before it considers imposing burdensome and costly mandates on American industry that, in turn, harm the civil liberties of American citizens.

Defining Data Retention

A starting point in any discussion of "data retention" must be to identify what is meant by the term. In the narrowest possible definition relevant to this hearing, we understand "data retention" to refer to the retention by Internet Service Providers (ISPs) of records of "IP address allocations" indicating which subscriber was assigned which "IP address" for a particular period of time. An IP address (standing for "Internet Protocol" address) is the unique numeric address (such as, for example, 143.228.146.10) used on the Internet to route communications to their proper destination. For any Internet traffic to reach the right place, it must contain the unique address of the destination computer or server.

For common residential broadband Internet access, each customer's household is assigned an IP address at the time the household turns on its service. This IP address can persist for days or weeks, but it can change (both on a regular schedule and whenever the hardware in the household is turned off or loses power). This use of "dynamic IP addresses" is an efficient and effective way for an ISP to manage its service to customers. A consequence of dynamic IP addresses, however, is that the person who is communicating with a given IP address on one day may not be the person who was using that same IP address last week or last month. To assist law enforcement, the leading ISPs in the United States have voluntarily kept records of these "IP address allocations" so that, for limited periods of time, the ISPs would be able to tell law enforcement who had a given IP address on a particular date and time.

Retention of IP address allocations by ISPs, especially if made mandatory, raises a host of serious policy and economic concerns, as discussed below (and as addressed in the testimony today from the ISP industry). But some data retention proposals have gone much farther. Some have advocated that ISPs monitor and record their users' online activities. Other proposals have suggested that *any* entity that gives temporary, dynamic IP addresses (such as coffee shops or WiFi "hotspots") be required to gather and retain data about their users. And in the Department of Commerce Online Safety and Technology Working Group ("OSTWG") process last year, law enforcement went even further to urge that any online site or service that allows users to communicate (such as blogs, social networks, and e-mail services) be required to track and retain "source data"

about every communication that any users make online.[2] These proposals raise enormous concerns.

It is critical to differentiate data *retention* from data *preservation*. A data retention mandate would affect all users, not just bad actors. By contrast, a far more targeted approach – preserving the data of suspects – can already be found in current law. Section 2703(f) of U.S. Code Title 18 permits law enforcement, without any judicial permission or notice at all, to require an ISP or other service provider to retain data – including IP address and customer identifying information – for as much as 180 days. As discussed more fully below, data preservation orders do not raise the kinds of problems raised by data retention.

For the reasons set out below, we urge this Subcommittee to reject calls for mandatory data retention, whether narrow or expansive.

Risks Posed by a Data Retention Mandate

Data retention mandates would pose significant risks to individual liberties and, at the same time, would damage innovation and competition within the technology industry. The Subcommittee should carefully consider the serious costs that would flow from any law mandating that service providers track their customers' Internet usage and retain that data.

Data Retention Laws Would Harm Personal Privacy

Data retention laws threaten personal privacy at a time when the public is justifiably concerned about privacy online. A key to protecting privacy is to minimize the amount of data collected and held by ISPs and online companies in the first place. A data retention law would undermine this important principle. Mandatory data retention laws would require companies to maintain large databases of subscribers' personal information, which would be vulnerable to hackers, accidental disclosure, and government or other third party access, thereby aggravating the identity theft problem and undermining public trust in the Internet. And the longer data is maintained, the more at risk it is to compromise or disclosure. The risk of harm would be even greater if entities that do not now keep data on their customers – such as coffee shops, airports, libraries, and others offering wireless access – were required to keep information on customers who use wireless services. And if companies are forced to collect data on their customers, it is very likely that they would decide to use that data for their own commercial purposes as well.

Proposals to mandate data retention cannot be viewed in a legal vacuum, but rather must be considered in light of the very limited privacy protections that are currently afforded to the data held by service providers. The Electronic Communications Privacy

[2] "Youth Safety on a Living Internet," Online Safety and Technology Working Group (OSTWG), June 4, 2009, at 105. OSTWG was established by Congress in the "Protecting Children in the 21st Century Act," (part of the "Broadband Data Improvement Act," Pub. L. No. 110-385), available at http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf (hereafter "OSTWG Report"). I served as a member of OSTWG and participated in the drafting of the privacy-focused portion of the data retention section of the final report.

Act (ECPA) was a forward-looking statute when enacted in 1986, specifying standards for law enforcement access to electronic communications and associated data, and affording important privacy protections to subscribers of emerging wireless and Internet technologies. But, as underscored by hearings held last year by the Constitution Subcommittee,[3] technology has advanced dramatically since 1986 and ECPA has been outpaced. The statute has not undergone a significant revision since it was enacted in 1986 – light years ago in Internet time.

Because of the out-dated and inadequate standards, data that might be required to be retained – including data that reveals highly sensitive information – could be obtained by law enforcement with almost no restrictions or limitations. This data is available with a mere subpoena and no notice need be made to the record subject. The legal process would involve no proof of specific facts, no judge, and no opportunity for the subject to object for any reason.

As a result, law enforcement requests for such inadequately protected data can target people who are likely entirely innocent. Were websites and other online services required to retain data on visitors, such information would be subject to a mere subpoena, which could, for example, be issued to require a online site to supply identifying information about every person viewing a particular Web site. Although one could argue that this would be acceptable if the web site contained child pornography, the problem is that a data retention mandate might apply to all online sites, including sites that provide sensitive or controversial – but completely lawful – content.

Not only would retained data be at risk of inappropriate and overbroad exposure to the government, but a database of retained data would also serve as a honeypot for lawyers in civil cases. As the OSTWG Report explained, looking back on early data retained by telephone companies, "private litigants soon recognized that [telephone] call record databases contained information that could facilitate investigations and litigation."[4] The exact same thing would happen with online data that might be required to be retained by ISPs, websites, and other online services, except that the online information can be dramatically more sensitive than the record of a phone call. Already, we understand that the great majority of requests that ISPs and others receive for customer information come not from the government but from private litigants in divorce cases, copyright enforcement actions, and commercial lawsuits. A data retention law would aggravate this problem, and would increase the likelihood that whistleblowers and journalists would also be among those whose records were subpoenaed.

Beyond the government and litigant access concerns, there is also a significant risk that service providers, once they were forced to build tracking databases on their customers, would decide to repurpose that data for other uses, such as behavioral advertising. There is bi-partisan interest in improving online users' "baseline" privacy rights relating to commercial uses of data, and it would be important for users to be protected in the context of any data that service providers are mandated to retain.

---

[3] *See* http://judiciary.house.gov/hearings/legislation11.html

[4] OSTWG Report, at 101

At a time when there is increasing concern about the privacy and security of personal information, and when there is increasing fear of governmental intrusion into our citizens' personal lives, Congress should be extremely cautious before it imposes a costly and invasive obligation that service providers monitor and track their users.

Data Retention Laws Would Harm Core Free Speech Rights

Data retention laws would threaten a core First Amendment right: the right to speak and access content anonymously. Anonymity fosters public discourse and political debate. Some of our founding fathers – including James Madison, John Jay and Alexander Hamilton – authored the Federalist Papers anonymously, publishing them under the pseudonym "Publius." The leading anti-Federalist also responded anonymously, under the name the "Federal Farmer" – and today we still are not sure of the identity of that political commentator.

The activists and political commentators of today are no more likely to deal in child pornography than those two hundred years ago. But a data retention mandate would sweep in everyone, whether or not they have committed a crime or are engaging in protected political speech that is vital to our society.

The constitutional right to anonymity is well established in our country. In *Talley v. California*, 362 U.S. 60 (1960), the Supreme Court wrote that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." More recently, in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), the Supreme Court reiterated that anonymous speech is part of "an honorable tradition of advocacy and dissent. . . . Anonymity is a shield from the tyranny of the majority." Data retention mandates would harm the ability of commentators and dissenters to express their views anonymously.

The speech harms that would flow from a data retention mandate are not limited to political speech. At least one study has shown that data retention in Europe (which, as discussed more fully below, has a data retention rule that is under attack and is being reconsidered) has significantly diminished citizens' willingness to discuss and obtain information about mental health issues online.[5] This is *precisely* the type of vital speech that would be harmed by a data retention mandate. Congress should not be chilling the discussion of politics, mental health issues, or a vast range of other sensitive topics, when less intrusive tools are already available.

Data Retention Laws Would Harm Innovation and Competition Online

Data retention laws would also harm American consumers – and American businesses, including small businesses – because retention mandates would diminish both competition and innovation in the online context.

---

[5] *See* A.M. Arnbak, "Plenary Presentation on 'Taking on the Data Retention Directive,'" Brussels, Dec. 3, 2010, available at http://www.edri.org/files/Data_Retention_Conference_031210final.pdf (find that as a result of data retention, "half of Germans will not contact marriage counsellors and psychotherapists" via e-mail), citing FORSA, "Opinions of citizens on data retention," June 2, 2008, available at http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf.

A threshold concern is simply one of cost. To our knowledge, ISPs have no business reason to retain IP address allocations. A mandate that all ISPs retain IP address allocations would impose significant costs on those providers. Extending a data retention mandate to the other end of Internet communications – the vast array of large and small online services that allow users to communicate with each other – would be an overwhelming and extraordinarily costly burden. Such a data retention mandate would, without question, drive some providers out of business.

Three scenarios can help illustrate the types, and magnitude, of the business harms that would flow from data retention mandates:

Scenario: Mandate on all online service providers such as e-mail, chat, blogging, and social networking websites to retain "source data" tracking the origins of all user communications: This type of mandate would impose a devastating burden on any website – large or small – that allows users to communicate (and, accordingly, it would certain discourage at least some U.S.-based sites from offering user interaction capability that would trigger the federal mandate). The magnitude of the proposed mandate is breathtaking. As one example, in mid-2009 users on Facebook posted one billion chat messages *per day*,[6] all of which would have to be tracked in a database; a mandate on Facebook alone would likely require that company to add more than *one trillion* entries to a mandated retention database every year.[7] The cost of creating and maintaining such a database would be hard for any company to handle, but a retained data mandate would be especially hard on small and innovative websites seeking to compete with the larger players. Most successful sites on the Internet began as small start-ups and a retention mandate on online companies would certainly chill (or drive offshore) the development of new sites and services.

Scenario: Mandate on any entity that provides Internet access using dynamic IP addresses to retain IP address allocations: Some proposals for data retention have called for mandates on *any* entity that provides access to the Internet to retain dynamic IP address allocations. Yet this type of data retention would burden many small retail businesses and other establishments (such a coffee shops and libraries) that seek to attract customers by offering free wireless Internet access. Such a mandate would also create additional privacy and identity theft risks arising from the mandated storage of personal information by large numbers of retail businesses.[8] And smaller businesses would be particularly hard hit, as they would likely be less able to comply with a federal mandate than would the large national chain shops.

---

[6] *See* "Chat reaches 1 billion messages sent per day," June 15, 2009, at http://www.facebook.com/note.php?note_id=91351688819&id=94455471199.

[7] Facebook's user base has more than doubled since the one billion chat message mark was hit in 2009, and thus it is likely that the chat message count has at least doubled. On top of that, Facebook reports that users post more than a billion other pieces of content to the site each day. *See* "Statistics," at http://www.facebook.com/press/info.php?statistics. Collectively, this equals in the neighborhood of 1.1 trillion separate user communications that Facebook would have to track in a data retention database each year.

[8] The privacy risks cannot be overstated. The small businesses that would be bound by the requirement that they retain significant amounts of personally identifiable data about their customers who access the Internet would become targets of ID thieves, particularly if the businesses lack the sophistication necessary to protect sensitive data. These risks would likely lead many users to decide not to use the Internet services in the first place.

Scenario: Mandate on small ISPs to retain IP address allocations: Today, in an effort to assist law enforcement, the leading broadband ISPs voluntarily retain IP address allocations for limited periods of time. But there still are smaller ISPs, competing with the major ISPs, and most of those ISPs do not have (and could not afford to maintain) tracking databases and the 24/7 law enforcement response offices that larger ISPs operate. Some of these ISPs are small businesses that might be driven from business by an additional federal mandate to retain data.

Any data retention law would be burdensome and costly, requiring investments in storage equipment and design costs, and forcing service providers to incur large annual operating costs. Currently, Internet access is relatively affordable and therefore available to many. The costs associated with mandated data retention would be passed on to consumers, inhibiting efforts to expand Internet access. For online services – many of which are currently free – data retention costs could draw sites' business models into question, or lead companies to seek ways to monetize the data they are forced to collect (by selling it, for example, to behavioral advertising firms).

And, by increasing costs on a broad range of service providers, data retention mandates would reduce competition in Internet access and online services. This reduced competition would likely lead to higher costs and less innovation. At the end of the day, data retention mandates would entrench larger providers, to the detriment of innovators and users.

By increasing costs on Internet access and online services, data retention mandates would harm American businesses, and they would likely drive services overseas to markets that do not have burdensome "source data" retention mandates. The United States has been the leading engine of innovation on the Internet, but costly federal mandates could make this country unfriendly to innovation and new services. Exciting new online services would still be developed – but not as frequently in the United States.

Moreover, a "source data" mandate would be devastating to the American industry's ability to compete in the burgeoning global "cloud computing" market. Few foreign corporations would trust American providers if they were required by the U.S. government to monitor and record data about every communication made over the cloud computing service. Indeed, it is possible that laws in foreign countries would prohibit their companies from using U.S.-based services subject to a data retention mandate.

Congress should reject calls for burdensome federal mandates on a range of service providers to track and retain data on their customers.

Data *Preservation* is an Appropriate Alternative to Data Retention

As noted above, there is an important alternative to data retention: data preservation orders. Current law already allows holding data about *criminal suspects* (rather than retaining data on *all* users of any given system).[9] It permits law enforcement (or any

[9] 18 U.S.C. § 2703(f), Requirement to preserve evidence, provides:

> **(1) In general.** – A provider of wire or electronic communication services or a remote computing service, upon request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order o other process.

other governmental entity), without any judicial permission or notice at all, to require both ISPs and online service providers to retain data – including IP address and customer identifying information – for 90 days (with an additional 90 days available on request). No supervisory approval is required, nor is any finding (even within the requesting agency) of specific facts that the records to be preserved are relevant to an investigation.

In the child pornography context, data preservation is *automatic* in cases where service providers report possible child pornography to the National Center for Missing and Exploited Children (NCMEC).[10] Whenever a provider sends a child pornography report to NCMEC, the provider must automatically preserve the data to give law enforcement enough time to open an investigation (and, if appropriate, obtain lawful process to demand the preserved data).

From a privacy and civil liberties perspective, the benefits of this approach are enormous: data about only the tiny fraction of individuals who have fallen under criminal suspicion is subject to a data preservation requirement. Everyone else would continue to enjoy the same level of privacy he or she would otherwise enjoy regardless of the law enforcement investigation. Under a data preservation regime, service providers can focus their attention and scarce resources on competition and innovation, rather than building tracking databases full of customer information.

Some countries have rejected data retention mandates in favor of the data preservation approach taken to date in the U.S. In November 2010, the Canadian Department of Justice called for new investigative tools – including data preservation authority – and it specifically rejected data retention because of its overbroad impact.[11] In Europe, many countries and courts are backing away from the European Union data retention mandates that were enacted (but not fully implemented) a few years ago. At least three national courts have questioned the validity of a data retention regime,[12] and another (the Irish High Court) has referred to the European Court of Justice a case that could call into question the validity of the entire European data retention scheme itself.[13]

For all of the reasons discussed in this testimony, data preservation is far preferable to a blanket mandate that extensive data on *all* users should be retained.

---

(2) **Period of retention.** – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day periods upon a renewed request by the governmental entity.

[10] *See* 18 U.S.C. § 2258A(h).

[11] *See* "Backgrounder: Investigative Powers for the 21st Century Act," Nov. 2010, at http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32567.html.

[12] For example, the German Constitutional Court found that aspects of the German retention law violated the fundamental right to privacy. *See* Vorratsdatenspeicherung Bundesverfassungsgericht, 2 March 2010, 1 BvR 256/08. The Romanian Constitutional Court went further and invalidated general mandatory data retention as a violation of the Romanian Constitution and EU law. *See* Decision no.1258, Romanian Constitutional Court, 8 October 2009. Unofficial translation by Bogdan Manolea and Anca Argesiu at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decisionconstitutional-court-romania-data-retention.pdf. *See also* http://www.edri.org/edrigram/number7.20/romania-data-retention-law-unconstitutional. *See also* EDRi, "Bulgarian Court Annuls a Vague Article of the Data Retention Law," EDRi-gram No. 6.24, December 17, 2008, http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention.

[13] Digital Rights Ireland v. Minister for Communications and others, No. 2006/3785P §106. *See also* EDRi, "Irish Court Allows Data Retention Law to be Challenged in ECJ," EDRi-gram No. 8.10, May 19 2010. http://www.edri.org/edrigram/number8.10/data-retention-ireland-ecj.

In the Face of the Serious Risks and Costs of Data Retention, Congress Should Carefully Investigate What Benefits There Would Be, If Any, in the Prosecution of Child Pornography Cases

Although no data is publicly available, and law enforcement officials have consistently refused to release information of this type when asked, a common perception in the child safety world is that law enforcement agencies already have far more child pornography cases on their plates than they can investigate and prosecute. In other words, even if a vast data retention regime were imposed on the American Internet industry, and even if data were retained for a lengthy period of time, law enforcement agencies would *still* not be able to investigate and prosecute more child pornography cases.

Moreover, it appears that many of the cases that are not being pursued because of a lack of resources are very recent reports (not older cases). In 2008, in testimony before the Senate Judiciary Committee, Special Agent Flint Waters of the Wyoming Internet Crimes Against Children Task Force testified about a broad range of *very current* cases that were not being pursued because of a lack of law enforcement resources.[14]

Congress recognized in 2008 the critical problem of a lack of resources to investigate child pornography cases, and it responded by authorizing for appropriation an additional $300 million (over five years) aimed at increasing prosecution of child pornographers. Unfortunately, to our knowledge, none of these funds have actually been appropriated.

In light of the continuing critical lack of resources to prosecute child pornography cases, and in light of all of the problems raised by data retention as detailed above, Congress should not impose huge costs on the Internet industry to implement a data retention regime.

As part of the OSTWG process, one of the OSTWG subcommittees addressing child pornography discussed the important need for Congress – before it takes additional action in this area – to learn the critical facts about the timing of and resources available to the investigation and prosecution of child pornography cases. As an Addendum to the OSTWG report, *see* OSTWG Report at 92-94,[15] I suggested a detailed series of questions that Congress should ask to inform any further policy decisions. We urge this Subcommittee to review those questions, and obtain answers to them.

Conclusion

Mandatory data retention is a risky and costly path to go down, and one that is all the more problematic because once Congress opens the door to mandating that service providers amass huge tracking databases documenting citizens' Internet usage, it will be hard to close it. If Congress were to impose data retention on even just a narrow category of service providers, and even for a narrow category of crimes, there would be

[14] Waters wanted to emphasize that he was not criticizing law enforcement: "I would like to be clear, I am NOT saying law enforcement isn't doing enough with what they have. I am saying they could do so much more if they only had the resources." *See* Testimony of Special Agent Flint Waters before the Senate Committee on the Judiciary Subcommittee on Crime and Drugs, April 16, 2008, at http://judiciary.senate.gov/pdf/08-04-16WatersTestimony.pdf

[15] *See* OSTWG Report, http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf, at 92-94.

a strong and inevitable push to broaden the scope and reach of data retention. Congress should not cross this risky line.

CDT appreciates the opportunity to testify today and we look forward to working with the Subcommittee on these issues.

For more information, contact John Morris, jmorris@cdt.org, Greg Nojeim, gnojeim@cdt.org, or Jim Dempsey, jdempsey@cdt.org, or at (202) 637-9800.

Mr. SENSENBRENNER. Thank you, Mr. Morris.

The Chair has written down the approximate order of appearances of the Members of the Subcommittee and will call on Members for 5 minutes in the order in which they appeared, alternatively by side.

And I will start by recognizing myself for 5 minutes.

And I want to direct my question to Ms. Dean. It seems to me that one of the problems that exists in this area is that there is not a uniform standard for how long the data has to be retained. It varies by Internet Service Provider. Would your association be

willing to propose such a voluntary compliance order, picking a time and cooperation with law enforcement for the retention of this data in order to eliminate Congress stepping in?

Ms. DEAN. Thank you, Mr. Sensenbrenner, thank you Chairman.

First of all, I guess I should say that we are here today because we are interested in the conversation, and we are interested in all opportunities to sit down with law enforcement and figure out if there is a solution to this problem that they describe today.

US ISPA is always willing to be part of the dialogue with law enforcement at all levels. And I think that the questions that have been raised already today in opening statements are really what we should have the discussion about. We really need to learn more from law enforcement about the breadth of this kind of a requirement. Who do they want to keep data and specifically what kind of data do they want kept and for how long?

Mr. SENSENBRENNER. Well, let me say that I am a firm believer in carrots and sticks, and I am tossing you a carrot now. I think that there is a desire on the part of both the Administration and Congress to legislate in this area. I am giving you or tossing an oar for you to put in the water to try to bring your industry together to deal with this problem on a voluntary basis.

And Mr. Morris has had a whole long list of questions that need to be answered. The fact is, is if you aren't a good rabbit and don't start eating the carrot, I am afraid that we are all going to be throwing the stick at you. So this is an opportunity for you to come up with some kind of a solution to all of the problems that both law enforcement and Mr. Morris have discussed. Are you on board, or should I take the oar back?

Ms. DEAN. I can tell you that I have heard you, and I am sure that my members have heard you as well, and they are dedicated to this issue, and we will absolutely sit down with law enforcement.

Mr. SENSENBRENNER. Okay, we are listening.

I yield back the balance of my time.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you.

Mr. Morris, you talked about the cost of this data retention kind of in general, can you give something with a dollar sign in front of it, percentage of sales? What are we talking about in terms of cost?

Mr. MORRIS. Truthfully, Mr. Scott, I can't give you dollar signs.

Mr. SCOTT. Well, some of these data retention services retain huge amounts of data with negligible costs. Are we talking about anything significant?

Mr. MORRIS. Yes. I think that simply the challenge of creating a database that would allow access to literally trillions of records is an enormous financial cost.

Mr. SCOTT. Can you give something with a dollar sign in front of it, some numbers?

Mr. MORRIS. I can't. One dollar sign I can give is that the vast majority of content and Web sites on the Internet are available for free, for $0 to their users. And those sites are very close to the line on a day-to-day basis as to whether they will make money or not make money. And the extra cost of any sort of Federal mandate would be very debilitating to those sites.

Mr. SCOTT. Ms. Dean, you have been offered carrots and sticks. Right now, is it true that your industry is providing approximately 150,000 leads to law enforcement every year?

Ms. DEAN. In terms of the reporting apparent incidences of child pornography to the national center according to statutory obligations, I believe the number is somewhere around there. For the record, we could find out from NCMEC what the precise number is.

But yes, service providers do report tens of thousands of reports a year, and they are——

Mr. SCOTT. Now the way you reported, you have some kind of mechanism where somebody is sending a picture, and you can ascertain whether it fits a profile of what is known child pornography and that goes right to law enforcement; is that right?

Ms. DEAN. Well, the standard that service providers are required to transmit the images for referral to NCMEC is apparent. We don't know what is and is not child pornography. So when we, by either technical means or from user complaints, come upon such material, we box it up with all of the information that we have and transmit it to NCMEC.

Mr. SCOTT. Mr. Weinstein, when you get this information, what do you do with it? I mean, you have got about 400,000 the last couple of years; you have hundreds of thousands of leads. Do you have the staff to follow through on those leads today?

Mr. WEINSTEIN. Ranking Member Scott, let me actually address both of those in order.

When law enforcement gets referrals from NCMEC, from the national center, those referrals are distributed to law enforcement at the Federal level, depending on the part of the country that the referral comes from.

Under the PROTECT Act of 2008, there is a mandatory 90-day retention period by ISPs that kicks in when those ISPs actually discover or become aware of possible child pornography, and they make a referral to the cyber tip line, as Ms. Dean indicated.

The problem with that requirement, although it is a useful tool, is that it is limited in its effectiveness. Number one, it doesn't apply to other types of crimes beyond child exploitation, but even just within the realm of child exploitation, that obligation to retain and to report only kicks in when the ISP has actually discovered or become aware of the child pornography. And the statute doesn't impose any obligation on the ISP to do any monitoring of the network or to make any affirmative efforts to filed the child porn.

Mr. SCOTT. Wait a minute. Can you keep up with the tips that you have coming in today? And you know that with across-the-board budget cuts, you are looking at a loss of potentially thousands of FBI agents. Can you keep up with the tips that you are getting today?

Mr. WEINSTEIN. Well, it is fair to say that the scope of the problem far outpaces the resources we have available to fight it.

Mr. SCOTT. Now you mumbled something about all crimes, if we pass something of data retention, is it true that this might be used for all crimes, not just child pornography?

Mr. WEINSTEIN. Well, it is my view that if Congress were to go down this road and actually create a data retention requirement,

that it makes the most sense for it to apply to all crimes not just to child exploitation.

Mr. SCOTT. And all of this information, now is the information we are talking about just site specific or content to include the content, because Mr. Douglass pointed out that, without the content, that information would not have been particularly helpful.

Mr. WEINSTEIN. Well, it is actually the opposite that is true, sir. It would not be content information that we would be taking about. It would be——

Mr. SCOTT. Are we talking about retained—the policy, we are kind of vague here because we don't have a bill in front of us, but are you suggesting that we have content being preserved or retained as well as just the site information?

Mr. WEINSTEIN. No, I am talking about noncontent information about Internet communications, so IP addresses that are assigned to a user at the time of communication.

Mr. SCOTT. So if we had that, then what Mr. Douglass used about reading the text messages wouldn't have been available.

Mr. WEINSTEIN. Well, as I understand it, text messages are generally not retained by providers.

Mr. SCOTT. Well, that is what we are talking about retaining.

Mr. WEINSTEIN. Well, the case Mr. Douglass talked about was one in which text messages were crucial in solving the crime.

Mr. SCOTT. The content of the message was important.

Mr. WEINSTEIN. Sure. The cases I am talking about, Mr. Scott, are cases in which an Internet user——

Mr. SCOTT. Is it your proposal that content not be retained?

Mr. WEINSTEIN. Well, the Administration doesn't have a proposal today, but I think that one of the issues that Congress should engage in a discussion on is whether it should include content. My own view is that the most useful information to us in solving crimes is noncontent.

Mr. SCOTT. Okay. Now, if this information is available, would it be—sitting up there, would it be available for private subpoena, like in a divorce case?

Mr. WEINSTEIN. Well, that is another issue that I think is worth discussing, whether it is only available to law enforcement or available to private litigants as well. My primary interest, obviously, is making sure it is available to law enforcement.

Mr. SCOTT. Would we need to, if we passed something like this, turn around and have some regulations to protect privacy?

Mr. WEINSTEIN. Again, I think that sort of—the questions—there are five or six questions that I think Congress should ask as we engage in this discussion. Number one—and some of these have already been alluded to. Number one is, what data needs to be retained, the issue we have been discussing? Number two is how long the data should be retained for. Number three is, who would need to retain it? Number four is, who would have access to it, the issue you just raised, whether it would be law enforcement only or private litigants as well? And number five is whether some additional protections for consumers are necessary, whether those need to be legislated or something industry can do on its own to enhance privacy and security of their networks.

Mr. SCOTT. And Mrs. Dean is going to be very helpful in making sure that we follow through and particularly helpful in continuing to send you more information and more tips that you can follow through on.

Mr. SENSENBRENNER. Time of the gentleman has expired. The Chair recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank you, Mr. Chairman.

Ms. Dean, did you say that every year your business supplies law enforcement 190,000 tips?

Ms. DEAN. No. There is a statutory obligation under 18 U.S.C. 2258(a), that required ECS and RCS providers—we will call them service providers today. So it is much broader——

Mr. POE. How many? Cut to the chase. How many do you provide?

Ms. DEAN. I think last year it was over 140,000.

Mr. POE. One hundred and forty thousand. Those go to whom, local, Federal?

Ms. DEAN. They go to the National Center for Missing & Exploited Children, according to statute, and NCMEC are the experts, and they deal with it from there. They refer it out to the proper jurisdiction.

Mr. POE. Mr. Weinstein, how many Federal cases were made on child pornography in 2010 or 2009? Give me a figure that I can understand.

Mr. WEINSTEIN. I would be happy to, Congressman, I just don't have it available. I find as I enter my 40's, my own personal data retention is not what it should be. But I would be happy to provide a number to you.

Mr. POE. I mean, can you give me a ball park figure? It wasn't 145,000, was it?

Mr. WEINSTEIN. No, I don't believe it was 145,000.

Mr. POE. How many cases? Do you have any idea?

Mr. WEINSTEIN. I don't and I would also want to be able to get you that information at the local level, too. As you know, a great many of these cases are prosecuted by State and local law enforcement and are pursued by the ICAC task force, which the Department helps fund and which exists in every State in the United States.

Mr. SCOTT. Would the gentleman yield?

Mr. POE. I will yield.

Mr. SCOTT. Thank you. There is a report from the Department of Justice, the list is 8,352 in the last 4 years.

Mr. POE. Reclaiming my time. So it is about 2,000 a year.

Chief Douglass, how many cases, since you are the chief, do you know how many cases local law enforcement has made in any given period of time?

Chief DOUGLASS. Mr. Poe, I can't give you a specific number. I can tell you, however, that we have—in Overland Park, it is a city of 170,000 people, and we have a three-man or three-person unit person working on it full time. And as far as I know, none of those cases came through the channels we are talking about. So they are working on their own leads in significant numbers.

Outside of the arena, we are talking in a Federal sphere. The exact number I can't give you. But I can tell you we are working several peer-to-peer cases, two to three to four, every single month just in Overland Park.

Mr. POE. Can you supply the Committee with that data?

Chief DOUGLASS. Yes, sir, I will.

Mr. POE. And Mr. Weinstein, can you as well supply that?

Mr. WEINSTEIN. I will, yes, sir.

Mr. POE. Appreciate that.

I am concerned about the overbroad idea of Federal legislation in any area.

Certainly I think people that engage in this type of criminal activity ought to get their day in court before a jury as often as possible.

But do you see any Federal concerns, constitutional concerns, Mr. Weinstein, since you are encouraging us to come up with some kind of legislation about the overbroad concept of more storage of personal information?

Mr. WEINSTEIN. Congressman, the way I approach the issue is this, to the extent that the collection of data creates privacy risks or creates risks to people's anonymity, those risks exist today right now. Much of the noncontent data that we are talking about here today, that law enforcement needs to solve these crimes is already being retained right now by a large number of communication providers for their own commercial and marketing purposes, and that includes ISPs. That includes the New York Times. That includes a lot of Web sites that you visit every day.

A mandatory data retention requirement would only extend that retention time to make sure that it was applied universally across industry.

To the extent that there are risks to privacy from those databases existing, those risks exist on day 1 when you open your account; they exist on day 30, day 60, day 90 day 180, day 365. Whether a provider keeps the data for a day or a year, the provider has an obligation to protect that data. There is no system that is foolproof, but responsible providers take steps to safeguard the networks, and we can always do more.

In terms of the impact on privacy of law enforcement having access to that data, as I said in my opening remarks, what we are not talking about, expressly not talking about, is in any way increasing the authority of law enforcement to get that data. The authorities Congress has already provided and that we exercise consistent with statute and constitutional obligations every day are the same authorities that will govern our access to these expanded databases or these databases that are kept for longer periods of time. We cannot—law enforcement cannot obtain that data unless lawful process is used, and that would continue to be the case.

The ultimate safeguard against law enforcement abuse is that we are subject to be supervision of Congress, of the courts, of the Department of Justice, and prosecutors' ethical obligations to make sure that they use the lawful authorities properly and in accordance with the Constitution.

Mr. POE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman.

This has been a very useful hearing and what I want to propose to you, Chairman Sensenbrenner, why don't we—the question is always, where do we go from here? Why don't we get the Smith proposal and my proposal and meet with Eric Holder and the deputy assistant attorney general and come up with a bill and let's just move it along.

We can study this, you know. We are pretty good at studying things, but——

Mr. SENSENBRENNER. Would the gentleman yield?

Mr. CONYERS. Of course.

Mr. SENSENBRENNER. I would be happy to participate in that meeting, but it seems to me you are yanking the carrot away from Ms. Dean.

Mr. CONYERS. Well, the Humane Society may be looking for you pretty soon anyway with this carrot and stick approach. It has raised some very interesting questions, Mr. Chairman.

But I think we all see where we are going here. It is not like this hasn't been worked on before. So I offer that proposal for your examination and, hopefully, action.

Now John Morris, were you shocked as I was when the deputy assistant attorney general began to theorize about how far we could carry this business? I mean, I thought he would be a little bit more restrained in trying to get us on board, but he has left the door open for this to go all the way.

Mr. MORRIS. Well, certainly there have over the years been a number of proposals for data retention that have always been targeted at child exploitation cases, which are certainly, I agree, among the worst of the worst cases out there. But I think that is one concern we have always had about those proposals, is that that simply would open the door to broad data retention applying to even, you know, to the broad range of cases. So, yes, it is a very serious concern that I have that we are talking about.

Mr. CONYERS. So he didn't surprise you?

Mr. MORRIS. I am afraid it didn't surprise me that that is the direction that law enforcement is going, yes.

Mr. CONYERS. Do you have any defense at all to offer, Weinstein?

Mr. WEINSTEIN. Well, I must say, I don't think I have ever been referred to as "unrestrained" before. So I apologize if I gave that impression, Mr. Chairman Emeritus.

To be clear, the government doesn't have a specific proposal. My purpose here today is to emphasize to you law enforcement's concern about the lack of the data and to flag the issues——

Mr. CONYERS. So when are you going to get a proposal? How many years is this going to take?

Mr. WEINSTEIN. I don't know where we are exactly in the process of developing a proposal, but we are here today and we are committed to engaging in this conversation with you and with the entities represented by the other people on the panel.

Mr. CONYERS. Well, I am going to call Eric Holder right after this hearing and see if we can get this moving. I mean there are a lot of things to study in the Crime Subcommittee, but I don't think we

need a whole lot of time on this. And besides, why don't you take advantage of the bipartisanship that is raging all over the 112th Congress?

Mr. WEINSTEIN. I certainly think that in a lot of areas, we should take advantage of that bipartisanship.

If I could, just to be clear, there are a number of permutations of this that could be done in terms of the type of providers that are covered, the type of information that is covered, the length of time, whether it is 30 days, 60 days, 6 months, a year or more. As you know, the European Union has a data retention directive that its member states have been ordered to implement where data is retained for a minimum of 6 months and maximum of 2 years. Within that range there are a number of possibilities, and also in terms of the scope of the crimes covered, there are a number of possibilities. We don't endorse any particular one of them, although, as I said, we are eager to participate in this process going forward and to come up with a proposal that we think balances all those costs.

I should also be clear, we completely understand that there are costs imposed. While data storage costs are dropping dramatically, there will be costs imposed if data has to be retained longer than it currently is being retained. There is no doubt about that. And one of the greatest costs will be data retrieval in response to requests from law enforcement, although if we follow the practice that we do currently those costs will to a large extent be reimbursed.

At the same time, I didn't mean in my remarks earlier to suggest that we don't think privacy is an issue. My only point is only that the privacy risk exists currently. The point here is to try to find a balance among all three interests, and I am confident we can do that.

Mr. SENSENBRENNER. The gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman, and thank you for holding this hearing. This is an issue that is of keen interest to me. I have long worked with Chairman Smith and Chairman Sensenbrenner and others on the issue of child pornography and other related issues on the Internet. Sometimes we have had successes. Sometimes the Court has set us back, but it is a concern and an ongoing effort.

I have also spent a lot of time meeting with leaders over the years from the European Union and urged them not to impose a hard 2-year data retention requirement. The European Union sort of found not quite a 2-year requirement. It requires that the ISPs retain data for a period of between 6 months and 2 years, and the EU has faced a great deal of difficulty in implementing this requirement.

So it seems to me that if there is a lot of interest in this issue—and I share some of the concerns expressed by Ms. Dean and Mr. Morris and the problems that will ensue—it seems to me that the first place we ought to look is what the experience of the European Union is. And Ms. Dean, would you care to comment on that? And I will ask Mr. Weinstein, too.

Ms. DEAN. Well, I think that the experience in the European Union and the fact that they have had to come back to the table

recently and they are reassessing their original approach begs that maybe we should look to a different approach for the United States. Certainly in different member states, the implementing legislation in the EU has been ruled unconstitutional, and I think that asks us to really come back to the table and look at innovative approaches, things like preservation.

Mr. GOODLATTE. Thank you. Mr. Weinstein?

Mr. WEINSTEIN. Yes, Congressman. My understanding—although I must say I can't speak with expertise about the state of affairs in the EU—but my understanding is that the European Court of Justice in 2009 ruled that the directive I referred to earlier was legal. There have been some issues with the implementing legislation, as Ms. Dean just indicated. And my understanding is that the process that is underway now is a process to harmonize and fix some problems with the implementation of the directive but that it is only a minority of the member states who have failed to comply; that is, that a majority of the states have complied. And so to the extent that they have, I think, as you suggested, there are some lessons to be gleaned from studying the way that the directive has been implemented in those places where it has been.

Mr. GOODLATTE. Mr. Morris?

Mr. MORRIS. One lesson I think we can look at in Europe is what has the impact been? And studies have begun to show that data retention mandates in Germany, just to take one study, have reduced the willingness of citizens to go online for mental health services. And that, I think, is something—that is precisely the kind of very sensitive information that I think that Congress should be very concerned about, chilling the access that citizens have and the comfort that citizens have in going online.

So I think there are at lot of lessons one can take from Europe, and certainly in Europe, there is a move to revisit data retention. And certainly I have heard many of the European politicians say that, you know, at the maximum one would say, you know, 6 months. Clearly that is the direction that they are going, to reduce the length of time. But there are serious concerns that are raised in Europe.

Mr. GOODLATTE. Thank you. Ms. Dean, what would a blanket data retention requirement have on smaller ISPs?

Ms. DEAN. This is a serious concern because we don't quite understand at this point what the breadth is. I mean, you could take some of the earlier comments made and assume that this is meant to apply to Web sites. And just because it is noncontent data does not mean that that data is not revealing and very interesting about people's behavior online. And it is not clear exactly what it is that companies will be called upon to retain. Are we looking at, you know, what Web sites they go to? And this all brings us back to the scope and the breadth and the duration of time. For small companies, I guess it is really up to the Subcommittee to consider whether these kinds of mandates could really be stomached by smaller companies. I can say that within my membership, I have large companies, but I also have small companies who provide services to rural areas and to lower-income Americans. And their services, because they are low-cost or free, would be greatly affected by a data retention mandate.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentlewoman from California, Ms. Chu.

Ms. CHU. Chief Douglass, internetworldstats.com, which is a Web site for international Internet usage statistics, said that as of 2007, there were 66 million Internet broadband subscribers in the U.S., which is about 22 percent of our population. Is it law enforcement's belief that we should retain all these subscribers' data? Or is it possible to do something that is more targeted? How would you determine which subscribers' data should be retained? And are you actually saying that all of those 66 million's information should be retained?

Chief DOUGLASS. Well, ma'am, essentially there is no way to specifically target it because if we knew who the bad guy was, we could just target them. But unfortunately we don't. And what we have to do is to assume that this information is like a bank that has a vault full of safety deposit boxes. Those safety deposit boxes remain totally sealed, totally inaccessible to the law enforcement until something happens and we are given direction to open one particular box. That is how this particular system would work.

I would point out that there is a lot of information there. But in my own history in the last 2 weeks I applied for a loan. And when I applied for a loan, they pulled up my credit report and my credit report knew everything about me. That is on the Internet and that is maintained for 7 years. So my point being is, we all have to sacrifice to a certain extent for those particular component parts that require addressing. In this particular case with the credit report, my credit is good, but we had to sacrifice that access because some people's credit isn't so good. In this case, all of us would have to contribute to a certain balance of that sacrifice and privacy so that the criminal element can be addressed. And there is no way to target it or narrow it or move it down because we are dealing with the unknown.

Ms. CHU. Mr. Morris, how do you respond to that? And also, how would the retention of the data of the 66 million people harm Americans' privacy rights and aggravate the problem of identity theft?

Mr. MORRIS. Thank you, Congresswoman. Let me first respond, to take the credit reporting example, credit reporting, you know, Congress has passed very, very strong legislation to protect the privacy of that information. It is very strongly controlled. In contrast, data held by service providers has extremely little protection. The Electronic Communications Privacy Act was enacted in 1986. It is woefully out of date. Law enforcement can obtain the data that we are talking about, the noncontent data that we are talking about, with very, very minimal process or protection. And so, I mean, there are some very, very serious privacy concerns.

I believe the Internet usage in the United States has now risen to about 70 percent. I think we are now talking about 230 million Americans who would be covered by this. And the proposals that all of their access everywhere they go, all of their e-mails be monitored and tracked is really breathtaking. In the context of call records, telephone call records that were kept by telephone companies, we have seen very broad use of civil subpoenas by divorce at-

torneys and other civil uses. And my understanding—I am not sure if Ms. Dean may be able to tell me—but my understanding is that actually civil use, noncriminal use of data that is held by service providers represents one of the largest types of demands and requests that companies receive for this data.

So it is clear if the data is required to be held, it will be used in a broad context.

Ms. CHU. You are saying that there are far less protections that are provided by the Electronic Communications Privacy Act than for, say, credit reports.

Mr. MORRIS. Right.

Ms. CHU. Should that be updated first?

Mr. MORRIS. Absolutely. The need to update ECPA is really critical. I mean, it is critical for privacy grounds. It is also critical for business grounds because it really is harming the American industry's ability to compete in the global marketplace, given the low standards of protection that ECPA affords.

Ms. CHU. Is there a way to have a more effective use of existing data preservation requirements rather than having mandatory data retention?

Mr. MORRIS. Well, Congress in 2008 authorized the appropriation of additional resources for both prosecution and also for the technical investigation of child obscenity crimes, which would allow law enforcement to get access to the information they need sooner, which would reduce the need or the argued need for a data retention mandate. If law enforcement is able to more promptly investigate these cases instead of being overwhelmed with other cases, then there is really not such an issue that data retention would be needed to address.

Ms. CHU. Thank you.

Mr. SENSENBRENNER. At this point, the Chair asks unanimous consent that a statement by Ernie Allen of the National Center for Missing & Exploited Children be inserted in the record.

[The prepared statement of Mr. Allen follows:]

STATEMENT

ERNIE ALLEN

PRESIDENT AND CEO

THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

for the

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

"Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes"

January 25, 2011

Mr. Chairman and distinguished members of the Subcommittee, the National Center for Missing & Exploited Children ("NCMEC") appreciates the invitation to submit this statement on the subject of data retention and crimes against children on the Internet. NCMEC is grateful for the Subcommittee's commitment to the safety of our children.

As you know, the National Center for Missing & Exploited Children is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice. NCMEC is a public-private partnership, funded in part by Congress and in part by the private sector. For 26 years NCMEC has operated under Congressional authority to serve as the national resource center and clearinghouse on missing and exploited children. This statutory authorization (see 42 U.S.C. §5773) includes 19 specific operational functions, among which are:

- operating a national 24-hour toll-free hotline, 1-800-THE-LOST® (1-800-843-5678), to intake reports of missing children and receive leads about ongoing cases;
- operating the CyberTipline, the "9-1-1 for the Internet," that the public and electronic service providers may use to report Internet-related child sexual exploitation;
- providing technical assistance and training to individuals and law enforcement agencies in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children;
- tracking the incidence of attempted child abductions;
- providing forensic technical assistance to law enforcement;
- facilitating the deployment of the National Emergency Child Locator Center during periods of national disasters;
- working with law enforcement and the private sector to reduce the distribution of child pornography over the Internet;
- operating a child victim identification program to assist law enforcement in identifying victims of child pornography;
- developing and disseminating programs and information about Internet safety and the prevention of child abduction and sexual exploitation; and
- providing technical assistance and training to law enforcement in identifying and locating non-compliant sex offenders.

Our longest-running program to help prevent the sexual exploitation of children is the CyberTipline, the national clearinghouse for leads and tips regarding crimes against children on the Internet. It is operated in partnership with the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security's Bureau of Immigration and Customs Enforcement ("ICE"), the U.S. Postal Inspection Service, the U.S. Secret Service, the Military Criminal Investigative Organizations, the Internet Crimes Against Children Task Forces ("ICAC"), the U.S. Department of Justice's Child Exploitation and Obscenity Section, as well as other state and local law enforcement. We receive reports in eight categories of crimes against children:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- sex tourism involving children;
- extrafamilial child sexual molestation;
- unsolicited obscene material sent to a child;
- misleading domain names; and
- misleading words or digital images on the Internet.

These reports are made by both the public and by Electronic Service Providers ("ESPs"), who are required by law to report apparent child pornography to law enforcement via the CyberTipline (18 U.S.C. §2258A). The leads are reviewed by NCMEC analysts, who examine and evaluate the content, add related information that would be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and provide all information to the appropriate law enforcement agency for investigation. These reports are triaged continuously to ensure that children in imminent danger get first priority.

The FBI, ICE and Postal Inspection Service have direct and immediate access to all CyberTipline reports, and assign agents and analysts to work at NCMEC. In the 13 years since the CyberTipline began, NCMEC has received and processed more than 1 million reports. To date, ESPs have reported to the CyberTipline more than 8 million images/videos of sexually exploited children. To date, more than 44 million child pornography images and videos have

been reviewed by the analysts in our Child Victim Identification Program ("CVIP"), which assists prosecutors to secure convictions for crimes involving identified child victims and helps law enforcement to locate and rescue child victims who have not yet been identified. Last week alone, CVIP analysts reviewed more than 240,000 images/videos.

These images are crime scene photos. According to law enforcement data, 19% of identified offenders in a survey had images of children younger than 3 years old; 39% had images of children younger than 6 years old; and 83% had images of children younger than 12 years old. Reports to the CyberTipline include images of sexual assaults of toddlers and even infants.

NCMEC's role has given us a unique depth of knowledge about how the Internet is used to victimize children and the challenges this presents to both law enforcement and ESPs.

The Internet consists of various communications platforms, including the World Wide Web, peer-to-peer file sharing, newsgroups, and Internet Relay Chat, to name just a few. The reports received by the CyberTipline include apparent criminal activity on all of these platforms. Each platform offers distinct advantages to someone seeking to sexually exploit a child. An offender might use peer-to-peer technology to distribute child pornography and the World Wide Web to directly communicate with a child victim, perhaps persuading the child to perform sexual acts via a webcam.

What all of these platforms have in common is access to the Internet. Advancements in technology have changed the way people use the Internet today. What started with desktops, servers, and dial-up modems is now smartphones, cloud computing, and wireless hotspots.

Members of the public and ESPs can report online crimes against children that occur on any of these Internet platforms to the CyberTipline, making it a major source of leads for many law enforcement agencies. This reporting mechanism helps streamline the process from detection of child sexual exploitation to prosecution and conviction. This process increases the efficiency of law enforcement's efforts and maximizes the limited resources available in the fight against child sexual exploitation.

In 2008 Congress passed the Securing our Adolescents From online Exploitation (SAFE) Act, which requires ESPs to preserve their CyberTipline reports for 90 days in anticipation of legal process by law enforcement. This is an important step forward. However, the CyberTipline is not the only source of leads for law enforcement investigating these crimes. All cases involving online crimes against children, regardless of the source, should benefit from having information critical to the investigation.

The value of the CyberTipline as a source of leads for law enforcement is greatly enhanced by the collaboration of ESPs. Since its creation, ESPs have worked with NCMEC staff on ways to improve their reporting procedures. And because investigation and prosecution is only part of the solution, ESPs are partnering with NCMEC in other ways, too.

The Technology Coalition --- AOL, Earthlink, Google, Microsoft, Time Warner, United Online and Yahoo --- was formed by these industry leaders to explore how new technology could be used to combat the proliferation of online child pornography. One of its early successes is a software program called PhotoDNA, Microsoft's tool that can be used to identify specific child pornography images more efficiently and accurately than ever before.

To date, 88 ESPs are participating in NCMEC's URL Initiative. CyberTipline analysts identify active web pages with apparent child pornography and compile a daily list of Uniform Resource Locators ("URLs"). ESPs participating in this voluntary program can access the list and take steps to limit the availability of these sexually abusive images, reducing the continued re-victimization of the child victims.

Despite these efforts, the Internet continues to present challenges to investigations of crimes against children. The greatest challenge to law enforcement is that all of these technologies allow offenders to use the Internet with perceived anonymity.

There are those who argue that the right to remain anonymous on the Internet is protected by the First Amendment. It is important to note that the Supreme Court has never held that such a right

exists for criminal acts. In fact, when faced with the issue of child pornography in 1982, the Court unequivocally held that child pornography is not constitutionally-protected speech.

There is a significant missing link in the chain from detection of child pornography to conviction of the offender. Once the NCMEC analysts review a CyberTipline report, add necessary information and refer it to law enforcement, there can be no prosecution until law enforcement connects the date and time of that online activity to an actual person – the type of information found in a connectivity log. There is currently no requirement for ESPs to retain connectivity logs for their customers on an ongoing basis. While some have policies on retention, these policies vary, are not implemented consistently, and some are for too short a time to have meaningful prosecutorial value. As a result, offenders are willing to risk detection by law enforcement, believing that they can operate online anonymously.

To clarify, connectivity logs are similar to the records that telephone companies are required to keep by federal law -- the date and time that a phone number was dialed. Connectivity logs provide the link between an Internet Protocol address and an actual person. These records are vital to law enforcement who are investigating and prosecuting these cases.

One example: in a 2006 Congressional hearing an Internet Crimes Against Children Task Force Officer testified about a movie depicting the rape of a toddler that was traded online. In hopes that they could find the child by finding the producer of the movie, law enforcement moved quickly to identify the ESP and subpoenaed the name and address of the customer who had used that particular IP address at the specific date and time. The ESP did not retain the connectivity information and, as a result, law enforcement was forced to suspend the investigation. Tragically, the child has never been located by law enforcement – but we suspect she is still living with her abuser.

We think this is just not acceptable.

We recognize that online child exploitation presents challenges for both the Internet industry and law enforcement. However, we are confident that there is a way to balance the needs and

priorities of both. Too many offenders have gone undetected by law enforcement and are willing to gamble that they can operate online anonymously. Federal, state, and local law enforcement have become more resourceful, but the lack of connectivity logs present a significant barrier to their investigations. Please help ensure that law enforcement has the tools they need to identify and prosecute those offenders who are misusing the Internet to victimize children. Too many child pornographers feel that they have found a sanctuary. Let's not prove them right.

7

Mr. SENSENBRENNER. And now the Chair recognizes the distinguished Vice-Chair of the Committee, the gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

Mr. Weinstein, you had said in your statement that in some ways the problems of investigations being stymied by a lack of data

retention is growing worse. Could you elaborate on what you mean by that?

Mr. WEINSTEIN. Yes, sir, Congressman. Certain types of providers, principally in the cell phone community, are not retaining data at all. Increasingly, we are having providers who are retaining data for shorter and shorter periods of time, if they retain it really at all. We also have encountered the problem repeatedly of providers who publish or state that their retention period is 6 months or some period of time, only to find that when we submit requests to those providers within the stated retention period, we are told that the data is no longer being retained. So in that sense, the problem is growing worse.

As I said before, a great many providers are already retaining the data that we are talking about here. So the points that were made over privacy before, I think it is important to recognize that that data will continue to be retained by the providers and not by the government; that is, the government can only obtain it through lawful process. The data will be retained by providers, as it is currently. The problem is the inconsistency. The problem is that it is not held for a sufficient period of time, that it is not consistent across the board, that the decisions about how long to retain data for are made unilaterally by the providers and are subject to change at will and, as I said, are often not even honored.

So what we think is essential is that whatever the decision is about the scope of the requirement, if Congress goes down this road, is that it be one that is clear and consistent across industry.

In 2008, the Electronic Frontier Foundation published a user guide or a guide that was entitled, Best Practices for Online Service Providers, which I think is unintentionally the best argument for Congress to intervene in this space than anything that I could say today. It advises providers that they can't be forced to provide law enforcement with data that doesn't exist. It provides guidance about how to minimize what they referred to as "the challenges of law enforcement compliance." It calls upon providers to obscure, delete as much data as possible. It advises providers to use secure deletion utilities to scrub the hard drives so that the logs cannot be obtained. The fact that providers are being guided to conduct themselves in this way I think speaks to the fact that the problem is growing worse and that congressional action—or congressional engagement on the issue is probably as timely as it has ever been.

Mr. GOHMERT. Well, you touched on this perhaps. But the Electronic Communications Privacy Act currently allows investigators to request preservation of records. And I would ask you, Mr. Douglass, if that is not being honored. And if it is, why is that not adequate?

Chief DOUGLASS. Well, congressman, I have no evidence, but it is not being honored. The problem is, it is not a question of honoring our request. The problem is that it is not there when we ask for it. So if the information has already been deleted or if it has already been spoiled in some respect, we can ask all day. But if it is not there, it is not there to get. And that is why the time requirement of 30 days is onerous because many cases are not brought to light in 30 days.

Mr. GOHMERT. Mr. Weinstein, have you made requests for preservation that have not been honored?

Mr. WEINSTEIN. Except in the sense that—the largest problem with preservation is what the Chief said. That is that the preservation tool, while a useful tool, is only valuable if the data still exists at the time that the preservation letter is submitted. For reasons that I alluded to in my oral remarks, these are extraordinarily complex crimes. In the child exploitation arena, increasingly they are international and global investigations. They are investigations that often start when law enforcement in another country seizes a server or seizes a computer that is being used by the administrator of a child sexual abuse distribution network. And it takes time to go from that seizure in Australia or New Zealand or Germany to identifying IP addresses of people in the United States who are engaging in that activity, and then having to follow the trail of those people here to the U.S. And invariably, really quite often, too often, by the time we are able to—and no matter how quickly we work, by the time we are able to find the provider——

Mr. GOHMERT. My time is running out. Let me ask quickly. We have talked in generalities. Is there a large ISP that consistently deletes information to prevent you from having that information preserved? I am asking specifically.

Mr. WEINSTEIN. Sure. I appreciate why you are asking specifically. But I would rather not talk about specific providers. But what I would say is that for the most part the ISP community is very cooperative.

Mr. GOHMERT. Well, pardon me for my background being a judge, but as a judge, if people weren't willing to get specific, then obviously it was not legitimate testimony that would come into evidence. Is there no specific——

Mr. SENSENBRENNER. The time of the gentleman has expired. You don't have to answer that one.

The gentlewoman from Florida, Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman. Mr. Chairman, some of the Members and the witnesses may know that I was the House sponsor of the PROTECT Our Children Act of 2008 which was a major effort and continues to be a major effort to develop a national strategy which has been developed, appoint the National Coordinator for Child Exploitation Prevention and Interdiction, which is Francey Hakes, who is actually here with us today and is in the audience and who has been doing an excellent job in this area, to finally coordinate the work of the Internet Crimes Against Children Task Forces and provide them with the resources that they need because previously they have really been only able to investigate less than 2 percent of the cases that occur when it comes to the transmission of child pornography online and other kinds of sexual predatory activities on the Internet.

But all the money in the world and the coordination and the planning isn't going to help at all if we don't have the assistance from the Internet service providers. And with all due respect, Ms. Dean, I think we need to be clear that this is not about watching or tracking people's behavior online, which is how you described it a couple of minutes ago. It is about helping law enforcement connect the dots. And one of the things that I think is extremely im-

portant to underscore here is that that is the difficulty, is that right now, because there are varying degrees of cooperation, varying degrees of time that ISPs actually preserve this data—some as short as 7 days, without naming names, Mr. Chairman, as you suggested—that it really becomes extremely difficult, if not impossible, for law enforcement to be able to actually get to the information they need not about the individuals and their activity but about specifically the connectivity logs. I mean, that is what really we need to be able to get at are these connectivity logs. Because as people know who follow this stuff, an individual ISP address is not helpful because people have a different one for every computer that they log on to. So having the ability to track one individual's connectivity is what is necessary. Law enforcement already have the pictures. They already have the ability to lift the digital fingerprints. They lose that ability if ISPs don't hold onto that information for a standardized period of time.

So my question to you, Ms. Dean, really is this: Voluntarily would be a lot better than mandating this. I think that is what we would all like to see, including law enforcement. So what are the ISPs willing to do voluntarily? You should come together and decide on a standard and propose it. Because that is going to be the best way that we can get this problem addressed without us being in a situation where we have to figure out legislatively how to make you do it.

Ms. DEAN. Thank you, ma'am. And I have been given some carrots and sticks today earlier from the Chairman, and I recognize the need to go back and work with my membership and to talk about this.

We have been following data retention for many years. We have been engaged in this conversation. And certainly in the area of fighting online child exploitation, it is something that U.S. ISPA and our members are certainly committed to, so I can guarantee that we will be getting back to you and talking to your staff about this.

Ms. WASSERMAN SCHULTZ. Thank you. Mr. Chairman, at some point, if we could hear from Francey Hakes, who is the person that is coordinating all of this activity from the Department of Justice, it would be incredibly helpful. Mr. Weinstein, I know that you are doing your best, but Francey really is the person that is responsible in the law for coordinating all of this activity, and I know that she would be able to give us some very helpful information, one of which is—I am really not understanding why you don't have a specific proposal because, Mr. Weinstein, that is supposed to be in the National Strategy. So is it in the National Strategy? If it is not, then the National Strategy is deficient.

Mr. WEINSTEIN. Well, I don't believe that there is a specific data retention proposal, Congresswoman, in the National Strategy, although the National Strategy is designed to do a lot more than just address the issue of data retention, as you know. It is meant to lay out a framework for coordinating all of law enforcement's operations to address the problem.

Ms. WASSERMAN SCHULTZ. Before I run out of time, that is just a big concern that I think we need to address. You really do need to do a better job of giving us a number or a percentage of cases

that have been hindered or reached a dead-end. The anecdotal information is somewhat helpful, but if you don't really give us a concrete number.

But the question that I have for you specifically is: In the Republican budget proposal, which proposes to cut 20 percent across the board, what would that do to your ability to continue to investigate and solve these cases, if their budget proposal actually went through?

Mr. WEINSTEIN. Well, if I can address both pieces of that quickly. In terms of the concrete number, it is a challenge and it is frustrating to me, to Francey, and to all of us who are involved in working on this issue that we can't come up with a concrete number. And there are a number of reasons for that. But the primary one is that the Justice Department, like all levels of law enforcement, doesn't typically keep statistics on cases that do not result in charges. And very often what happens when an investigation hits a dead-end so that the investigator or the prosecutor moves on to another case, we don't log the fact that we tried but were not successful. The other thing is that law enforcement officers are smart, and they figure out over time which ISPs will keep data for which periods of time. And when they obtain a lead and they need to go to a provider, if it is outside what they understand to be the data retention period, they won't even bother to submit a request because they know it is not going to be fruitful, and they will try—sometimes successful, often not—to obtain the evidence they need from another source.

So the anecdotal example that we could talk about, some of which I alluded to in my testimony, are not hypotheticals. They are illustrations. There are new anecdotal examples we get every day, every week, every month of cases that were not able to be made.

Ms. WASSERMAN SCHULTZ. And can you address my budget proposal question?

Mr. WEINSTEIN. If I may, Mr. Chairman.

Mr. SENSENBRENNER. Go ahead.

Mr. WEINSTEIN. The only thing I would add, this goes beyond child exploitation because every type of crime that we worry about is committed through online means now. And so I think that losing prosecutors and losing agents would seriously impact our ability to prosecute really virtually any type of online crime or crime committed through an online means at the level that we would like to.

Mr. SENSENBRENNER. The gentlewoman's time has expired. The gentleman from Arizona, Mr. Quayle.

Mr. QUAYLE. Thank you, Mr. Chairman. And thanks to all of you for coming in today.

My first question is going to be for Ms. Dean. What specific actions have your members voluntarily taken to combat child pornography so far?

Ms. DEAN. Well, I can speak as an association and as someone on behalf of the individual members. We have promulgated a number of sound practices to be more helpful to law enforcement in the areas of child pornography reporting and in general subpoena compliance when it deals with child exploitation cases. The members participate in a number of important task forces, things like the Technology Coalition and Financial Coalition Against Child Por-

nography, which we can get you more information about in the future. And certainly the companies interact with the ICACs on a regular basis. And moreover, they have highly skilled staff that work on these compliance issues, understand that child exploitation cases are a priority, and are trained to deal with them in a timely manner.

Mr. QUAYLE. And also in your testimony, you spoke about some of the problems that we are facing with data retention in terms of it might slow down the process for immediate emergency situations, such as child abductions and the like. Obviously we don't want to negatively impact with legislation having these unintended consequences of maybe we have this increased data storage issues, but then it actually has some problems with the speed of recovery. Can you address that and maybe talk about it a little more?

Ms. DEAN. Yes. And thank you. I appreciate that opportunity. Because as we thought about data retention this most recent round, one of the things that occurred to the companies was that, you know, we have a number of concerns about the cost to innovation and so forth. But the main concern that we would have with building these massive data bytes—we are talking exabytes of information—how it would be that we would be 100 percent accurate in retrieving precisely the record that law enforcement requested and doing so in a timely and efficient manner and doing so in an emergency situation because we do get frequently emergency requests from law enforcement and want to be helpful. The reason this is so important to the companies is because, one, they take their responsibilities under ECPA and other statutes very seriously. But secondly, because we are dealing with people's lives and liberty here. And out of all this data, we have to make sure that, say, 18 months down the road that tiny particular piece of information is exactly the right information linking that exact target, and there is a concern in that area, yes.

Mr. QUAYLE. Mr. Weinstein, can you give your side on that issue in terms of how that might affect emergency responses in slowing down the recovery time?

Mr. WEINSTEIN. Congressman, what I can say is that in those situations, as I have indicated a number of times, there is already a substantial number of providers who are keeping the kind of data that we were talking about and do keep it for a period of time. So it is not like they are creating systems out of whole cloth. They just need to figure out a way to keep it for longer, and there would be some potential additional cost of storing it for longer. But those same providers who have that data have to respond to the kind of requests you are talking about every day. And they manage to do so quite well. So if they are keeping a larger volume of data, it seems to me it would be a software engineering problem that is beyond my expertise. But to the extent that they are able to comply with those requests today when they have got the data available, I would expect them to be able to do so in the future.

I do acknowledge, as I said before, that I think the principal additional cost of a data retention regime would be in data retrieval, not so much in data storage but in the data retrieval. But I wouldn't anticipate that there would be a significant impact on—negative impact, that is, on ISP's ability to respond to emergency

requests. I think what it would mean though is that the non-emergency requests, there may be some additional delay in responding to them. But given where we are now, we are happy if they are being responded to at all.

Mr. QUAYLE. All right. And further, do you have any suggestions in terms of retention period? Is it 1 year, 2 years, 3 years, 4 years, keeping it forever? I mean, that is one thing that I was wondering is that, you know, with the statute of limitations—I don't know what they are for child pornography cases, but wouldn't you want to have that match up to when the statute of limitations expires?

Mr. WEINSTEIN. Well, I think that the statute of limitations for child sex abuse cases, I think there actually is none. So that would be keeping it indefinitely. For most Federal crimes, it is 5 years. I think that if the only consideration at play here was law enforcement, then I would think the statute of limitations would be the place to start the discussion. But that clearly is not the case. And I don't want to suggest for a second that that is what we would suggest.

There are clearly other competing interests. The economic impact on the providers, to some extent privacy. And I think that when you balance those out, it clearly has to be something that is much more modest than the statute of limitations period. Where that number is, I can't say today. Although, as I have said, I think this is a very useful first step. I know this is an issue the Subcommittee has worked on for years and years. And I am hopeful that, working together, we can come to a place, come to a number that maximizes law enforcement's chances of solving the crimes it needs to solve without overwhelming the providers and without creating unintended consequences.

Mr. SENSENBRENNER. The time of the gentleman has expired. The gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman, for holding this very important hearing today on using Data Retention As a Tool for Investigating Internet Child Pornography and Other Internet Crimes. And this bill, H.R. 1076, is actually cited as the Internet Stopping Adults Facilitating the Exploitation of Today's Youth Safety Act of 2009. But it is a fact, isn't it, that the provisions of H.R. 1076 go far beyond stopping Internet child pornography; is that a fair assessment, Mr. Morris? Is that true?

Mr. MORRIS. Well, certainly H.R. 1076 would very broadly sweep—the terms of that legislation would very broadly sweep——

Mr. JOHNSON. Yes. I mean, section 5—yes, section 5, Retention of Records By Electronic Communication Service Providers is not limited to only investigations or matters concerning child pornography.

Mr. MORRIS. Certainly I read that draft bill the same as you do. Yes, sir.

Mr. JOHNSON. Okay. So it is kind of like perhaps you could say—and I don't say this disparagingly—but kind of like a Trojan horse. And you could have things in that Trojan horse that come out and surprise you.

Mr. MORRIS. Yes. Certainly I agree that once the data is mandated to be retained, it will be used for a broad diversity of rea-

sons, including civil litigation, perhaps even commercial use by the service provider, and a range of other things that concern us.

Mr. JOHNSON. Well, let's talk about that in just a second. But let me look down at section 9 of the proposal. It grants $150 million to the Innocent Images National Initiative, $150 million. Now does anybody have any idea what the Innocent Images National Initiative is?

Mr. WEINSTEIN. Yes, Congressman. The Innocent Images Initiative is a law enforcement initiative that was set up by the FBI and the Justice Department. The Innocent Images Task Forces are the groups that have primary responsibility on the Federal level for investigating child exploitation crimes.

Mr. JOHNSON. Where would this money go to? Who would be the recipients of the $150 million?

Mr. WEINSTEIN. I can't speak to the specifics of the proposal, Congressman, because I am not as familiar with it. So I don't know what the intended use of that $150 million is. My guess would be that it would be primarily to support investigative resources, investigators and prosecutors.

Mr. JOHNSON. But you would not say that there are any limits on how the money could be spent as provided by section 10, is that correct?

Mr. WEINSTEIN. Well, again, I can't speak to the details of that specific proposal.

Mr. JOHNSON. So in other words, can anybody on this panel tell me where the $150 million and to whom would the $150 million provided under section 9 go to? Yes, Mr. Douglass, do you want to give it a stab?

Chief DOUGLASS. I will try to do so.

Mr. JOHNSON. I have limited time now. Just answer me this: Do you know where the $150 million is going to?

Chief DOUGLASS. I know where a small part of it is going to.

Mr. JOHNSON. Well, a small part. I want the big part. And I find it somewhat disturbing that we are not able to get at that in this hearing.

So we have got Internet child pornography being the Trojan horse. And then inside that, we have a data retention situation, mandatory, that may fall upon the backs of commercial and private Internet service providers. And then we have $150 million to boot going to some——

Mr. SENSENBRENNER. The gentleman's time has expired.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. Last, but not least, the gentlewoman from Florida, Ms. Adams, is recognized for 5 minutes.

Ms. ADAMS. Thank you, Mr. Chairman.

Mr. Weinstein, I was listening. And coming from a law enforcement background, I am kind of curious. You made a comment about when your agents get to a point where they just stop because they have hit a dead-end and they move on, and you couldn't give us a caseload count. Is it your testimony today that your caseloads are not counted based on open/closed caseloads?

Mr. WEINSTEIN. Well, Congresswoman, certainly at the Federal level—I can't speak to the State and local—but at the Federal level we do, both the agencies and the Justice Department, keep track

of cases that are open and closed. What I mean to suggest is that we couldn't look at that data and figure out how many of those were closed because of a failure of data retention. There are any number of reasons why a case is opened and then ultimately not able to be successfully concluded or result in a charge. It could be that there is a lack of evidence, it could be that there were other investigative hurdles. But I couldn't pinpoint within that gross number of cases how many were a data retention issue specifically.

Ms. ADAMS. And so then I am not to be concerned at the fact that you would base your budget on caseload. You are basing it on your open caseloads, correct?

Mr. WEINSTEIN. You know, those cases take an extraordinary amount of time, as you know, especially now. And in the child exploitation arena, this is particularly true, but it is true in a lot of others as well, that to the extent that those cases involve international law enforcement, to the extent that the criminal is sophisticated and takes steps to try to anonymize himself or herself, there are a number of steps in the chain you have to go through that take a long time. You can investigate a case for years only to find that you are not able to bring a charge. So I think the fact that the case is open and how long it is open for reflects the amount of man and woman hours that are going into it. It is just that sometimes, for any number of reasons—data retention being one of them—you can't actually successfully complete the investigation and indict anyone.

Ms. ADAMS. And while sometimes it is a lot of man hours when the case is open or it sits there because you have hit a dead-end and you haven't closed it quite yet, and I recognize that. But that goes again to what Mr. Quayle asked you, and that was, how long then, how long would you recommend that these providers hold this data?

Mr. WEINSTEIN. Well, as I said to Mr. Quayle, I think the Administration doesn't have a position at this time on what the appropriate amount of time is. What I do believe is the case is that—at least as a starting point for discussion, I think the EU range of 6 months to 2 years is a useful starting point for discussion, but I wouldn't suggest, even as I sit here today, that it should be 6 months or 2 years or 1 year. I do believe that there is a time period that we could come to that would be long enough that law enforcement could maximize the chances of getting the evidence it needs to successfully complete a larger number of investigations and bring a larger number of criminals to justice but that wouldn't be so long or that would be moderated and would not overwhelm, in terms of cost or privacy impact, the other equities involved.

I mean, ultimately, I think the fact that we haven't come to a conclusion on this issue successfully over the last 2 or 3 years reflects the fact that it is really a complex exercise to try to figure out what that time period is; you know, what is the magic number that gives law enforcement what it needs but doesn't overwhelm the providers and that moderates the risk to privacy of having data held for a long period of time? I can't come up with that number today, but I am pretty confident that if we work at it, we will come to it.

Ms. ADAMS. And your earlier testimony is something that I have had along my law enforcement career is that a lot of times when you start investigating these you end up going to different countries, and that adds time to the process, does it not?

Mr. WEINSTEIN. It does. In fact, I was thinking this morning about a case that we did that we call Operation Achilles, which was a multinational law enforcement operation to take down a network that was producing and distributing images and videos of child exploitation, and there was a little, little girl in the Northern District of Georgia who was rescued as a result of that investigation, but she was rescued 2 years after the video of her being abused was discovered when a search was done in Australia of one of the members of the organization's computers. And it took 2 years of work every single day by the investigators, both in Australia and here in the U.S., to try to find out where that girl was so they could rescue her and ultimately capture the abuser, who was her father. Those cases can inherently take a long period of time. We are obviously committed to them, and we will investigate them as long as we humanly can.

Ms. ADAMS. I hope so.

Ms. Dean, hearing this testimony, I would agree with my colleagues that you go back to your membership and see if there is some kind of compromise you can come up with within your membership and to the law enforcement that doesn't require the Congress to intervene on this. It is really important that if there are children being abused, taken advantage of, or worse, we would like to have that information given to law enforcement so that the bad guys can be prosecuted.

Mr. SENSENBRENNER. The time of the gentlewoman has expired. The gentleman from Florida, Mr. Deutch.

Mr. DEUTCH. Thank you, Mr. Chairman. I have a question, Mr. Weinstein, for you about the way that we investigate. There is a constituent of mine in my district of south Florida that runs a business. It is a data fusion program, child protection systems, which is a program that is used by the vast majority of ICAC task forces as well as 38 countries free of charge. I would like to know, since this is a system that enables law enforcement to track files across the vast expanse of the Internet and then identify the specific computers that are responsible, first—actually for you and for Mr. Douglass—are you aware of this opportunity, this program?

Chief DOUGLASS. I am aware of several programs that allow us to pinpoint peer-to-peer intersections and gives us a starting point to start with the subpoenas and search warrants. I do know this, that they are relatively successful but somewhat limited at this stage in scope.

Mr. DEUTCH. Mr. Weinstein.

Mr. WEINSTEIN. Congressman, I am not familiar with that particular software, but I am familiar with a number of programs, as the Chief said he is as well. And you should know, the Department, under section 105 of the PROTECT Our Children Act, was directed to develop a technological solution known as the National Internet Crime Data System, and we are in the process of doing that. We have issued grants I think to the Massachusetts State Police in relation to the development of that. And once that system is oper-

ational, it will support efforts by Federal, State, local, and tribal enforcement, including the ICAC task forces, to more effectively investigate and deconflict those cases. So we are working very hard on developing technology that will enhance our ability to pursue those cases.

Mr. DEUTCH. I would just suggest that the technology of this company has been used—their expertise has been used to catch criminals. They also helped identify the 9/11 terrorists. I would encourage you to reach out, and I would be happy to make that happen.

Getting back to something you said earlier this morning, Mr. Weinstein, moving beyond this issue of data retention. I would like to ask you about other ways to streamline the prosecution of these cases and make it more likely that we will actually catch these people. The Internet, as was just discussed, is global, and the criminal activity bounces over local, State, and even national boundaries, borders. Does it make sense from a national law enforcement perspective to create a centralized place—at least for the United States—to subpoena ISP records rather than having to subpoena each company in a different way?

Mr. WEINSTEIN. Well, I haven't given a lot of thought to a proposal like that, although my first reaction is that to the extent people are concerned about privacy from having multiple databases of Internet activity, I would think that there would be some significant privacy concerns if there was one megadatabase of that activity. But I think that ultimately, Congressman, the challenge in these cases is not just the ability to get data, of course. They are inherently time consuming, and they take a long time. I think as our relationships improve with foreign law enforcement, we are able to proceed then more quickly and more efficiently. But ultimately, if providers were able to retain the data we needed for a reasonable and uniform period of time, we would have fewer deadends and we would be able to move the cases more quickly. Sometimes the cases take longer than they otherwise would because, having hit a roadblock when the data is not available, you have to figure out some other way around it, some other way around the lack of data, and to try to basically investigate the case over again from a different angle. If the data were available, whether it was in one common source, as you suggested, or maintained by individual providers for a reliable period of time, I think we would be able to pursue the cases more expeditiously and in larger numbers to a successful conclusion.

Mr. DEUTCH. Mr. Douglass, from your perspective, would a centralized database help in pursuing these criminals?

Chief DOUGLASS. Well, again, I agree with Mr. Weinstein. A centralized database would certainly be the most efficient. However, the tenor of these conversations have been all about balance, and balance means that we balance out the effects of privacy and the effects of efficiency at the same time. So consequently, while it would absolutely be more efficient, I would also think it would raise a lot more concerns about concerns over privacy. I think we can work around that. If we have the locations we can go to that maintain those files, that is not a big deal.

Mr. DEUTCH. Finally, Mr. Chair, Mr. Douglass, I appreciate what you are saying. And certainly we need to balance those interests, ultimately though being on the front lines of Mr. Weinstein in trying to catch these guys. I am just trying to figure out if that is something that we ought to be entertaining, and it sounds like it is something that could be helpful.

Chief DOUGLASS. I would have concerns about going that direction because I don't think that the benefits would outweigh the risks.

Mr. SENSENBRENNER. The gentleman's time has expired. The gentleman from Arkansas, Mr. Griffin.

Mr. GRIFFIN. Thank you, Mr. Chairman.

Ms. Dean, I wanted to ask you, I was looking through your testimony, and it may just be a misunderstanding. But it appears that you make a distinction between data retention and data preservation. And I apologize for being out if you have explained that. But could you comment on that?

Ms. DEAN. Certainly. I would be happy to.

Data presentation and data retention are—my luck today—are very different. Data preservation is a targeted request from law enforcement to a provider to hold on to a specific person's data. And to be clear, to clear up some of the conversation from earlier, that is not simply an IP log. That is a very broad aspect of—it is a snapshot. Think of it as a snapshot at the exact moment that the request comes in of that person's account, e-mails, buddy lists, anything that we have got that is taken, set aside, and it is able to be preserved for up to 180 days. Now that doesn't go into the future because then you can get wiretap problems and things like that.

Retention, what we are talking about here today, would be to hold on to a category of data, a category of providers on all of their users into the future.

Mr. GRIFFIN. So preservation would include the type of information that you would get in a subpoena such as method of payment, credit card records, all of that stuff, and the retention is just the data that relates to the ISP?

Ms. DEAN. Well, to be clear, preservation is so effective and valuable, we see it as very effective and valuable because we don't make a distinction as to what kind of process may come in the future. We simply freeze the account, set it aside, and it is available to law enforcement, pending the issuance of process. So they can get whatever it is the order calls for into the future.

Mr. GRIFFIN. What is your ideal? Are you happy with the status quo? I know that when I came back in, Mr. Weinstein had been asked by Representative Quayle about his ideal in terms of the time frame. I want to ask you what your ideal is.

Ms. DEAN. Well, one of the things I want to say is that, you know, we really do want to be involved in this conversation. We want to talk to our colleagues in law enforcement and find out what it is specifically that they need. We really do want to understand better which providers. And that is very important. Do you want the Facebooks of the world? Do you want you know access providers? Do you want the nytimes.com? It is very important.

Mr. GRIFFIN. I am running out of time. So there is not a specific time frame. It sounds like you are still sort of grappling with it. Chief Douglass, do you have an ideal time frame in mind that you think would capture most of the data that you would need?

Chief DOUGLASS. Yes, sir. My personal opinion is 6 months up to a year, maybe up to 18 months. But after that period of time, there is a point of diminishing returns. Certainly 6 months does not seem to be unreasonable from an investigative standpoint. We will get quite a bit. That will be six times more than the best we can get right now. And in that event, I think that would be logical. But there are other factors to consider. And when we shape out whatever agreements or legislation or compromises that take place, those things should be fleshed out with all parties, understanding exactly where it goes. But from a law enforcement standpoint, I would think a minimum of 6 months would be advantageous. More like a year would probably be the best.

Mr. GRIFFIN. Have you been in any talks with the Department of Justice on this? Apparently, the Department of Justice has not settled on a specific time frame.

Chief DOUGLASS. No, sir. We haven't. And, you know, we come from two different localities with two different things in mind. The Department of Justice is looking at overall arching philosophy and policy for the entire country in that regard, and we are looking at it from how it affects Overland Park, Kansas and how it affects cities in your State. So we have common interests, but they are not necessarily parallel interests.

Mr. GRIFFIN. Maybe you can grab Mr. Weinstein there, and y'all can talk about that. Thank you. That is all I have, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman's time has expired. And again, last but not least, the gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Mr. Chairman.

And if I do ask a question that has already been asked because I was at another meeting, please tell me that and I will go on.

Deputy Weinstein and Chief Douglass, I couldn't agree with you more on your approach, what you have done, and what you continue to do, particularly in the area of child abuse and cybercrime. As a prosecutor, as a district attorney for 12 years, the State level, and as an United States attorney for 6 years, I have personally prosecuted both types of cases in both courts. And on many instances, the evidence that we have gathered could be as much as 2 years old. So I implore you to please keep doing what you are doing, bring back to us any insight that this Committee can do to see that you can carry on that mission. And I thank you for that.

Director Dean, again, please, I beg you to talk with your organizations, the individuals with whom you work. I am sure that you can come to a consensus. But please, please utilize the frontline law enforcement men and women when asking what can we do to improve the tools that you need to track down these child abusers. Many of the cases that I worked on personally involved photographs and pornography that came into the United States from other countries. But unfortunately, we have a fair number of those individuals in this country. So I implore you, please regulate this to the extent where it is effective and efficient yourselves because,

I can agree with the Chairman and my colleagues, at one point, we will step in.

And Attorney Morris, let me refer to something in your statement. And could you please correct me if I am wrong on this. Maybe it is just written or taken out of context. I am reading toward the end—actually, the next to the last page of your statement. It says in bold at the top, In the face of the serious risk and cost of data retention, Congress should carefully investigate what benefits there would be, if any, in the prosecution of child pornography cases.

You are not suggesting that we do not investigate and prosecute child pornography cases, are you?

Mr. MORRIS. Not in the least, Congressman. What I am suggesting is that given the current lack of resources, given the fact that, as I believe Congresswoman Wasserman Schultz said, that only 2 percent of the cases that are currently known do we have resources to prosecute that adding a massive data retention obligation is not going to increase the ability for us to put the child pornographers in jail. I certainly very, very strongly support the goal of putting these people in jail.

Mr. MARINO. Thank you. Now I do disagree with the percentage that was stated as to the cases that a re prosecuted. As a prosecutor, we could prosecute more crimes in any situation if the district attorney or the Chief or the deputy attorney general had more bodies and more investigators. But with that said, in my experience—and perhaps Deputy Weinstein and the Chief can respond to this—any case that came into our offices or series of cases would be investigated and eventually prosecuted.

Gentlemen, what do you say about this?

Ms. WASSERMAN SCHULTZ. Would the gentleman yield just for 1 second?

Mr. MARINO. Yes.

Ms. WASSERMAN SCHULTZ. I just want to thank you very much. I just wanted to clarify in saying that they are investigating less than 2 percent of the cases. It is not because they are unwilling to. It was because of the lack of resources, the lack of individuals, the lack of resources to be able to investigate more than that. But specifically in among the cases that they are able to investigate, they rescue a child in about 30 percent of the cases. So it is incredibly important. I just wanted to make sure I was clear.

Mr. MARINO. Thank you. I understood that it is just a percentage, the 2 percent. I don't mean to brag about it, but our conviction rates in our office and our investigations and prosecutions were far more than 2 percent of the cases that came into the office.

Mr. WEINSTEIN. Congressman, I think, as you know, as a general matter, we follow the same approach that I know you followed in your office when you were the U.S. attorney. We don't turn cases away at the door. If they are there to pursue, we will pursue them.

I think that it is not just increasing the number of cases. It is taking the existing cases as far as they can go. I used the case of the father who was abusing his daughter in northern Georgia a few moments ago. Because it took 2 years to identify that man as the abuser, by the time his computer was searched, the data that would have helped identify the other members of the group here

in the U.S. with whom he was trading videos of child sexual abuse, we couldn't pursue those people because the data didn't exist. So a lot of times, it is taking the case that we have made and making it bigger and making sure that we are actually dismantling the entire organization so we can protect more children at the same time.

Mr. MARINO. Thank you. I think my time has expired.

Mr. SENSENBRENNER. The time of the gentleman has expired.

I want to thank our witnesses for their testimony today. And, Ms. Dean, I hope you got the message, and I hope you will get to work with your organization to help us come up with a way that deals with this problem fairly. It is going to mean that your members are going to have to do a little bit more, and I think we all recognize that. But this is going to be a lot easier if this is worked out. There is a need to deal with this issue. I always prefer to have it done voluntarily in a trade organization. But I think you have got the message that if it isn't being dealt with voluntarily, the train will leave the station.

So again, thank you all for your testimony today. Without objection, all Members will have 5 legislative days in which to submit to the Chair additional written questions for the witnesses which we will forward and ask them to respond as promptly as they can so that their answers may be made a part of the record. Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

And without objection, this hearing is adjourned.

[Whereupon, at 12 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE HENRY C. "HANK" JOHNSON, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA, AND MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Congressman Henry C. "Hank" Johnson, Jr.
Statement for the Hearing on
"Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes."
January 25, 2011

Mr. Chairman, I thank you for holding this very important hearing on using data retention as a tool for investigating internet child pornography and other internet crimes.

The internet has drastically improved and revolutionized our lives.

It allows us to share information quickly and communicate with friends and family across the globe.

Unfortunately, internet child pornography has been on the rise.

Last Congress, Chairman Smith introduced H.R. 1076, the Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009. This bill has been referred to as the SAFETY Act.

It would have required Internet Service Providers to retain all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user for two years.

Child pornography is one of the most devastating and egregious crimes in this country. Chairman Smith's goal of wanting to catch child predators and bring justice to the victims is an admirable goal.

I, too, share Chairman Smith's goal of fighting child pornography, but I have serious concerns about the SAFETY Act, including cost, privacy, and First Amendment issues.

Like Chairman Smith, I want to keep our kids safe online, but think there are more effective ways of getting to this goal.

Instead of giving private companies millions of dollars to retain data, a better way may be to spend that money on hiring more investigators so that these types of investigations are prioritized which would avoid unnecessary delays in the issuance of subpoenas.

Money could be spent on public awareness campaigns and additional crime preventions efforts.

It does not appear that a mandatory data retention law is necessary.

We already have the Electronic Communications Privacy Act which gives the government the ability to compel providers to retain for 90 days, without having to make any showing of relevance and without any judicial action.

Law enforcement can renew these orders for an additional 90 days, if necessary.

Further, the Republicans, in the "Pledge to America," stated that creating jobs and competitiveness is their top priority.

A mandatory data retention law could have some unintended consequences that could be detrimental to our country. What affect will this type of legislation have on small businesses?

The costs of complying with a broad data retention policy will be burdensome for all companies, particularly smaller companies that could be put out of business by having to comply with such a requirement.

Any additional costs on Internet Service Providers adversely affects the public as the costs would probably be passed down to consumers.

This would curtail job creation and exacerbate and already high unemployment rate. Shutting down small businesses will not make our economy grow, but would stifle competition and limit consumer choice.

Further, there are serious privacy and First Amendment concerns that come along with any mandatory data retention legislation. Beyond invasion of privacy issues, there would be increased threats of security breaches and identity theft. The unintended consequences of law enforcement's access to and use of data will have a chilling effect on First Amendment speech rights.

If the American public knows that law enforcement has access to their online activities, even if perfectly legal, it will affect people's usage and conduct on the Internet.

Additionally, this will infringe on our Fourth Amendment right to a reasonable expectation of privacy – especially if ISPs start storing content for longer periods of time.

As a Member of Congress, I expect my email communications with staff to be private. I am sure that family members and friends that communicate over the internet have a reasonable expectation of privacy over their content.

It is crucial that we explore all of these issues before implementing any mandatory data retention law.

I look forward to hearing from our witnesses about how we can make the internet a safer place for our children to visit within the confines of the law and yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE TED DEUTCH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA, AND MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Congressman Ted Deutch (FL-19)

Statement for Subcommittee on Crime, Terrorism, and Homeland Security
Hearing on
"Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes"
January 25, 2011 at 10:00 a.m.
2141 Rayburn.

Mr. Chairman,

I want to thank you for holding this important hearing today. As a father, I am disgusted that criminals are able to evade the reaches of law enforcement by hiding in the shadows of the Internet. I know that much work has already been done to shine a light into these vile places and stop the perverts who are victimizing our children.

From what I have read on the issue, there seems to be a lack of uniformity in terms of what information is retained by individual companies and for how long. I think it would be helpful to have uniform standards of data retention – based on the reasonable needs of law enforcement working in this field. I would hope that the industry could work to create a "best practices" standard, since I am sure that everyone involved is committed to doing whatever it takes to bring down these criminals. In the absence of that standard though, it is the responsibility of Congress to look at whether the federal government is needed to bring uniformity to what I understand is a hodgepodge of a current system – and get these criminals.

Internet service providers and online services providers do have a responsibility to do their part to assist with legitimate investigations properly conducted. The Internet is an amazing tool that has completely changed our society, but what is a crime in the real world is still a crime on the Internet. It is certainly easier to hide in anonymous chat rooms and file-sharing sites, but those who prey on children must be found wherever they lurk. While we cannot lose sight of the need to safeguard all users' personal information, we cannot let this concern prevent us from action. Given the explosion of child pornography rings since the birth of the Internet and with file-sharing sites in particular, I think it is safe to say that we have not found the right balance yet, and I look forward to hearing from the witnesses today.

○