AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING CHILDREN FROM INTERNET PORNOGRAPHERS ACT OF 2011

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

ON

H.R. 1981

JULY 12, 2011

Serial No. 112–60

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

67–309 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
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
[Vacant]

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 R. 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 R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida

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

CONTENTS

JULY 12, 2011

Page

THE BILL

H.R. 1981: The "Protecting Children from Internet Pornographers Act of 2011" 3

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 14
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 15
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 17

WITNESSES

Ernie Allen, President and CEO, National Center for Missing and Exploited Children
Oral Testimony 24
Prepared Statement 27
Michael J. Brown, Sheriff, Bedford County Sheriff's Office
Oral Testimony 34
Prepared Statement 37
Marc Rotenburg, President, Electronic Privacy Information Center
Oral Testimony 42
Prepared Statement 44

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 19
Material submitted by the Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 75
Material submitted by the Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 79

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Subcommittee on Crime, Terrorism, and Homeland Security 81
Letter from Douglas C. Gillespie, President, Major County Sheriffs' Association here 84

Page

Letter from Chuck Canterbury, National President, National Fraternal Order of Police 85
Letter from Mai Fernandez, Executive Director, The National Center for Victims of Crime 86
Letter from Paulette Sullivan Moore, Vice President of Public Policy, the National Network to End Domestic Violence (NNEDV) 87
Letter from Penny Nance, Chief Executive Officer and President, Concerned Women for American Legislative Action Committee 88

PROTECTING CHILDREN FROM INTERNET PORNOGRAPHERS ACT OF 2011

TUESDAY, JULY 12, 2011

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

The Subcommittee met, pursuant to call, at 9:59 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Smith, Goodlatte, Lungren, Poe, Marino, Gowdy, Conyers, Scott, Cohen, Chu, and Quigley.

Staff Present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Sam Ramer, Counsel; Sarah Allen, Counsel; Allison Halatei, Deputy Chief of Staff; Sean McLaughlin, Chief of Staff and General Counsel; Tony Angeli, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Lilliana Coronado, Counsel; Joe Graupensberger, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will be in order.

Without objection, the Chair will be authorized to recess the Committee during votes today.

Hearing none, so ordered.

I am not using the prepared statement that was given to me today by the staff. I move myself 5 minutes.

This is the second hearing that this Subcommittee has had on this subject. The bill that is before us today, I think it is very bad policy. And I will say right now that I will do my best to kill it, should it proceed any further.

I do not believe that there should be a statutory declaration on how long Internet service providers should maintain records. That should be a business decision that they should make.

Furthermore, I am very disturbed at the administrative subpoena power that is given to the Marshals Service by this bill.

People may recall that I introduced a similar bill when I was the Chair of the Committee and withdrew it, because I was concerned for both of these points, and that concern remains.

People should also be aware that I fought vigorously to avoid granting more administrative subpoena power to any Federal law enforcement agency during both the PATRIOT Act consideration and the PATRIOT Act reauthorization in 2005 and 2006.

This bill strikes out in both respects. It is my feeling that the administrative subpoena power that is given to the Marshals Service will allow not only the Marshals Service but any other law enforcement agency with existing administrative subpoena power to rummage through Internet service providers' records, whether it is on the subject of child pornography or any other subject relating to law enforcement, and that we should restrict severely administrative subpoena powers that are given to law enforcement for, particularly, the gathering of evidence.

This is not to say I am not concerned about the child pornography issue. I think my record has been very clear from the beginning of my service in Congress that I have fought to strengthen legislation to allow law enforcement to crack down on child pornography. And as the author of both the Child Protect Act of 2003 and the Adam Walsh Act of 2007, I think my record is quite clear on this issue.

However, it seems to me that this goes far beyond the issue of trying to prevent people from using the Internet to purvey child pornography, which I think is the most disgusting smut of all the smut that ends up being purveyed, whether it is by electronic means or other means.

We ought to forget about having a statutory retention passed by Federal law. We ought to forget about granting the Marshals Service administrative subpoenas.

This does not strike at the problem in an effective manner, and it runs roughshod over the privacy rights of people who use the Internet for thousands of lawful purposes. And that is why this bill ought to be defeated and be put in the dustbin of history.

And I now yield to the gentleman from Virginia, Mr. Scott, the Ranking Member.

[The bill, H.R. 1981, follows:]

I

112TH CONGRESS
1ST SESSION

H. R. 1981

To amend title 18, United States Code, with respect to child pornography and child exploitation offenses.

IN THE HOUSE OF REPRESENTATIVES

MAY 25, 2011

Mr. SMITH of Texas (for himself and Ms. WASSERMAN SCHULTZ) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, with respect to child pornography and child exploitation offenses.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting Children From Internet Pornographers Act of 2011".

SEC. 2. FINANCIAL FACILITATION OF ACCESS TO CHILD PORNOGRAPHY.

(a) OFFENSE.—Chapter 95 of title 18, United States Code, is amended by adding at the end the following:

"§ 1960A. Financial facilitation of access to child pornography

"Whoever knowingly conducts, or attempts or conspires to conduct, a financial transaction (as defined in section 1956(c)) in or affecting interstate or foreign commerce, knowing that such transaction will facilitate access to, or the possession of, child pornography (as defined in section 2256) shall be fined under this title or imprisoned not more than 20 years, or both.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 95 of title 18, United States Code, is amended by adding at the end the following new item:

"1960A. Financial facilitation of access to child pornography.".

SEC. 3. MONEY LAUNDERING PREDICATE.

Section 1956(c)(7)(D) of title 18, United States Code, is amended—

(1) by inserting "1466A (relating to obscene visual representation of the abuse of children)," before "section 1708";

(2) by inserting "1960A (relating to financial facilitation of access to child pornography)," before "section 2113"; and

(3) by inserting "2260A (relating to increased penalties for registered sex offenders)," before "section 2280".

SEC. 4. RETENTION OF CERTAIN RECORDS BY ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

(a) IN GENERAL.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(h) RETENTION OF CERTAIN RECORDS.—A provider of an electronic communication service or remote computing service shall retain for a period of at least 18 months the temporarily assigned network addresses the service assigns to each account, unless that address is transmitted by radio communication (as defined in section 3 of the Communications Act of 1934).".

(b) SENSE OF CONGRESS.—It is the sense of Congress that records retained pursuant to section 2703(h) of title 18, United States Code, should be stored securely to protect customer privacy and prevent against breaches of the records.

SEC. 5. NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.

Section 2703(e) of title 18, United States Code, is amended by inserting "retaining records or" after "other specified persons for".

SEC. 6. GOOD FAITH RELIANCE ON REQUIREMENT.

Section 2707(e)(1) of title 18, United States Code, is amended by inserting ", or the requirement to retain records under section 2703(h)," after "section 2703(f)".

SEC. 7. SUBPOENA AUTHORITY.

Section 566(e)(1) of title 28, United States Code, is amended—

(1) in subparagraph (A), by striking "and" at the end;

(2) in subparagraph (B), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(C) issue administrative subpoenas in accordance with section 3486 of title 18, solely for the purpose of investigating unregistered sex offenders (as defined in such section 3486).".

SEC. 8. PROTECTION OF CHILD WITNESSES.

Section 1514 of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)—

(i) by inserting "or its own motion," after "attorney for the Government,"; and

(ii) by inserting "or investigation" after "Federal criminal case" each place it appears;

(B) by redesignating paragraphs (2), (3), and (4) as paragraphs (3), (4), and (5), respectively;

(C) by inserting after paragraph (1) the following:

"(2) In the case of a minor witness or victim, the court shall issue a protective order prohibiting harassment or intimidation of the minor victim or witness if the court finds evidence that the conduct at issue is reasonably likely to adversely affect the willingness of the minor witness or victim to testify or otherwise participate in the Federal criminal case or investigation. Any hearing regarding a protective order under this paragraph shall be conducted in accordance with paragraphs (1) and (3), except that the court may issue an ex parte emergency protective order in advance of a hearing if exigent circumstances are present. If such an ex parte order is applied for or issued, the court shall hold a hearing not later than 14 days after the date such order was applied for or is issued.";

(D) in paragraph (4), as so redesignated, by striking "(and not by reference to the complaint or other document)"; and

(E) in paragraph (5), as so redesignated, in the second sentence, by inserting before the period at the end the following: ", except that

in the case of a minor victim or witness, the court may order that such protective order expires on the later of 3 years after the date of issuance or the date of the eighteenth birthday of that minor victim or witness"; and

(2) by striking subsection (c) and inserting the following:

"(c) Whoever knowingly and intentionally violates or attempts to violate an order issued under this section shall be fined under this title, imprisoned not more than 5 years, or both.

"(d)(1) As used in this section—

"(A) the term 'course of conduct' means a series of acts over a period of time, however short, indicating a continuity of purpose;

"(B) the term 'harassment' means a serious act or course of conduct directed at a specific person that—

"(i) causes substantial emotional distress in such person; and

"(ii) serves no legitimate purpose;

"(C) the term 'immediate family member' has the meaning given that term in section 115 and includes grandchildren;

"(D) the term 'intimidation' means a serious act or course of conduct directed at a specific person that—

"(i) causes fear or apprehension in such person; and

"(ii) serves no legitimate purpose;

"(E) the term 'restricted personal information' has the meaning give that term in section 119;

"(F) the term 'serious act' means a single act of threatening, retaliatory, harassing, or violent conduct that is reasonably likely to influence the willingness of a victim or witness to testify or participate in a Federal criminal case or investigation; and

"(G) the term 'specific person' means a victim or witness in a Federal criminal case or investigation, and includes an immediate family member of such a victim or witness.

"(2) For purposes of subparagraphs (B)(ii) and (D)(ii) of paragraph (1), a court shall presume, subject to rebuttal by the person, that the distribution or publication using the Internet of a photograph of, or restricted personal information regarding, a specific person serves no legitimate purpose, unless that use is authorized by that specific person, is for news reporting purposes, is designed to locate that specific person (who has been re-

1 ported to law enforcement as a missing person), or is part
2 of a government-authorized effort to locate a fugitive or
3 person of interest in a criminal, antiterrorism, or national
4 security investigation.".

5 **SEC. 9. SENTENCING GUIDELINES.**

6 Pursuant to its authority under section 994 of title
7 28, United States Code, and in accordance with this sec-
8 tion, the United States Sentencing Commission shall re-
9 view and amend the Federal sentencing guidelines and
10 policy statements to ensure—

11 (1) that the guidelines provide an additional
12 penalty increase of up to 8 offense levels, if appro-
13 priate, above the sentence otherwise applicable in
14 Part J of the Guidelines Manual if the defendant
15 was convicted of a violation of section 1591 of title
16 18, United States Code, or chapters 109A, 109B,
17 110 or 117 of title 18, United States Code; and

18 (2) if the offense described in paragraph (1) in-
19 volved causing or threatening to cause physical in-
20 jury to a person under 18 years of age, in order to
21 obstruct the administration of justice, an additional
22 penalty increase of up to 12 levels, if appropriate,
23 above the sentence otherwise applicable in Part J of
24 the Guidelines Manual.

SEC. 10. ENHANCED PENALTIES FOR POSSESSION OF CHILD PORNOGRAPHY.

(a) CERTAIN ACTIVITIES RELATING TO MATERIAL INVOLVING THE SEXUAL EXPLOITATION OF MINORS.—Section 2252(b)(2) of title 18, United States Code, is amended by inserting after "but if" the following: "any visual depiction involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be fined under this title and imprisoned for not more than 20 years, or if".

(b) CERTAIN ACTIVITIES RELATING TO MATERIAL CONSTITUTING OR CONTAINING CHILD PORNOGRAPHY.—Section 2252A(b)(2) of title 18, United States Code, is amended by inserting after "but, if" the following: "any image of child pornography involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be fined under this title and imprisoned for more than 20 years, or if".

SEC. 11. ADMINISTRATIVE SUBPOENAS.

(a) IN GENERAL.—Section 3486(a)(1) of title 18, United States Code, is amended—

(1) in subparagraph (A)—

(A) in clause (i), by striking "or" at the end;

(B) by redesignating clause (ii) as clause (iii); and

(C) by inserting after clause (i) the following:

"(ii) an unregistered sex offender conducted by the United States Marshals Service, the Director of the United States Marshals Service; or"; and

(2) in subparagraph (D)—

(A) by striking "paragraph, the term" and inserting the following: "paragraph—

"(i) the term";

(B) by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following:

"(ii) the term 'sex offender' means an individual required to register under the Sex Offender Registration and Notification Act (42 U.S.C. 16901 et seq.).".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 3486(a) of title 18, United States Code, is amended—

(1) in paragraph (6)(A), by striking "United State" and inserting "United States";

(2) in paragraph (9), by striking "(1)(A)(ii)" and inserting "(1)(A)(iii)"; and

1 (3) in paragraph (10), by striking "paragraph
2 (1)(A)(ii)" and inserting "paragraph (1)(A)(iii)".

○

Mr. SCOTT. Thank you, Mr. Chairman.

I will read the prepared statement, but I must say I am pleased to join you for the hearing.

The Crime Subcommittee convenes this morning to examine the bill H.R. 1981 that, among other things, imposes an 18-month data retention requirement on non-wireless Internet service providers known as ISPs, gives the United States Marshals Services administrative subpoena power, and substantially increases penalties for certain Federal sex offenses.

The legislation, known as Protecting Children From Internet Pornographers Act of 2011, does many things that I suspect that, if passed, it may not actually be the most effective way of protecting children from Internet pornographers.

Section 4 imposes an 18-month mandate on certain ISPs to retain IP addresses. The question that remains unanswered is whether this data retention mandate, which imposes unknown costs on ISPs, will add anything significant to the process.

When Congress imposes a costly mandate on private industry, there ought to be a corresponding and significant benefit to law enforcement. The information before me fails to demonstrate that the expansive policy proposed in H.R. 1981 will provide that benefit.

Indeed, the GAO reports that currently in 80 percent of investigations, law enforcement officials are already able to obtain the data that they need from ISPs. In the remaining 20 percent, they are virtually always able to obtain information through other means. This is most likely because the majority of ISPs already maintain data from 6 to 12 months.

In light of this, we must balance the additional marginal benefit that law enforcement may receive by extending the mandate to 18 months against the countervailing costs, privacy, and security concerns that such policy implicates.

Rather than address the myriad of factors that pose challenges to child pornography prosecutions, the bill mistakenly focuses entirely on data retention. The GAO's report on the Protect Act makes it clear the backlog in forensic examination of computers is the real issue in these cases, and the bill does nothing to address that problem.

According to the GAO, it can take up to a year for the FBI to conduct a forensic evaluation of a suspect's computer. This bill actually creates more cases in forensic examinations that will be necessary without providing any additional resources. The legislation seems to ignore that the real issue is in fact resources.

So we must ask ourselves about the utility of adding more data, and older data at that, to this queue and exacerbate what is already a significant backlog.

It is undisputed that the overwhelming majority of the 230 million Americans that use the Internet are law-abiding. The ISPs assign millions of IP addresses every day to these users. And when one is looking for a needle in a haystack, the last thing you need is more hay. This is exactly what section 4 would do, accumulate more hay without providing any more tools to sort through it.

The low number of prosecutions also underscores the bill's misplaced focus on data retention. The ISPs provide law enforcement with well over 100,000 cyber-tips every year. These tips require the

preservation of not just the IP address of the suspect, but also as much content from the suspect's account as is available at the time the tip is made. Yet there are only a little over 2,000 prosecutions every year, according to the DOJ's own figures.

Given the data preservation requirements, the lack of data cannot be blamed for the small percentage of prosecutions. It does not take a statistician to see that DOJ already has more data than it has adequate personnel to investigate.

Prosecution surely cannot increase under the House-passed budget, which proposes to cut 4,000 FBI agents. What we need is more resources, not less; more FBI agents assigned to investigate these cases, not less; more personnel to tackle the backlog in forensic investigation of suspect computers, not less; and not more data without resources to process it.

In addition to the failure to provide additional resources to law enforcement, the blanket exemption for all wireless Internet service providers and the potential uses of the data in addition to child pornography cases also concerns me.

The wireless Internet is the largest and fastest-growing mechanism for accessing the Internet. In fact, by the end of the year, there were over 300 million wireless connections in the United States. The exemption for wireless providers would thus appear to exempt almost as much as it covers and undermine the goal of the legislation.

The other uses of data, in addition to child pornography prosecutions, is also a concern. Can that data be vulnerable to hackers for ID theft or available for marketing, copyright infringement cases, divorce cases, or other crimes? These are some concerns that we need to look into it.

And, finally, I join the Chairman in his concern about the administrative subpoena. Under the bill, the Marshals would have more power and more expensive subpoena power than the Secret Service has even faced with an imminent threat on the life of the President of the United States.

I look forward to hearing the witnesses' opinion about the most curious carveout, the wireless carveout, as well as the other issues that I have raised this morning.

And, Mr. Chairman, thank you, and I yield back.

Mr. SENSENBRENNER. The Chair recognizes the Chair of the full Committee, the gentleman from Texas, Mr. Smith, for an opening statement.

Mr. SMITH. Thank you, Mr. Chairman.

Child pornography may be the fastest growing crime in America, increasing an average of 150 percent per year. The Justice Department estimates that there are now more than 1 million pornographic images of children on the Internet. The department also estimates that one third of the world's pedophiles involved in organized pornography rings worldwide live in the United States.

Since the National Center for Missing and Exploited Children, called NCMEC, created the cyber-tip line 12 years ago, electronic service providers have reported 8 million images and videos of sexually exploited children. The number of reports to NCMEC's cyber-tip line of child pornography, child prostitution, child sex tourism, and child sexual molestation, and online sexual enticement of chil-

dren, increased from about 4,000 in 1998 to 102,000 in 2008, an average increase of 200 percent a year.

H.R. 1981, the 'Protecting Children From Internet Pornographers Act of 2011," enables law enforcement officials to successfully locate and prosecute those who want to hurt our children. Often the only way to identify a pedophile who operates a website or exchanges child pornography images with other pedophiles is by an Internet protocol address.

Law enforcement officials must obtain a subpoena and then request from the Internet service provider the name and address of the user of the IP address. Unfortunately, ISPs regular purge these records, making it difficult if not impossible for investigators to apprehend child pornographers on the Internet.

H.R. 1981 directs Internet service providers to retain Internet protocol addresses to assist Federal law enforcement officials with child pornography and other Internet investigations. This is a narrow provision that addresses the retention of only the Internet protocol addresses that providers assign to their customers. It does not require the retention of any content. So the bill does not read any legitimate privacy interests of the Internet users.

Some Internet service providers currently retain these addresses for business purposes, but the period of retention varies widely among providers from a few days to a few months, and providers will even change their own retention periods from time to time. The lack of uniform data retention impedes the investigation of Internet crimes.

H.R. 1981 requires providers to retain these records for 18 months. This mirrors an existing FCC regulation that requires telephone companies to retain for 18 months all toll records, including the name, address, and telephone number of the caller, plus each telephone number called and the date, time, and length of the call. In effect, this bill merely applies to the Internet what has applied to telephones for decades.

Without the identity of the perpetrator, law enforcement officials cannot track down pedophiles, so they continue to threaten our children. The Justice Department describes a disturbing trend in child pornography, that pedophiles who document their sexual abuse of children will only exchange images with other pedophiles who do the same. The result is that people who may have previously only viewed these images now have the incentive to sexually abuse children and produce their own images.

Data retention enables law enforcement officials to catch the abusers and save the children from being abused.

Critics contend that data retention is unnecessary because current law already requires ISPs to preserve records at the request of law enforcement agents for 90 days. But ISPs can only preserve information they still have. By the time investigators discover the Internet child pornography and make the request under this provision, the provider has often already purged the Internet protocol address records.

Both Democratic and Republican administrations have been calling for data retention for a decade. In January, the Justice Department testified that shorter even nonexistent retention by providers frustrate criminal investigations. Every time a provider purges IP

address records, it erases forever the evidence needed to save a child.

In hearings before the Committee this spring, both Attorney General Holder and FBI Director Mueller testified that data retention is invaluable to investigating child pornography and other Internet-based crimes. H.R. 1981 also creates a new Federal offense allowing for Federal prosecution of any person who conducts a financial transaction knowing that it will facilitate access to child pornography.

This bill strengthens protection for child witnesses and victims, who are often subjected to harassment and intimidation throughout the trial period. The bill allows a Federal court to issue a protective order if it determines that a child victim or witness is being harassed or intimidated, and imposes criminal penalties for violation of a protective order. And the bill increases the penalties for child pornography offenders in cases that involve children less than 12 years old.

Parents who once relied on the four walls of their homes to keep the children safe are now faced with a new challenge. The Internet has unlocked the doors and opened the windows. The Internet has proved to be of great value in many aspects of our lives, but it has also become a virtual playground for sex predators and pedophiles to distribute child pornography images and encourage others to engage in child pornography.

Mr. Chairman, I would like to thank my colleague Debbie Wasserman Schultz for cosponsoring this much-needed legislation. I look forward to hearing from the witnesses today and yield back my nonexistent time.

Mr. SENSENBRENNER. The Chair appreciates that.

The Chair recognizes the Ranking Member of the full Committee, Chairman Emeritus John Conyers.

Mr. CONYERS. Thank you, Chairman Sensenbrenner.

I come here to help bring our conservative Members together here. On one level, I am working with the Speaker and the majority leader. There are great differences there that need reconciliation.

And here on the Judiciary Committee, I am working with the Chairman of the full Committee and the distinguished Subcommittee Chairman, who is also an emeritus Chairman. I suppose if I am junior grade that makes him senior grade, since he was there first.

Now we are here today examining 1981, which is to protect children from Internet pornographers, a laudable goal worthy of praise, a noble objective. But the problem here is, first of all, that 1981, if enacted in its present form, would not achieve that goal. And number two, it does other damage that doesn't even exist.

It would create a whole new host of problems, and it is not accidental that there are negative views about this bill or this proposal that are shared by a wide group of leaders and other organizations. I name three or four. The American Civil Liberties Union is opposed to this measure. The Center for Democracy and Technology and the Electronic Privacy Information Center, there are also Internet providers and other organizations that advocate for children, all opposed.

And the fundamental problem is that it fails to achieve its intended purpose to protect children from Internet pornographers, and here is why. First, we need to—and this bill can be made, I think put in a form that people on both sides of the aisle might be able to support it.

Here's the first thing we have to do: Eliminate the exemption of data retention mandate for wireless providers. We need to eliminate the exemption from the data retention mandate for wireless providers. They have got to be included. And why not? If it is that important, why wouldn't we include them?

The bill completely, in its present form, exempts every wireless Internet service that exists from the data retention requirement. If it is good enough for the others, it might be very important for the wireless Internet providers, the same thing.

And as a result, by doing what it does now, the bill would exempt 55 million residential mobile wireless service subscribers. That should be unacceptable to everybody that is supporting the bill. And it doesn't take a scientist to know that criminals will exploit this loophole in 1981 and simply migrate to a wireless service. So that makes the bill useless.

And I wish that was the only thing we needed to correct. But if we corrected that, it would begin to put it on the path to general acceptability.

Mr. SMITH. Will the gentleman yield?

Mr. CONYERS. Of course.

Mr. SMITH. To reassure the gentleman, we are working to do just as you suggested and figure out a way so that we do not exempt the wireless providers, in which case, I look forward to your support.

Mr. CONYERS. Thank you very much, Chairman Smith.

Now there is another consideration that I would put forward to the authors of the bill, both my friends, and whom I respect here on the Committee. And that is limit law enforcement's access to Internet pornography crimes against children, limit law enforcement's access to Internet pornography crimes against children.

The Department of Justice says that this bill would institute a data retention policy for all types of crimes, including routine street crimes. And I have expressed this in an earlier meeting in January, and I think that we may want to revisit this second very important consideration I think that would be needed to get this bill together.

The bill's title, the Protecting Children From Internet Pornographers Act, is a misnomer, because the legislation really is not about those types of crime at all, because if it were, it would certainly not contain a broad exemption for the largest Internet service providers, such as AT&T, and it would target child exploitation.

I will submit the rest of my statement. Thank you.

[The prepared statement of Mr. Conyers follows:]

Statement of John Conyers, Jr. for the Hearing on H.R. 1981, "the Protecting Children from Internet Pornographers Act of 2011" before the Subcommittee on Crime, Terrorism, and Homeland Security

Tuesday, July 12, 2011, at 10:00 a.m.
2141 Rayburn House Office Building

As the title of H.R. 1981 sets forth, this legislation is ostensibly aimed at protecting children from internet pornographers, which is without doubt a laudable goal.

The problem, however, is that H.R. 1981 not only fails to achieve that goal, but does damage in many other respects.

My concerns with the bill are shared by a broad range of organizations, including the ACLU; various privacy advocates, such as the Center for Democracy and Technology and the Electronic Privacy Information Center, Internet service providers, and even some organizations that advocate for children.

My fundamental problem with H.R. 1981 is that it fails to achieve its intended purpose, namely, to protect children from Internet pornographers for several reasons.

Although I tried to reach out to the bill's proponents to suggest changes, none have yet been considered. Were the sponsors to make three simple changes, I would support the bill.

First, eliminate the exemption from the dta retention mandate for wireless providers. The bill completely exempts all wireless Internet service providers from the data retention requirement.

As a result, this bill would *exempt 55 million residential mobile wireless service subscribers*.

It does not take a rocket scientist to know that criminals will exploit this loophole in H.R 1981 and simply migrate to wireless service.

Second, limit law enforcement's access to Internet pornography crimes against children.

The Justice Department says that this bill would institute a data retention policy for *all* types of crimes, including routine street crimes.

I expressed reservations about such a policy at our hearing on data retention last January and I continue to have them.

The bill's title "the Protecting Children from Internet Pornographers Act" is a misnomer because the legislation really is not about those types of crimes as at all.

If it were, it would certainly not contain a broad exemption for the largest internet service providers, such as AT&T, and it would target child exploitation

crimes, rather than mandate an indiscriminate and broad retention policy.

Third, allow the U.S. Sentencing Commission to decide what, if any, enhanced penalties are necessary in these cases.

H.R. 1981 troubles me because it usurps the role of the U.S. Sentencing Commission to set appropriate sentencing guidelines for federal judges.

It does so by *directing* the Commission to drastically increase the sentencing guidelines for sex offenses across the board, not simply those involving children.

These drastic increases are not informed by any research or data about the need for longer sentences.

Therefore, we simply do not know if these augmented sentencing guidelines will actually have

a positive impact on public safety, or simply increase prison costs and exacerbate prison overcrowding like so many of Congress' other misguided sentencing policies.

Considering that it costs $28,284 to house an inmate in federal prison per year, Congress should know whether in fact increased prison terms are necessary and not simply politically expedient.

While I have articulated several concerns with H.R. 1981, I remain open to listening to the testimony and working with Chairman Smith and Congresswoman Wasserman Schultz to address them.

I hope that today's hearing will result in an improved version of the legislation that I could support because it, in fact, protects our Nation's children from Internet pornographers.

5

Mr. SENSENBRENNER. I thank very much the gentleman from Michigan.

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

Ernie Allen is cofounder of the National Center for Missing and Exploited Children and has served as president and CEO for 22

years. He is also the founder of the International Center for Missing and Exploited Children and serves as the CEO. Under his tenure at NCMEC, more than 150,000 missing children have been recovered. He received both his bachelor and jurist doctorate degrees from Louisville University.

Mark Rotenberg is executive director of the Electronic Privacy Information Center, or EPIC, in Washington. He teaches information privacy law at Georgetown University Law Center. He served as counsel to Senator Patrick J. Leahy on the Senate Judiciary Committee after graduation from law school. He is a graduate of Harvard College and Stamford Law School.

Each of the witnesses' written statements will be entered into the record in its entirety, and I ask that each witness summarize his or her testimony in 5 minutes or less.

To help you stay within that time limit, there is a timing light on your table. When the light switches from green to yellow, you will have 1 minute to include your testimony. And when it turns red, your time is up.

And now I will yield to the gentleman from Virginia, Mr. Goodlatte, to introduce his constituent, Sheriff Michael Brown.

Mr. GOODLATTE. Thank you, Mr. Chairman, I appreciate this honor.

Sheriff Brown has been a dear friend of mine for 20 years and for the past 15 years as sheriff of Bedford County. I know of no sheriff or other local law enforcement official anywhere in America who has done more to combat online child pornography. And he has led that through groups such as the Safe Surfing Foundation that educates parents and children about how to keep their children safe on the Internet and through Operation Blue Ridge Thunder, which has led to the prosecution of online child pornographers, not only in southwest and central Virginia but all across the country, in fact, even overseas. His team has uncovered activities that have led to prosecutions in many, many jurisdictions around the country.

He is a retired special agent of the U.S. Treasury Departments Criminal Enforcement Division. And prior to his election as sheriff in 1996, he served as criminal justice consultant and instructor with the Justice Department's International Criminal Investigative Training Assistance Program in Central and South America and the Caribbean.

Sheriff Brown is a member of the executive committee, board of directors of the National Sheriffs' Association, where he currently serves as the Chair of the Technology Committee and is a member of the Congressional Affairs Committee.

This is not the first time Sheriff Brown has made presentations before the Congress, and I welcome him back.

Mr. SENSENBRENNER. I thank you.

Mr. Allen, you are first up and you will be recognized for 5 minutes.

TESTIMONY OF ERNIE ALLEN, PRESIDENT AND CEO, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Mr. ALLEN. Thank you, Mr. Chairman.

As you mentioned, I have submitted written testimony. I would like to briefly summarize.

Mr. SENSENBRENNER. Without objection, all the witnesses' written testimony will be inserted into the record at the point of their testimony.

And the clock will be reset for your 5 minutes.

Mr. ALLEN. Thank you, Mr. Chairman.

I would like to focus on three provisions of the bill, first section 2 on financial facilitation. Our primary concern is that there be nothing in the legislation that impedes the ability of financial companies to work with law enforcement and our center in attacking commercial child pornography.

The basis for that is, in 2006 we created a financial coalition made up of 35 companies, representing 90 percent of the U.S. payments industry. The first priority is always criminal prosecution. However, we know it is impossible to arrest and prosecute everybody. So what has been happening is our center identifies illegal child pornography sites with method of payment information on it. These companies donate to us live accounts, which we provide to law enforcement around the country, which attempts to make purchases on those accounts. When the transaction goes through, we are able to capture that information, we report it to law enforcement and to the payment company. This is an illegal use of the payment system, so they are able to stop payments and shut down accounts.

In 2006, McKinsey Worldwide estimated that the commercial child pornography industry was a multibillion-dollar industry. Just last year the Treasury Department's Office of Terrorist Financing and Financial Crimes indicated that the problem is now effectively zero, that it is less than a $1 million a year. And they attribute that to enforcement and to the ability of private sector companies to stop the use of the payment system to support their enterprises.

So we want to make sure that nothing in the bill keeps these companies from their voluntary action that they are now engaged in that has had such dramatic impact on the commercial child pornography problem.

Second point I want to raise is section 4, the Retention of Certain Records. What we like about this proposal, much as Chairman Smith has indicated, is that there has been long discussion and debate over data retention. We think this is a reasonable, balanced approach that does not mandate retaining content. What it mandates is retaining conductivity information.

There can't be prosecution until law enforcement connects the date and time of the online activity to an actual person, the type of information that is found in electronic service providers' connectivity log. We have to be able to establish the linkage between that IP address and an actual person.

As Chairman Smith indicated, we think this is analogous to the records that telephone companies are required by Federal law to keep, the date and time that a phone number was dialed. There is currently no requirement to do that. And while many companies have policies on data retention, the policies vary widely, are not implemented consistently, and may be for too short a time to have meaningful prosecutorial value.

The third area I want to comment on is section 11, Administrative Subpoenas. And with great respect to the Chairman and the Ranking Member, we believe that it is essential that the Marshals Service receive administrative subpoena power.

Now the basis for that is identifying and tracking noncompliant fugitive sex offenders is a huge challenge assigned to the Marshals Service by the Adam Walsh Act. In 95 percent of the Marshals' cases, the fugitives' use of a communication device, such as the Internet or the telephone, is the key piece of evidence in locating the fugitive.

Currently what the Marshals must do is contact the United States Attorney and obtain an All Writs order, which typically takes about 2 months. In addition, there has already been judicial review, because the is a warrant issued for the fugitives' arrest. Time is vital in searching for a fugitive who, by their very nature, are highly mobile.

Let me mention that since 1948, and with the new law in 1970, administrative subpoena power has been provided to Justice Department law enforcement. However, that has only applied historically to the FBI and not the Marshals Service.

And also, a final point is under the statute, the administrative subpoena power provided to the Marshals Service specifies electronic service provider records and only in child sexual exploitation cases. So I think the intent of Chairman Smith and Congresswoman Wasserman Schultz is to create a surgical, narrow exception that we believe the intent has always been to include Justice Department law enforcement in the administrative subpoena power.

In conclusion, I think that the statute is a great beginning, is an attempt to provide a balanced, reasonable approach to addressing a serious problem.

[The prepared statement of Mr. Allen follows:]

TESTIMONY

of

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

"The Protecting Children From Internet Pornographers Act"

July 12, 2011

Mr. Chairman and distinguished members of the Subcommittee, I welcome the opportunity to appear before you to discuss the Protecting Children from Internet Pornographers Act. We are grateful for the Subcommittee's commitment to the safety of our children.

As you know, the National Center for Missing & Exploited Children ("NCMEC") 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 27 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 1.1 million reports. To date, ESPs have reported to the CyberTipline more than 8 million images/videos of sexually exploited children. To date, more than 51 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.

The child pornography industry has exploded. New technologies such as smart phones, digital cameras and webcams have made it easier for offenders to produce, access, and trade images. More robust storage devices enable offenders to collect unprecedented volumes of images.

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.

There are millions of child pornography images being traded online by individuals who view them for sexual gratification. Offenders can access them for free on all platforms of the Internet, including the World Wide Web, peer-to-peer file-sharing programs, and Internet Relay Chat.

There is also another side to this problem: offenders who treat these children as a commodity, profiting by selling online access to child pornography images. Who is behind this? Law enforcement investigations have found that organized crime networks operate some of these enterprises. One such case was that of the Regpay Company, a major Internet processor of subscriptions for third-party commercial child pornography websites. The site was managed in Belarus, the credit card payments were processed by a company in Florida, the money was deposited in a bank in Latvia, and the majority of the almost 300,000 credit card transactions on the sites were from Americans.

This is but one example of the connection between child pornography and the financial system. In response to concerns about child pornography distributors' use of our financial systems, with the urging of Senator Richard Shelby, then-Chairman of the Senate Banking Committee in 2006, NCMEC created the Financial Coalition Against Child Pornography ("Financial Coalition").

The Financial Coalition is an alliance between private industry and law enforcement in the battle against commercial child pornography. It is managed by the International Centre for Missing & Exploited Children ("ICMEC") and NCMEC. The Financial Coalition is made up of leading banks, credit card companies, electronic payment networks, third party payments companies and Internet services companies. Its members comprise nearly 90% of the U.S. payments industry. Our goal is twofold: (1) to increase the risk of running a child pornography enterprise; and (2) to eliminate the profitability.

In each case NCMEC works hand-in-hand with federal, state, local or international law enforcement, and the first priority is always criminal prosecution. However, our fundamental premise is that it is impossible to arrest and prosecute everybody.

How does the Financial Coalition process work? First, NCMEC identifies apparent child pornography websites with method of payment information attached. Then, the credit card industry works with undercover law enforcement officers to identify the merchant bank involved in the financial transaction. Finally, the merchant bank enforces its Terms of Service to stop the flow of funds to these sites.

The Financial Coalition has given us valuable information about how the commercial child pornography industry has evolved. When the Financial Coalition was launched, it was common to see commercial child pornography website subscription prices of $29.95 per month, payable by credit card. As law enforcement investigations of commercial child pornography websites increased, the websites evolved, requiring alternative payment methods in a multi-layered verification process involving passwords and text messages. More recently, the Financial Coalition has reported that many of these websites are refusing to accept credit cards from the United States. Now, we have found websites that appear to accept a customer's credit card information, but actually use the information to steal the customer's identity, not to sell them child pornography.

The Financial Coalition is critical in the global effort to dismantle enterprises that profit from the heinous victimization of children. What once was believed to be a multi-billion dollar global industry has recently been estimated to be less than a million dollar a year industry worldwide, according to the U.S. Department of Treasury. As the commercial child pornography industry continues to evolve, law enforcement efforts will continue to evolve as well. We urge Congress to ensure that its legislation does not impede the ability of financial companies to work with law enforcement in an effort to fight these criminal enterprises.

NCMEC's CyberTipline receives reports from members of the public and electronic service providers ("ESPs") regarding online crimes against children, 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. The value of the CyberTipline as a source of leads for law enforcement has been greatly enhanced by the collaboration of ESPs.

The greatest challenge to law enforcement investigating online crimes against children is that technology allows offenders to use the Internet with perceived anonymity. There is a significant missing link in the chain from detection of child pornography to conviction of the offender. For example, once a NCMEC analyst reviews a CyberTipline report, adds necessary information and refers 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 an ESP's connectivity log. Connectivity logs provide the link between an Internet Protocol ("IP") address and an actual person. These records are vital to law enforcement investigating and prosecuting these cases.

ESPs' connectivity logs are analogous to the records that telephone companies are required by federal law to keep -- the date and time that a phone number was dialed.
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 may be for too short a time to have meaningful investigative value. As a result, offenders are willing to risk detection by law enforcement, believing that they can operate online anonymously. Federal law requires telephone companies to retain their records for 18 months (47 C.F.R. 42.6).

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 rescue 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 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 retention presents 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.

Identifying and tracking non-compliant fugitive sex offenders has become one of law enforcement's biggest challenges. The Adam Walsh Child Protection and Safety Act of 2006 tasked the U.S. Marshals Service ("USMS") with apprehending these absconded sex offenders. Since 2006 the USMS has arrested over 1,300 fugitives for violations of the Adam Walsh Act.

One of NCMEC's Congressionally authorized responsibilities is to provide training and assistance to law enforcement agencies in identifying and locating non-compliant sex offenders.

NCMEC analysts run searches of non-compliant sex offenders against public-records databases donated to us by private companies for the assistance of law enforcement. We also conduct internal searches for potential linkages of non-compliant sex offenders to NCMEC cases of child abduction, online exploitation and attempted abductions. We forward all information to law enforcement, who uses it to locate the offenders so they can be charged with the crime of non-compliance.

In 95% of the USMS cases, the fugitive's use of a communication device, such as the Internet or telephone, is the key piece of evidence in locating the fugitive. Currently, U.S. Marshals working to locate fugitives must undertake a burdensome and time-consuming legal process to obtain the Internet information. Timeliness is critical in these cases because the Marshals are trying to locate a fugitive, who by nature is mobile in order to evade law enforcement. The delay in the current process provides a window of time during which the fugitive can move again, evading capture by the Marshals.

The U.S. Marshals are key players in the fight against child sexual exploitation. They have made remarkable progress in tracking down non-compliant sex offenders. However, their efforts would be dramatically enhanced if they were granted administrative subpoena authority.

In conclusion, we would like to thank Chairman Smith and Representative Wasserman Schultz for sponsoring this important piece of legislation. Your efforts will undoubtedly help law enforcement better combat child sexual exploitation.

7

Mr. SENSENBRENNER. Thank you.
Sheriff Brown?

TESTIMONY OF MICHAEL J. BROWN, SHERIFF, BEDFORD COUNTY SHERIFF'S OFFICE

Mr. BROWN. Good morning.
Mr. SENSENBRENNER. Could you turn your mike on?

Thank you.

Mr. BROWN. As my Congressman, Congressman Goodlatte, so graciously noted, my name is Michael Brown. I am a retired Federal agent, and I have had the honor of serving as the sheriff of Bedford County, which is the home of the National D-Day Memorial, for the past 16 years.

I also serve on the executive committee and the board of directors for the National Sheriffs' Association. The National Sheriffs' Association represents the 3,083 elected sheriffs across the country and more than 20,000 law enforcement professionals.

I am pleased to have this opportunity to appear before you today to discuss H.R. 1981, the "Protecting Children From Internet Pornographers Act of 2011."

Additionally, the Bedford County Sheriff's Office has been Internet Crimes Against Children Task Force since 1998. We are known as the Southern Virginia Internet Crimes Against Children Task Force.

The expansion and the development of technology has enabled child pornography to become a worldwide epidemic. Child predators have become adept at exploiting their perversion and hiding behind the anonymity of the Internet, making it extremely difficult at times for law enforcement to identify these predators.

As such, unmasking child pornographers on the Internet is a painstaking and complex process for law enforcement officers and typically requires assistance from Internet service providers to accurately identify the perpetrator. I am speaking specifically to section 4 on the Internet service providers.

Having some ISPs only retain their client records for a short period of time—it could be hours, it could be days, it could be weeks, it could possibly be months, so it could be months. And it varies from ISP to ISP.

As such, the limited data retention time and lack of uniformity among these companies can significantly hinder law enforcement's ability to identify predators when they come across child pornography.

To help law enforcement combat Internet child pornography, Congressman Lamar Smith of Texas and Congresswomen Debbie Wasserman Schultz of Florida introduced H.R. 1981. Through 1981, ISPs will be required to retain the IP addresses assigned to customers for 18 months. The 18-month provision is critical, as it will ensure that when law enforcement contacts an ISP looking for a child predator, the identifying information will still exist.

If I could give you just a brief example of why we need this time limit: A cyber-tip from the National Center for Missing and Exploited Children came into the Southern Virginia Internet Crimes Against Children Task Force in February of this year. The case involved someone posting that they were exposing themselves to their 2-and-a-half-year-old child. The only piece event evidence was the IP address that was posted to a Yahoo chat room through an Internet service provider.

While going through the legal process to retrieve the information, we discovered that the ISP only kept the IP history for a period of 30 days. Sadly, the 30-day limit had passed since the evidence was

posted. The case had to be closed due to the lack of further investigative material.

This case, and hundreds like it from the files of the Internet Crimes Against Children Task Forces across the country clearly demonstrate the need to ensure that ISPs retain customer information for law enforcement.

Therefore, it is imperative that this data be retained by ISPs for a significant and standard period of time, so that when law enforcement goes to lawfully request the online information and records, the information still exists.

Additionally, H.R. 1981 provides legal protection for ISPs to further facilitate cooperation with law enforcement and help ease concerns that the ISPs could be held civilly liable for sharing customer information with law enforcement doing a valid investigation.

H.R. 1981 also creates a new Federal offense for individuals who profit from child pornography, greatly enhances penalties for possession of child pornography, provides administrative subpoena authority to the U.S. Marshals to access critical travel information records on fugitive sexual offenders, and strengthens the protections for child witnesses and victims.

Those who prey upon children are among the most violent and vilest offenders in society, and this act, 1981, will ensure that the predators are appropriately and strongly punished as shares.

As sheriffs, it is our responsibility to protect society's most vulnerable, our Nation's children, from the evils of the world. Child pornography is one such evil.

I have been in this business or 44 years. I have worked in Central America, South America, the Caribbean, and in Europe. I thought I had seen every man's inhumanity to man that I could imagine. But I really had not seen anything until I became involved in this arena of child pornography.

The provisions within H.R. 1981 provide law enforcement officers the capabilities necessary to combat child predators and child pornography. The National Sheriffs' Association strongly supports——

[The prepared statement of Mr. Brown follows:]

Testimony before the United States House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security

Hearing on "H.R. 1981 - Protecting Children From Internet Pornographers Act of 2011"

Michael J. Brown
Sheriff, Bedford County, VA
Executive Committee Member and Board of Directors
Member, National Sheriffs' Association

July 12, 2011

Good Morning Chairman Sensenbrenner, Ranking Member Scott, and Members of the Committee. My name is Michael Brown and I currently serve as the Sheriff of Bedford County, VA. I also serve on the Executive Committee and Board of Directors for the National Sheriffs' Association (NSA). The National Sheriffs' Association represents the 3,083 elected sheriffs across the country and more than 20,000 law enforcement professionals, making us one of the largest law enforcement associations in the nation. I am pleased to have this opportunity to appear before you today to discuss **H.R. 1981 – Protecting Children From Internet Pornographers Act of 2011**.

The expansion and development of technology has enabled child pornography to become a worldwide epidemic. Child predators have become adept in exploiting their perversion and hiding behind the anonymity of the Internet, making it difficult for law enforcement to identify these predators. As such, unmasking child pornographers on the Internet is a painstaking and complex process for law enforcement officers and typically requires assistance from Internet Service Providers (ISP) to accurately identify the perpetrator.

However, some ISPs only retain their clients' records for a short period of time. It could be hours. It could be days. It could be weeks. It could be months. And it varies from ISP to ISP. As such, the limited data retention time and lack of uniformity among retention from company to company significantly hinders law enforcement's ability to identify predators when they come across child pornography.

Mr. Chairman, protecting our nation's children against internet predators has been a personal crusade of mine. Since 1998, the Bedford County Sheriff's Office has administered the Southern Virginia Internet Crimes Against Children Task Force

(SOVAICAC) in an effort to crack down on child pornography distributed over the Internet and other computer-related crimes. The SOVAICAC Task Force includes a supervisor, four full time investigators, two forensic analysts, an intelligence analyst, and 64 affiliate law enforcement agencies who blend their talents and resources to fight child exploitation on the Internet.

To help law enforcement combat internet child pornography, Congressman Lamar Smith (R-TX) and Congresswoman Debbie Wasserman Schultz (D-FL) introduced the **H.R. 1981 – the Protecting Children From Internet Pornographers Act of 2011**.

Through H.R. 1981, ISPs will be required to retain the IP addresses and all associated customer information, i.e., billing, lease initiated and expiration information (date IP address assigned and expired) assigned to customers for 18 months. The 18-month provision is critical as it will ensure that when law enforcement contacts an ISP looking for a child predator, the identifying information will still exist.

I would like to give you a real life example of why we need this time limit in regards to ISP data retention. A cybertip from the National Center for Missing and Exploited Children (NCMEC) came into the Southern Virginia ICAC office in February of this year (2011). This case involved someone posting that they were exposing themselves to their 2 ½ year-old child. The only piece of evidence was the IP address that was accessing a YAHOO chat room through a NTelos wireless connection. While going through the legal process to access the information, we discovered that the ISP only kept the MAC (Media Access Control) address and IP history for a period of 30

days. Sadly, the 30-day limit had passed since the evidence was posted. The case had to be closed due to the lack of further investigative material.

This case, and hundreds like it from the files of the ICAC Task Forces, clearly demonstrates the need to ensure that ISPs retain customer information for law enforcement.

Child predators have become technologically savvy and are able to skillfully conceal their identities. As such, it can take law enforcement time to comb through the multitude of online information to successful identify and locate the child pornographer. Therefore, it is imperative that data be retained by ISPs for a significant and standard period of time so that when law enforcement goes to lawfully request the online information and records, the information still exists.

Additionally, H.R. 1981 provides legal protections for ISPs to further facilitate cooperation with law enforcement and help ease concerns that the ISPs could be held civilly liable for sharing customer information with law enforcement during valid investigations.

H.R. 1981 also creates a new federal offense for individuals who profit from child pornography; significantly enhances penalties for possession of child pornography; provides administrative subpoena authority to the U.S. Marshals to access critical travel information and records on fugitive sex offenders; and strengthens the protections for child witnesses and victims. Those who prey upon children are among the vilest offenders in society and the aforementioned provisions will ensure that the predators are appropriately and strongly punished.

As sheriffs, it is our responsibility to protect society's most vulnerable – our nation's children – from the evils of the world. Child pornography is one such evil. The provisions within H.R.1981 provide law enforcement officers the capabilities necessary to combat child predators and child pornography. The National Sheriffs' Association strongly supports H.R. 1981 and looks forward to working with Congress on passage of this legislation.

I want to thank you for the opportunity to come before you today to discuss **H.R. 1981 – the Protecting Children From Internet Pornographers Act of 2011**.

5

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

TESTIMONY OF MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Chairman Sensenbrenner, Mr. Scott, Members of the Committee, thank you for the opportunity to testify today.

My name is Marc Rotenberg, and you have asked me to look at H.R. 1981, Mr. Smith's bill.

I want to begin at the outset by saying that the purpose of privacy laws is of course to protect the privacy of the customer information that a company acquires through provision of a service. And ECPA, although a complicated statute, at its heart has this purpose.

The circumstances under which personal information may be disclosed are set out in a variety of provisions, and there are many safeguards that are built in, including, for example, typically a judicial determination, some type of public reporting, and even notice to the target of an investigation.

Now there are situations that ECPA currently allows for law enforcement to preserve information for up to 90 days and even to seek renewal in those circumstances perhaps where a warrant cannot be obtained right away. That's an exigency. Or for the service provider on a voluntary basis to turn over to the government information when they have a good faith reason to believe that there is actually some threat posing a risk of life or serious physical harm to an identifiable individual.

So there is already in the statute a number of provisions that can be used to address the concerns that have been addressed.

Now I am going to speak to the data retention provision, but I also want to draw your attention to two related provisions that have not yet received much attention in the discussion of the bill.

As several of the Members have indicated at the outset of the hearing, there are serious concerns about data retention. We, of course, live in a time where there is a great deal breach and security breach taking place. Companies are not able, oftentimes, to protect the information that they require themselves for providing services.

This statute would have the effect of mandating the retention of information that businesses might not otherwise keep. And the problem is not only that section 4 establishes that requirement for the assigned IP address, but sections 5 and section 6 create a new type of immunity that has never existed before in the Wiretap Act.

In other words, at the same time that the ISPs would be told: Keep this information. It may be useful for law enforcement. It may also pose some risk to your customers, but be assured that whatever happens to this information, if it is improperly accessed or improperly used, you are off the hook, because what section 5 does is provide a complete immunity for the record retention that is mandated by section 4.

And as we read section 5, by the way, it doesn't even seem to have the qualifying language that otherwise exists for the type of immunity when ISPs properly cooperate with the law enforcement investigations. So section 5 needs to be looked at much more closely.

In similar fashion, we believe that section 6, which creates a good-faith defense for those who are able to overcome the hurdle

in section 5, is also quite broad and would apply, in the plain language of the statute, not only to violations that could be charged under ECPA, but also under any other law as well.

And there are of course today many state laws that require companies to notify their customers when a security breach has occurred, because now the customers are at risk. And, therefore, with this second type of good faith defense that is introduced in section 6, it appears that ISPs will not be responsible, will not be obligated to notify their customers of these harms.

So in our statement, and we describe this in more detail, the problem here is not just the data retention obligation. It is being coupled with an immunity provision that means that information that is kept will not be subject to the same type of responsibility and obligation.

There are two other key points that I would like to make.

The first is that there is clearly a movement toward data minimization in the security field. Now, this is not a new development. In fact, you can go back 25 years to the Video Privacy Protection Act and find a statutory obligation for businesses to destroy information on a customer once it is no longer needed. It is a sensible approach that prevents misuse.

Data retention pulls in the opposite direction from data minimization, which is already in statute, and we think the better approach for privacy.

Finally, I spent quite a bit of time in the prepared statement discussing the experience of the European countries, which have over the last 5 years tried to implement a sweeping data retention obligation. Now I say "tried to implement" because there has been an enormous controversy. The users have objected. The ISPs have objected. The telephone companies have objected.

And when this European directive has been brought into court in the constitutional courts of the European countries, invariably those courts have found these obligations to be unconstitutional.

And I hope you will also take that into account as you consider the proposal.

Thank you again for the opportunity to testify.

[The prepared statement of Mr. Rotenberg follows:]

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

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

Hearing on H.R. 1981, the Protecting Children from Internet Pornographers Act of 2011

Before the

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

July 12, 2011
2141 Rayburn House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, thank you for the opportunity to testify today on "H.R. 1981, the Protecting Children from Internet Pornographers Act of 2011."

My name is Marc Rotenberg. I am the President and Executive Director of the Electronic Privacy Information Center (EPIC), a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. We have a particular interest in legislative proposals that may adversely impact users of communications technology. EPIC, in collaboration with Privacy International, also publishes an extensive survey of international privacy law.[1] I have taught Information Privacy Law at Georgetown University Law Center for more than two decades, and was involved in the development and drafting of the original Electronic Communication Privacy Act.

We appreciate the interest of this Committee in protecting children and cracking down on criminal activities. We have worked with several Congressional committees to strengthen protections for children on the Internet and we support the efforts of this Committee to reduce and prevent harms to children.[2] There are several provisions in the bill before the Committee that we support. However, we have a specific objection to the data retention provision in section 4 of H.R. 1981 and the accompanying immunity provisions in sections 5 and 6. We believe that these provisions would undermine basic Fourth Amendment safeguards, create new risks to Internet users, and are unlikely to solve the problem that Congress seeks to address.

It is also significant that the European Union, which tried to impose a similar data retention obligation on the European member countries, has met continued political resistance, legal objections, and practical problems in implementation. The Europeans are now stepping back from the effort to put in place the same legal rules that this Committee is now considering. That is a warning that should be considered by the Committee as it examines this proposal.

---

[1] EPIC & Privacy International, PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAW AND DEVELOPMENTS (EPIC 2006), *available at* https://www.privacyinternational.org/phr.

[2] EPIC, Comments to the Federal Trade Commission, "2010 Children's Online Privacy Protection Act Rule Review," FTC Matter No. P104503, July 9, 2010, *available at* http://epic.org/privacy/ftc/COPPA_070910.pdf; Marc Rotenberg, EPIC, Testimony and Statement for the Record on the Children's Privacy Protection and Parental Empowerment Act, H.R. 3508, before the House of Representatives, Committee on the Judiciary, Subcommittee on Crime, September 12, 1996, *available at* http://www.epic.org/privacy/kids/EPIC_Testimony.html.

I. The Electronic Communications Privacy Act

A. Background on Privacy Laws

Privacy laws typically establish a statutory framework that sets out the rights and responsibilities for those who collect and use personal information. There is a presumption that companies will not disclose the data concerning their customers unless there is an explicit legal basis to do so. One of the most important circumstances when companies may disclose the data is when a law enforcement agency needs access to information concerning a customer in the course of a criminal investigation. In such circumstances, privacy laws set out a legal standard for disclosure,[3] a process for judicial review, and public reporting requirements providing for the publication of aggregate data that makes possible an analysis of this investigative technique.[4] There is also notice to the customer and others, at an appropriate time, that they were subject to a lawful intercept undertaken by a police agency.[5]

It is also significant that privacy laws often include a data minimization or data destruction provision that makes clear that companies have an obligation to destroy consumer information once it is no longer needed. For example, the Video Privacy Protection Act requires businesses to:

> Destroy personally identifiable information as soon as practicable, but not later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information . . .[6]

Other privacy bills include similar requirement.[7]

B. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") sets out the privacy obligations for the customer records associated with electronic communications, such as email. For purposes of ECPA, there are two types of service providers: electronic communication service providers, which provide " the ability to send or receive wire or electronic communications,"[8] and remote computing service providers, which provide

---

[3] Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 2510 et seq.).
[4] See, e.g., U.S. Courts, "2010 Wiretap Report Shows Increase in Authorized Intercepts," (June 30, 2011), *available at* http://www.uscourts.gov/News/NewsView/11-06-30/2010_Wiretap_Report_Shows_Increase_in_Authorized_Intercepts.aspx.
[5] 18 U.S.C. § 2518.
[6] 18 U.S.C. 2710(e) ("Destruction of old records.")
[7] See e.g. Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified at 15 U.S.C. §§ 6801, 6809, 6821, and 6827).
[8] 18 U.S.C. § 2510(15),

"computer storage or processing services by means of an electronic communication service."[9] An electronic communication service provider would be a company such as Facebook or Comcast, while a remote computing service provider would be a company like Iron Mountain or Amazon Cloud.[10]

C. "Data Retention" and "Data Preservation"

Currently, there is nothing in ECPA that would require service providers to routinely keep personal information concerning their customers beyond the need for providing a service. There are two instances, though, under which the preservation of customer records pursuant to a criminal investigation can be required. A service provider may be required "to preserve records and other evidence in its possession pending the issuance of a court order or other process" for a period of ninety days at the request of law enforcement; this may be "extended for an additional 90-day period upon a renewed request by the governmental entity."[11]

The other provision allowing data retention authorizes law enforcement to utilize a court issued subpoena or warrant to require a "backup copy of the contents of the electronic communications sought" as part of its investigation.[12] This order can only be issued to a remote computing service provider, and it is only for the actual electronic communications, not customer information. The customer is also given the right to challenge the order.[13]

In both of the above exceptions there must be a request from law enforcement for specific records in the context of a particular investigation. Federal law does not currently allow the government to mandate the collection of information about computer services prior to a determination that there is some reason to believe that a particular user has engaged in, or may be engaged in, criminal conduct.

This is a critical distinction. It reflects a central purpose of the Fourth Amendment: to ensure that the investigative powers of the government are directed toward those who have actually committed a crime or maybe planning a crime.

The ECPA data preservation provisions also address the exigency problem that may arise when the government has an adequate legal basis to get access to the information in the possession of the service provider but lacks the necessary legal authority, such as the warrant or subpoena. Recognizing that evidence may be lost in such circumstances, the ECPA allows the government to ensure that the information is preserved pending the receipt of the necessary authority.

---

[9] 18 U.S.C. § 2711(2).
[10] Hereinafter, both electronic communications service providers and remote computing service providers will be generally referred to as "service providers" unless otherwise noted.
[11] 18 U.S.C. § 2703(f)(2).
[12] 18 U.S.C. 18 U.S.C. § 2704.
[13] 18 U.S.C. § 2704(b).

D. Disclosures of records by service providers

There are additional provisions in current law that help address the problem of making user data available to law enforcement agencies. Under certain conditions, service providers are required to turn over records to law enforcement. These provisions enable law enforcement to use a warrant, court order, consent of the customer, or an administrative subpoena to compel the production of certain records.[14] These records include: "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and the means and source of payment for such service (including any credit card or bank account number)."[15]

There are also provisions for emergency voluntary disclosures by service providers.[16] These disclosures are permissible if they are:

> . . authorized in § 2703; with the lawful consent of the customer or subscriber, as may be necessarily [sic] incident to the rendition of the service or to the protection of the rights or property of the provider of the service; to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosures without delay of information relating to the emergency; to the National center for Missing and Exploited Children, in connection with a report submitted thereto under § 2258A; or to any person other than a governmental entity.[17]

In other words, even apart from an actual investigation, communications service providers already have authority to bring to the attention of law enforcement online activities that may raise significant concerns.

II. Current Industry Practices

Since the rollout of always-on broadband internet services meant that Internet Protocol (IP) addresses were no longer part of the phone records associated with dial-up modem phone calls, ISPs have recorded the assigned IP addresses assigned to customer accounts for the business purposes of resolving billing disputes, troubleshooting connections in the event of a failure, and to address security and fraud issues.[18] The costs

---

[14] 18 U.S.C. §§ 2703(c)(1) and (2).
[15] 18 U.S.C. §§ 2703(c)(2)(A) – (F).
[16] 18 U.S.C. § 2702(c).
[17] 18 U.S.C. § 2702(c)(1) – (6).
[18] Online Safety and Technology Working Group, *Youth Safety on a Living Internet*, 101 (June 4, 2010), *available at* http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf [hereinafter OSTWG Report].

and risks associated with retaining this data have led ISPs to limit the duration of retention, though that duration varies among providers. The costs of data retention include physical storage, organization, security, and archive retrieval.[19] More problematic than the monetary costs of implementing retention are the operational interference and competition inhibiting effects that data retention carries.

According to the head of the ISP Association, the close cooperation between ISPs and law enforcement agencies makes effective use of current standards of IP address retention.[20] US ISPA Director Dean stated "we continue to believe that targeted approaches like preservation are the best and most effective use of available resources."[21] Broad data retention requirements impose not only expensive technical compliance burdens, but also may jeopardize the speed and accuracy of investigations.

Mandating retention of IP addresses threatens to undermine effective implementation of the cybersecurity best-practice of data minimization. Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. Minimization also reduces the costs of data breaches.[22]

The Federal Trade Commission recommends that companies "adopt a 'privacy by design' approach by building privacy protections into their everyday business practices, such as not collecting or retaining more data than they need to provide a requested service or transaction."[23] FTC Jon Liebowitz has publicly stated that IP addresses are personally identifiable information, the loss of which could trigger breach warnings as well as a Commission investigation.

The prospect of a data breach at an ISP that retains eighteen months worth of IP addresses, as required under this bill, is particularly troubling. Data breaches are a serious problem, as illustrated by the recent data breaches at the Arizona Department of Public Safety, Epsilon, the Sony Playstation Network and Bethesda Softworks.[24]

---

[19] *Id.* at 102.
[20] Kate Dean, United States Internet Service Provider Association, "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," Testimony before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security, January 25, 2011, *available at* judiciary.house.gov/hearings/pdf/Dean01242011.pdf. (testifying that service providers retain IP addresses as long as they are useful or legally necessary, and that present ISP implementation of robust data preservation practices is superior in both practicability and law enforcement effectiveness to broad data retention.).
[21] *Id.*
[22] OSTWG Report, *supra* note 18 at 102.
[23] Testimony of Jessica Rich, Senate Committee on the Judiciary, Subcommittee for Privacy, Technology, and the Law, Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy (May 10, 2011), transcript *available at* http://judiciary.senate.gov/pdf/11-5-10%20Rich%20Testimony.pdf
[24] *See e.g. Sony Says PlayStation Hacker got Personal Data*, Nick Bilton and Brian Stelter, N.Y. TIMES, April 26, 2011, available at http://www.nytimes.com/2011/04/27/technology/27playstation.html.

Because the ISP must be able to link the IP address to a particular account and individual, hackers who compromised this data would be able to know which IP addresses correspond to which people in the general public. Without this information, it is difficult for a hacker to carry out an attack against an individual's computers; obtaining it usually requires a phishing attack or physical access to the computer.[25]

Aside from the risk of hacking by activist groups like LulzSec and cyber criminals, Congress should consider the national security risks associated with data breaches and targeted attacks by nation states. Rich logs of user network data held by ISPs could prove to be an attractive target for nation state attackers.

The escalating importance of data minimization has been emphasized by recent congressional action. As we explained recently to the House Commerce Committee, it has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset.[26]

III. Proposed Legislative Changes and Potential Problems

A. Data Retention Obligation

Section 4 of H.R. 1981 would modify 18 U.S.C. § 2703, a part of ECPA, by adding § 2703(h). The added section reads:

> Retention of Certain Records- A provider of an electronic communication service or remote computing service shall retain for a period of at least 18 months the temporarily assigned network addresses the service assigns to each account, unless that address is transmitted by radio communication (as defined in section 3 of the Communications Act of 1934).

This amendment would require electronic communication service and remote compı service providers to retain "the temporarily assigned network addresses the service assigns t each account" for a period of eighteen months. In other words, all Internet Protocol ("IP") addresses that are assigned by a service provider must be retained for eighteen months in a manner that links them to the accounts to which they were assigned. This IP address retenti though, would only be mandated to service providers that actually "assign[]" IP addresses.

---

[25] *See* How to Find the IP Address of a Remote Computer, GO HACKING, May 7, 2009, available at http://www.gohacking.com/2009/05/how-to-find-the-ip-address-of-a-remote-computer.html.

[26] EPIC, Hearing on the Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach Before the House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade (June 15, 2011), *available at* http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf. *See also* Edith Ramirez, Commissioner, Federal Trade Commission, Prepared Statement on Data Security, before the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, June 15, 2011, *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf.

Section 4 of H.R. 1981 would introduce an entirely new approach to criminal investigations. It would give the government sweeping authority to mandate the collection a retention of personal information obtained by business from their customers, or generated b business in the course of providing services, for subsequent examination without any reasor believe that information is relevant or necessary for a criminal investigation.

Service providers will no doubt say this will impose significant costs and burdens on the providers of communications services.[27] But more critical still may be the enormous risk it will create for Internet users.

Internet service providers ("ISPs") are the entities that assign IP addresses to individual customers, and they are the only companies that would be required to retain IP addresses for eighteen months. ISPs include companies such as AT&T, Comcast, Cox and Verizon. The proposed legislation would therefore have no impact on companies that do not assign IP addresses, such as Facebook, Google, or Yahoo!. Notably, although AT&T and Verizon would have to retain IP address information for their hardwired internet users, the bill exempts them from retaining IP addresses from their wireless accounts. The bill also exempts providers of public WiFi networks, such as hotels, schools, libraries, coffee shops as well as the vast number of consumers who have an unlocked WiFi router in their living room.

If the purpose of this bill is to create a data trail to catch sexual predators, it will not be very effective. Millions of consumers browse the Internet every day from mobile smartphones, from coffee shops and other open WiFi networks. If this Committee intends for the bill to address the threat from all people using the Internet, it would need to require that every coffee shop require ID before a consumer can browse the web, and establish penalties to prohibit consumers from leaving their own WiFi connections open to the world. Such legislation would not only be unpopular, but cause serious economic harm to small businesses around the country that depend upon easy WiFi access to draw in customers.

In order for the proposed IP address retention to be of use to law enforcement, it logically follows that the ISPs must maintain a database that links the IP addresses to individual identities. Nothing in the bill, though, indicates exactly what information must be retained. Furthermore, even if a customer closes an account with an ISP, that ISP would be required to maintain his records for a full eighteen months after he ceased service.

The government already has broad statutory authority to obtain customer records from ISPs and other service providers. Law enforcement need not rely upon a warrant or judicial subpoena; it is instead authorized to issue an administrative subpoena to seek the

[27] *See* Dean, *supra* note 20.

records.[28] Under this proposed legislation, though, law enforcement would be empowered to use an administrative subpoena, and therefore avoid judicial scrutiny, for records dating back eighteen months. This would be an unprecedented expansion of the ability for the government to directly link a person's online activities to his or her actual identity. Every time an individual uses the Internet and visits a website such as Facebook or Google and sends a message or performs a search, the receiving server, such as Facebook or Google, logs the IP address that is performing this action. With significantly lengthened IP address retention by ISPs, the government would be able to easily link any of those actions on third party websites back to the actual individual using the website. Internet anonymity would be further significantly eroded.

The storage of IP addresses also creates a data breach risk. The linkage of IP addresses with other personal information, including names, puts every customer at risk for computer hacking and electronic attacks.

B. Immunity Provisions

Section 5 amends 18 U.S.C. § 2703(e) to extend immunity from causes of action under ECPA for "retaining records." The amended text of § 2703(e) would read:

> No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for retaining records or providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

This extended immunity appears to apply broadly to any retained records and, unlike the rest of the bill, is not limited to IP addresses. This provides further support for the contention that some other customer records must also be retained to link accounts to IP addresses. Under this language, any civil lawsuits challenging the retention of any records would be barred. It is our reading that the requirement that records be retained pursuant to a court order, warrant, subpoena, statutory authorization or certification would not apply to the retention of records. Service providers would be immunized for the retention of any records, period, even if this retention goes beyond mere IP addresses. Potentially, ISPs could retain a multitude of personal information, including which websites individuals have visited, and be immune from suit under ECPA.

Similarly, Section 6 would amend § 2707(e)(1) to provide a good faith defense to a service provider for retaining IP addresses, amending the statute to read:

[28] 18 U.S.C. § 2703(c)(2)

> Defense — A good faith reliance on— a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703 (f), or the requirement to retain records under section 2703(h), of this title);

This "is a complete defense to any civil or criminal action brought under this chapter or any other law."[29] In our view, the grant of immunity in this provision is sweeping. While Section 5 immunity would apply only to lawsuits brought pursuant to ECPA, Section 6 would provide immunity from all lawsuits, period. If an ISP negligently stores IP addresses in such a way that they are disclosed to the general public, it would be immune from lawsuits. Any consequences that follow from the retention of IP addresses or other records necessary under Section 4 would not be able to be litigated. ISPs would have blanket immunity.

By extending blanket immunity and a good faith defense to these ISPs, Congress would foreclose the ability for consumers to seek damages under ECPA for violations of that law. Instead, ISPs would be free to share their retained IP address information with law enforcement at any time, even if the current legal exceptions, such as those for voluntary disclosure, are not met. Furthermore, there would be no incentives to protect users data. This bill would implement a long-term term retention policy and couple it with immunity for the service providers; it would provide no incentives for this data to be protected. Without blanket immunity, ISPs would be more careful regarding the data that they choose to share with law enforcement for fear of opening themselves up to civil liability under ECPA.

These provisions providing immunity to ISPs is unprecedented in federal wiretap law. The only other time that such immunity has been extended was in the controversial FISA Amendments Act of 2008, in which telecommunications companies that participated in a warrantless wiretapping program with the National Security Agency that targeted American citizens were immunized from civil suits. The proposed grant of immunity in H.R. 1981 would go even farther than that codified regarding FISA in 50 U.S.C § 1185. Under the FISA Amendments Act, the Attorney General had to certify that the electronic communications service provider was acting under statutory authority to assist law enforcement. Furthermore, the Act barred the immunity if a court determined that "such certification is not supported by substantial evidence."[30] Finally, the statute implemented a reporting scheme whereby the Attorney General had to report to Congress the use of the certifications every six months.[31]

In contrast, the proposed legislation goes even farther than the FISA grant of immunity by not requiring any government certification that records were retained in accordance with the statute, there is no provision for judicial review of the good faith

---

[29] 18 U.S.C. § 2707(e) (2009).
[30] 50 U.S.C. § 1885a(b) (2009).
[31] *Id.* at § 1885c.

retention, and there would be no reporting requirement to Congress on how many lawsuits were dismissed due to the grant of immunity.

By extending blanket immunity and a good faith defense to these ISPs, Congress would foreclose the ability of consumers to seek damages under ECPA for violations of that law. Instead, ISPs would be free to share their retained IP address information with law enforcement at any time, even if the current legal exceptions, such as those for voluntary disclosure, are not met. Without blanket immunity, ISPs would be more careful regarding the data that they choose to share with law enforcement for fear of opening themselves up to civil liability under ECPA.

IV. The Importance of Data Minimization Practices

In addition to the legal concerns EPIC has raised about the data retention and immunity provisions in H.R. 1981, it is important to consider the practical problems that might result if these provisions are adopted. Security experts have made clear that the best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the first place.[32]

In 2008, a group of six security experts analyzed the Protect America Act of 2007,[33] the amendments to the Foreign Intelligence Surveillance Act, looking for potential security hazards of the statutory scheme. These researchers included Whitfield Diffie of Sun Microsystems and Peter G. Neumann, a well-known expert in information security. They concluded that "minimization matters," specifically finding that "[a]n architecture that minimizes collection of communications lowers the risk of exploitation by outsiders and exposure to insider attacks. . . . It should be fundamental to the system's design that the combination of interception location and selection methods minimizes the collection of purely domestic traffic."[34]

Similarly Professor Fred H. Cate has recommended "[t]he use of data minimization and anonymization and other tools to limit the amount of information revealed to only what is necessary and authorized."[35] He goes further and identifies a number of tools and techniques so that "analysts can perform their jobs . . . without the need to gain access to personal data until they make the requisite showing for disclosure."[36]

---

[32] Larry Dignan, When it Comes to Data, Less is Better, eWeek (May 3, 2005), *available at* http://www.eweek.com/c/a/Data- Storage/When-it-Comes-to-Data-Less-is-Better/.
[33] Pub. L. No. 110-55, 121 Stat. 552 (2007).
[34] Steven M. Bellovin, et al., Risking Communications Security: Potential Hazards of the Protect America Act, IEEE SECURITY & PRIVACY, Jan.–Feb. 2008, at 24, 31.
[35] Fred H. Cate, Government Data Mining: The Need for a Legal Framework, 43 HARV. C.R.-C.L. L. REV. 435, 488 (2008).
[36] Id. at 488–89.

Data minimization is classified as a security method as much a privacy protection. In fact, while speaking on a recent panel on Information Security Best Practices, two professors at the Wharton School of Business characterized the retention of personal data as "increasingly a liability for companies" concerned about the risks of data breaches.[37]

If sensitive information must be stored and accessed, the principle of data minimization requires that the smallest possible amount of information be used. Congress has acknowledged the importance of data minimization. For example, the amendments to the Foreign Intelligence Surveillance Act require adoption of minimization procedures as appropriate for all data acquisitions authorized under the section.[38] The definition of "minimization procedures" is set forth in two different portions of the statute, one for physical searches[39] and one for electronic surveillance.[40] The two definitions include four types of procedures: procedures "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons;" procedures to prevent the unnecessary dissemination of nonpublicly available information "in a manner that identifies any United States person, without such person's consent;" procedures that require the disposal within 72 hours of the "contents of any communication to which a United States person is a party" acquired without a court order unless a new court order is obtained allowing retention, disclosure, or dissemination; and procedures that allow for exceptions to the retention and dissemination restrictions with respect to criminal evidence.[41]

These terms demonstrate Congress's awareness that acquisition limitations are necessary but not sufficient, and that limitations on the government use of sensitive personal information are also required. These terms are mirrored in other statutes governing similar searches, including the provisions for investigatory wiretaps in the criminal context.[42]

V. The European Experience with Data Retention Requirements

In considering this proposal to establish a broad mandate for data retention in the United States, it is also important to consider the recent experience of European countries with a similar proposal. In 2006, the European Union issued the Data Retention Directive, relating to telecommunications services.[43]

---

[37] Forbes, What Personal Data Should You Keep—And Toss? (Mar. 19, 2009), available at http://www.forbes.com/2009/03/19/heartland-paymentsecurity- entrepreneurs-sales-marketing-security.html.
[38] 50 U.S.C. § 1881a(e)(1) (2009).
[39] 50 U.S.C. § 1821(4) (2009).
[40] 50 U.S.C. § 1801(h) (2009).
[41] 50 U.S.C. § 1801(h) (2009).
[42] 18 U.S.C. § 2518(5) (2009).
[43] Directive 2006/24/EC amended the Directive 2002/58/EC on data protection

According to the Date Retention Directive, European countries were required to store the telecommunications data of every customer for a period of between 6-24 months during which time police and security agencies may request access to this data in order to discover information relating to IP addresses, email dates/times, text messages sent/received and phone calls made and received.

The response to the Data Retention Directive has been forceful and unequivocal. Service providers, technical experts, and privacy and human rights organizations have opposed it. As a consequence many European countries delayed implementation. Then the law was challenged in the national courts. All of the European countries that have considered the legality of the data retention obligation have found it unconstitutional.

Romania implemented the law, but subsequently declared it unconstitutional.[44] Germany found the law unconstitutional.[45] The Constitutional Court of the Czech Republic annulled the transposition law.[46] Most recently, the Supreme Court of Cyprus ruled that retained data can only be accessed "in cases of convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy administration."[47] Legal challenges continues in Ireland, Poland, and elsewhere.

The EU Home Affairs Commissioner Cecilia Malmström said that "so far not been convinced by the arguments for developing extensive systems for storing data, telephone conversations, e-mails and text messages. Developing these would be a very major encroachment on privacy, with a high risk of the systems being abused in many ways. The fact is that most of us, after all, are not criminals."[48]

The European Data Protection Supervisor has recently said, "The quantitative and qualitative information provided by the Member States is not sufficient to draw a positive conclusion on the need for data retention as it has been developed in the Directive.

---

[44] Romanian Constitutional Court Decision No. 1258, Oct. 8, 2009, *available at* http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

[45] Der Spiegel, *German High Court Limits Phone and Email Storage,* Mar. 2, 2010, *available at* http://www.spiegel.de/international/germany/0,1518,681251,00.html.

[46] The Jurist, *Czech Constitutional Court Overturns Parts of Data Retention Law*, Mar. 31, 2011, *available at* http://jurist.org/paperchase/2011/03/czech-constitutional-court-overturns-parts-of-data-retention-law.php.

[47] Techdirt, Apr. 5, 2011, *Czech Court Says No to Data Retention Rules, available at* http://www.techdirt.com/articles/20110404/00003913757/czech-court-says-no-to-data-retention-rules.shtml.

[48] European Parliament, Debates, Liberty and Security, 7 September 2005, Cecilia Malmström (ALDE), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20050907+ITEM-002+DOC+XML+V0//EN&language=EN&query=INTERV&detail=3-044.

Further investigation of necessity and proportionality is therefore required, and in particular the examination of alternative, less privacy-intrusive means."[49]

He further stated that the Directive "does not meet the requirements imposed by the fundamental rights to privacy and data protection, mainly for the following reasons: the necessity for data retention as provided in the Directive has not been sufficiently demonstrated; data retention could have been regulated in a less privacy-intrusive way; the Directive leaves too much scope for Member States to decide on the purposes for which the data might be used, and also for establishing who can access the data and under which conditions.[50]

The European Parliament committee responsible for evaluating the Data Retention Directive has just last month raised a wide range of objections. Parliament Members criticized the lack of proof for data retention, the lack of means for evaluation of the technique and further questioned whether it is an effective law enforcement technique.[51]

The European Digital Rights (EDRi), a network of human rights and civil liberties organizations across Europe, found clear opposition to the Data Retention Directive and called for repeal. It concludes that European citizens have 'gained nothing' from the Directive, but have had their privacy rights substantially hindered. Specifically, the EDRi reported that the Commission has failed to prove that data retention results in crime reduction, arguing that statistics provided by Member States have indicated that the vast majority of data used by law enforcement authorities would also have been available without obligatory data retention. EDRi cited the fact that neither Germany nor the Czech Republic have seen an increase in crime detection following the Directive's implementation, despite the absence of data retention.[52]

In conclusion, the EDRi report described the treatment of citizens' data under the European data retention requirement as "chaotic and lawless", and concludes that the Directive has failed on every level: it has failed to respect the fundamental rights of EU citizens, it has failed to harmonize the European single market, and it has failed in its objective to improve crime detection and prevention.

VI. Recommendations:

A. Remove Sections 4, 5, and 6

---

[49] Office of European Data Protection Supervisor, *Evaluation Shows that the Data Retention Directive Does Not Meet Privacy and Data Protection Requirements, Says EDPS*, May 31, 2011, *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-06_Data%20Retention%20Report_EN.pdf.

[50] *Id.*

[51] EDRi, "EDPS: Data Retention Directive Fails to Meet Data Protection Requirements," June 1, 2011, *available at* http://www.edri.org/edrigram/number9.11/data-retention-directive-failure-edps.

[52] EDRi, "EDRi evaluation of data retention shows it has significant costs but no benefits," Apr. 17, 2011, *available at* http://www.edri.org/data-retention-shadow-report

EPIC recommends that the Committee refer H.R. 1981 without Sections 4, 5 and 6, the data retention requirement and the immunity provisions. While we recognize the problems confronting law enforcement in combating child pornography, these sections will create many new problems and are unlikely to address the problem Congress has identified.

Adopting Section 4 as written would create new risks, including the danger of breaches of data that would not otherwise be retained that could cause harm to millions of customers. Section 4 is also contrary to current practice. ISPs have many reasons, including security, for not currently storing this data. Section 4 creates unbounded law enforcement authority and would enable surveillance of all Internet users, regardless whether there is any reason to believe that they engaged in unlawful activity.

In the event that the Committee includes Section 4, EPIC recommends that sections 5 and 6 be excluded. ISPs, like other private companies, should be held accountable for violating the law or negligently exposing consumer information to malicious parties on the Internet. To create a broad immunity provision for the collection of personal data unrelated to specific criminal conduct is to invite abuse, or the very least to allow for negligence in the storage of sensitive personal information.

B. New Reporting Requirement for Access to Transactional Data

As you consider new efforts to expand law enforcement authority in online investigations, we would ask you also to consider new reporting requirements, based on current reporting requirement in the federal wiretap law that would provide a clearer picture of how record requests are used in practice. The annual reports of the Administrative Office of the U.S. Courts have provided a clearer picture of the use of wiretap authority. [53]

Although this data retention requirement has been introduced as part of a bill focuse child sexual exploitation, there is no evidence to suggest that the majority of law enforceme requests for customer subscriber information relate to child protection cases. Congress shov great wisdom in the past by requiring the creation of annual reports that detail the use of wi authorities.

In the past decade, the ability of law enforcement, specifically the FBI, to obtain records without judicial oversight has raised substantial concerns, as documented by the FBI's own Office of the Inspector General.[54] Because administrative subpoenas could be utilized without judicial oversight to obtain eighteen months worth of IP address records

[53] 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy) (The wiretap reports provide a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area.")

[54] *See A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (Jan. 2010), available at http://www.justice.gov/oig/special/s1001r.pdf.

from ISPs, it is important that Congress be informed about how often such requests take place and how many United States citizens are targeted.

This committee should consider similar reporting requirements for law enforcement requests to Internet providers similar to those that were considered by this Committee in 20

Conclusion

Child pornography is certainly a substantial and difficult issue. But the data retention solution proposed in this bill is overly expansive and invasive. This collection of user data will, in fact, create a new threat for millions of internet users: the threat of dragnet law enforcement and data breaches. The experience with Europe is telling.

We urge you to take out sections 4, 5, and 6 of H.R. 1981. But if you choose to go forward with the data retention obligation contained in section 4 then it is critical to remove the immunity provisions in section 5 and 6. At a time of increasing security breaches and rising instances of identity theft, nothing could be worse than to unnecessarily collect vast amount of information on Internet users without establishing appropriate and necessary safeguards for users.

---

[55] House Committee on the Judiciary, Subcommittee on the Constitution, Hearing on the Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act (Sept. 6, 2000) *available at* http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0f.htm.

Mr. SENSENBRENNER. Thank you very much.

The Chair will defer his questioning and will begin by recognizing the gentleman from Texas, Mr. Smith.

Mr. SMITH. Okay. Thank you, Mr. Chairman.

Sheriff Brown, let me direct my first question to you, and it is this: Can you give us examples of cases that have not been able to be solved because ISPs have not retained the data necessary and that would have been used by law enforcement officials?

Mr. BROWN. Yes, sir, Congressman.

Mr. SENSENBRENNER. Sheriff, could you——

Mr. BROWN. Pardon me?

Mr. SENSENBRENNER. Please turn your mike on.

Mr. BROWN. You would be surprised that I am a head of an ICAC task force.

The example I used in my statement just a minute ago, this was in February of this year, and we had an incident of a posting on a Yahoo account of an individual exposing himself or herself—we don't know—to their 2-and-a-half-year-old child. And because of the inability—the ISP only kept the data for 30 days. And by the time we got the information, were able to start tracking, the 30 days had expired, and we no longer had an ability to bring this additional information, investigative evidence, into play.

We have had this happen on a number of occasions. I can't tell you exactly how many. I believe, and I think I speak for all of the ICAC task forces, if you bring a task force in, they are going to tell you and they are going to give you specific examples of the data not being retained, and as a result, the case had to be just closed.

Mr. SMITH. Okay. Thank you, Sheriff Brown.

Mr. Allen, let me ask a couple questions to you. The first is, is child exploitation some remote type of crime that does not occur very often? Or does it occur more often than a lot of us might expect?

Mr. ALLEN. Mr. Chairman, it is exploding with the advent of the Internet.

Just to give you one illustration, 2003 we began what was called a Child Victim Identification Program in which law enforcement and prosecutors would send us images. And what we would attempt to do is to identify the child victims, so the child could be rescued, located, identified, and identify the perpetrator.

Our staff reviewed 13 million child pornography images and videos last year. We are currently reviewing roughly 300,000 a week, so this is an exploding problem.

The second aspect of this I think is widely misunderstood, is we hear all the time, well, child pornography, isn't this really just adult pornography? Aren't these 20-year-olds in pigtails made to look like they are 15? Of these now 53 million images that we have reviewed, of the children identified, 77 percent had been prepubescent; 10 percent of the 77 percent have been infants and toddlers.

So just 23 percent, and that is not incidence study. I don't suggest that it is empirical. It is based on what is sent to us. But overwhelmingly, this is a problem involving very young kids who don't tell. When the image of their sexual abuse is captured on film or video, reporting drops to virtually zero.

Mr. SMITH. Mr. Allen, a related question, is there a link between the possession of child pornography and the actual victimization of children? And if so, how substantial is that link?

Mr. ALLEN. We believe there is. Now there is debate about, in many cases people are talking about mere possession, but what we see is that there is an escalating effect, that today's images are not going to be satisfactory to this person tomorrow.

Mr. SMITH. What percentage of people who possess child pornography actually victimize the child? Isn't it close to 40 percent?

Mr. ALLEN. Well, we think it is higher than that. There is some research at the Federal Bureau of Prisons that suggested it was higher than that.

We think that, ultimately, the images alone are not going to be enough for a percentage of these guys. Whether it is 20 or 40 or 80, we don't know, but it is substantial.

Mr. SMITH. Thank you, Mr. Allen.

Mr. Rotenberg, I take your comments about section 4 and 5 as legitimate and sincere constructive criticism, and we will take a look in more depth at your comments.

But also let me say to you that if a provision is unclear, or if it is a 50-50 kind of proposition, we are going to give the benefit of the doubt to saving children, and that is the point of this bill. But still, we will take a look at your suggestions.

Thank you, Mr. Chairman. I yield back.

Mr. SENSENBRENNER. The gentleman from Virginia, Mr. Scott?

Mr. SCOTT. Thank you.

And I would like to follow up on along the questions.

Mr. Allen, the Supreme Court has made a big deal out of whether or not these are real children or cartoons. It is no question that these are in fact real children; is that right?

Mr. ALLEN. Yes, sir. And in fact, that is why we created our Child Victim Identification Unit. It is because of the Supreme Court decision in 2002.

Mr. SCOTT. And when you provide law enforcement with all these leads, is it not true that they don't have anywhere close to the resources needed to follow through on all of the leads you give them?

Mr. ALLEN. Absolutely. I mean, the scale of the problem vastly exceeds the capacity of law enforcement to deal with it.

Mr. SCOTT. Mr. Rotenberg, what would be the cost to the ISPs to retain this data?

Mr. ROTENBERG. I don't know, Mr. Scott, exactly what their costs would be, but I suspect it would be significant, because it is not current practice. In fact, the ISPs I think have avoided trying to do this because of some of the concerns that have been raised but with respect to costs.

Mr. SCOTT. Well, the comparison has been made to telephone tolls, but it is a fact that the telephone companies already keep the toll data; is that right? That most of the calls are not toll calls. They just keep the toll records, not the local call records; is that right?

Mr. ROTENBERG. That is correct.

Mr. SCOTT. Now, one of the problems that you have articulated is if you keep all this data, it is sitting there for hackers to get access to. And you pointed to the immunity provision.

What is the liability now if you have data sitting around that somebody accesses and causes harm?

Mr. ROTENBERG. Well, there are a variety of the fines. Certainly under ECPA, they are both civil fines, there can be criminal penalties. And they are also important security breach notifications.

And I wanted to draw your attention to this point, because if you are looking at the papers nowadays it is clear that breach notices are very important. If the immunity provision is left in place, people won't even know if their personal data is improperly accessed or disclosed.

Mr. SCOTT. A suggestion that this information will be used for child pornography cases and the sneak and peek, when we were told that we needed sneak and peek warrant authority to protect us from terrorism, we look up and out of over 700 sneak and peek warrants, three were for terrorism. All the rest were something else.

If you have this data, would it be available for divorce cases?

Mr. ROTENBERG. I think it could be available for a wide range of cases. In fact, I looked at the January hearing record, and Mr. Weinstein from the Department of Justice said at that point he thought it would be obvious that the data would be used in other investigations.

Mr. SCOTT. Marketing?

Mr. ROTENBERG. Certainly.

Mr. SCOTT. Contract disputes?

Mr. ROTENBERG. Yes.

Mr. SCOTT. Copyright infringement, that kind of stuff?

Mr. ROTENBERG. Civil subpoena. Yes.

Mr. SCOTT. Sheriff, you indicated that you were following through on a case, and if you had the information, it would have been helpful.

If the information had been available, what probable cause information would you have already at your disposal to even seek to go through the retained data?

Mr. BROWN. Well, the IP address, all of the associated information with that, who it was registered to, when it was registered. If, in fact——

Mr. SCOTT. You have that already.

Mr. BROWN. Pardon?

Mr. SCOTT. You would have that already. What would you have already?

Mr. BROWN. We didn't have anything, and we would not have——

Mr. SCOTT. Well, if you don't have anything, how do you access—do you need any kind of probable cause to start searching through the data?

Mr. BROWN. The tip that we got is called a cyber-tip, and we receive them from the National Center for Missing and Exploited Children.

Mr. SCOTT. And what information does that provide you?

Mr. BROWN. That a posting of some type involving child pornography has been entered into and is on the Internet in some location. And then we at that point go to the Internet service provider to track that information.

Mr. SCOTT. What information—Mr. Rotenberg, what information is retained?

Mr. ROTENBERG. Well, a typical log would include the IP address, the date and time of access to the website, most likely a filename, maybe a security flag. And it is of course the linkage between the IP address which would be in the log with the actual account owner that I think people are interested in.

Mr. SCOTT. Does it give you any content?

Mr. ROTENBERG. It would give you access to content, because the log would typically include the name of the file that has been transferred.

Mr. SCOTT. If you had that information, would you know what information had actually been transferred? Or would it just note what site you were looking at?

Mr. ROTENBERG. Well, typically in a web log, I think you would know what information was transferred, because you would be able to see the record locator on the file and, therefore, have access to the content.

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

The gentleman from South Carolina, Mr. Gowdy?

Mr. GOWDY. Thank you, Chairman.

Mr. Rotenberg, ISPs currently maintain all sorts of data—name, address, Social Security number, credit card information. Do you really think getting an IP address is going to open up all sorts of mayhem that doesn't already exist?

Mr. ROTENBERG. Well, Mr. Gowdy, I won't dispute there is currently a lot of risk, but when you have a situation with a lot of risk, I don't think you want to add to the risk. And it is the reason that the ISPs are moving away from this extensive data collection.

The attacks have become much more severe in last few months.

Mr. GOWDY. I am not disputing that. What I am asking you is, are you willing after this hearing to sit down with the sheriff or any other sheriff and help them investigate crimes that are incredibly hard to investigate and incredibly hard to prosecute? Are you willing to strike some balance between privacy and his desire to protect children?

Mr. ROTENBERG. There is no dispute that these crimes are very serious, and they should be——

Mr. GOWDY. I didn't say serious. I said hard to investigate and hard to prosecute.

Mr. ROTENBERG. Yes. But it is not clear that this proposal would actually make it easier to investigate those crimes. You see, this is my concern. You are going to create a new data retention obligation that will create a risk to your 99.99 percent of innocent users of the Internet. And for the bad people who you are really tried to go after, it is not clear that this bill solves the problem.

You have an enormous carveout——

Mr. GOWDY. Do you have another way to investigate Internet crime other than capturing the IP address?

Mr. ROTENBERG. Well, I think when you prosecute and when you convict, I think you maybe need to send a more powerful message than is currently being——

Mr. GOWDY. How are we going to get a conviction? How are we going to get an indictment? How are we going to get an arrest war-

rant from a magistrate judge if we don't have the IP address and we can't link it to a perpetrator?

Mr. ROTENBERG. Well, I am not an expert in this field, but I do know that the forensic techniques have become considerably better over the last few years.

Mr. GOWDY. Forensic techniques assume that you have the computer. How are you going to get the computer if you can't link it to an IP address?

Mr. ROTENBERG. There is a lot of information associated with Internet communications, header information and detailed information contained in the content of the message that makes it easier today for people to get access to the type of information you are describing than just a few years ago.

And I actually think with the introduction of some of the new Internet protocols, some of the concerns you have will be addressed as well.

But it will not be perfect. I mean, I concede this. There will be cases that you may not be able to solve.

Mr. GOWDY. Mr. Allen, there are already cases we are not able to solve. There are millions of images?

Mr. ALLEN. Yes, sir.

Mr. GOWDY. You have identified about 3,500 children.

Mr. ALLEN. Yes.

Mr. GOWDY. I have been out of the prosecutorial business for a long time now. Is it still a defense that it is not a real child, that it is a computer—I am not talking about a cartoon that Mr. Scott made a reference to. I am talking about a commuter-generated image of a prepubescent youth that the defense says, it is not a real child.

Mr. ALLEN. Mr. Gowdy, absolutely. As a result of the 2002 Supreme Court decision, there are a lot of defense counsel in this country who, you know, you seize 10,000 images, who will argue these aren't real kids. And there are a number of judges who are saying to the prosecutors, prove that they are.

That was the genesis of the creation of our Child Victim Identification Program, so that if they send us 5,000 images and we are able to identify five of the kids who have been previously identified—because these images recirculate; they stay out there—that is enough to sustain a conviction.

But there is no question that that is an argument that continues to be made, and it is important to sustain the convictions. It is more important to identify who the kids are, because in many of these, this is ongoing abuse.

Mr. GOWDY. But it is one more layer that law enforcement and prosecutors have to overcome to get a conviction in this area of crime that everyone concedes is as evil and inhumane as any, the fact that we have to prove that it is a real child and not computer-generated.

Are other countries cooperative? I know a lot of these children come from other countries. I know you are doing the best job you can identifying kids. Are other countries helping?

Mr. ALLEN. Absolutely. We are making great progress. There is a virtual global task force now that links law enforcement efforts in Canada, United Kingdom, Australia, Italy, seven or eight other

countries. Interpol is playing a key role in terms of collecting these images of identified kids.

So there is enormous progress being made. More Federal prosecutions for child pornography last year in this country than at any time in history.

But as Mr. Scott points out, we are still barely scratching the surface.

Mr. GOWDY. All right, good.

Sheriff Brown, thank you for your long and distinguished service in law enforcement.

Mr. BROWN. Thank you. Did you get all five pages?

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

The gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Thank you, Chairman Sensenbrenner.

I think I sense that there is a feeling that we may be able to, through some kind of consideration after this hearing, began to move toward a more acceptable piece of legislation.

You know, I suppose there is an explosion, but the similar identification of horrible instances doesn't make me really feel that that proves there is an explosion. I take your word for it.

Now Chairman Lamar Smith has agreed with me that this exemption of all wireless Internet service providers from the data retention requirement needs to be re-examined. Would that be a good first step, attorney Rotenberg, for us to begin?

Mr. ROTENBERG. I think to address Mr. Gowdy's concerns, to have an effective response from a law enforcement side, you would have to apply to wireless providers. Otherwise, it becomes obvious how to escape detection.

Mr. CONYERS. Yes.

Sheriff Brown, do you concur that this is a part of the bill that we might want to look at again?

Mr. BROWN. Yes, sir. Absolutely.

Mr. CONYERS. How do you feel about this, Mr. Allen?

Mr. ALLEN. I agree, Chairman Conyers, that it is complex. There are a series of complexities to the issues——

Mr. CONYERS. Of course.

Mr. ALLEN. But I think it is a very important step to take.

Mr. CONYERS. Thank you.

Thank you, all.

Here is a little more sticky consideration, is that this bill might institute accidentally a data retention policy for all crime.

Is that over the top, Mr. Rotenberg? Is that just an exaggeration that we needn't concern ourselves with?

Mr. ROTENBERG. I think, Mr. Conyers, that is clear from the plain text of the bill. The bill simply says, let's establish the ability to identify in the ISP record every single user of that service. And there is no effort at the outset to distinguish those who may be engaged in criminal conduct from those who are not. So that is the starting point.

Mr. CONYERS. Sheriff Brown, I sense that you might be troubled by the whole idea that we might inadvertently or deliberately set about setting up a system that would have retention of all crime. That isn't what you came here today to testify for, is it?

Mr. BROWN. My primary concern today was with the retention. That is why I am here for the National Sheriffs' Association.

It is pretty simple to an old country sheriff that we need more time to investigate these instances that we are coming up against.

Mr. CONYERS. Sure. But Mr. Allen has already pointed out that we are so underresourced. That is your main problem. If we weren't in this room today on this subject, the big problem is we are not giving you the resources that you need. Isn't that it?

Mr. BROWN. Law enforcement always wants more. We need more people on the street. We need more funding. In this particular arena, we are completely snowed under.

And again, just more clear, defined information from these ISPs would be greatly appreciated.

Mr. CONYERS. But you are not about all crime. You are trying to get at child pornography. You are not trying to get at every crime that might be committed in the books. You are not for that, are you?

Mr. BROWN. I am sorry?

Mr. CONYERS. You are not for getting retention policy for every crime on the books, are you? No, you're not.

Mr. BROWN. No, I am here for the Internet Crimes Against Children Task Force.

Mr. CONYERS. Are you, Mr. Allen? Mr. Allen, you can answer.

Mr. ALLEN. No. Let me say, Mr. Conyers, I know that Director Mueller and Attorney General Holder feel that this is important not just for child pornography crimes.

I am here today to talk about access to this kind of——

Mr. CONYERS. Oh, you mean that they are for it? Are you implying that?

Mr. ALLEN. I think what they have said in the past is that data retention——

Mr. CONYERS. On all crimes?

Mr. ALLEN. I think that is right.

Mr. CONYERS. Oh, boy.

Mr. SENSENBRENNER. With that, the gentleman's time has expired.

The gentleman from——

Mr. CONYERS. Thank you very much.

Mr. SENSENBRENNER. Mr. Poe?

Mr. POE. Thank you, Mr. Chairman.

Thank you for being here, Mr. Allen. It is always good to see you. Thanks again for the hard work you do. You are the angel for America's children. And I mean that, you and your organization.

Sheriff, I appreciate you being here. Being a former judge, I always liked working with sheriffs. However, I don't really forgive the Sheriffs' Association for hiring Stephanie Garlock away from me. So anyway——

Mr. BROWN. And I can understand that, sir.

Mr. POE. Mr. Rotenberg, I would like to start with you. Being a former judge and a prosecutor, I still think judicial review, when appropriate, is much better than prosecutorial review, whether it is a Marshals Service or the U.S. Attorneys' Office.

Do you see any problems in the proposed legislation about warrants?

Mr. ROTENBERG. Well, there is a provision, sir, to give the Marshals Service new administrative subpoena authority. I didn't look closely at that provision, but I think it may be something that should get a little bit more scrutiny.

I agree with you that judicial review is always preferable, and when you are in the subpoena realm, you just don't quite know what the basis might be for the investigation.

Mr. POE. All right.

Mr. Allen, based on all the information that you have received and what you know about this issue, the sites that we are talking about here, how many of them are American sites? How many of them are from overseas? Can you give us a percentagewise?

Mr. ALLEN. It is hard to say, because so many of the overseas sites flow through U.S.-based servers.

Mr. POE. Okay.

Mr. ALLEN. But what we see in terms of the victims is that this is a global problem, but that a stunning number of the victims, as much as half of the victims, are American kids, and that overwhelmingly, the people who are creating this content are people who are close to them and have easy and legitimate access to them.

Mr. POE. Fifty percent.

How does all of this issue relate to human trafficking? Can you describe how human trafficking fits into this issue? Are we dealing with the same type of people? Or are we dealing with two different organizations? Explain that to me.

Mr. ALLEN. There are differences and there are similarities. The differences are that, as you know, we are now in the eighth year of a partnership with FBI and the Justice Department called Innocence Lost, attacking the trafficking of children for sexual purposes within the United States.

I have rescued 1,600 kids, 700 successful prosecutions. What we have found is that while pornography is an element of the operators transaction, the vast majority of those kids initially leave home as runaways, as runaways or homeless kids. So these are not kids who were snatched off the streets, by and large.

With child pornography, what we are seeing is that the vast majority of the victims are kids who are—to whom the offender already has legitimate access and control. Many of the perpetrators are their parents or other family members or neighbors or coaches or friends.

So overwhelmingly, these victims already have a hurdle in that they are very reluctant to tell, because the perpetrator is somebody trusted, who is in their lives already.

So they are different, but it there is also an overlap.

Mr. POE. Sheriff, how many cases do you have ongoing right now, child pornography cases?

Mr. BROWN. Child pornography, well, the ICAC task force working with, we have 67 other affiliated agencies throughout southern Virginia, western Virginia and eastern Virginia, and probably the caseload now is several hundred.

Mr. POE. How about the Sheriffs' Association? Do you know, based upon your leadership of the Sheriffs' Association?

Mr. BROWN. No, sir, I do not.

Mr. POE. Mr. Rotenberg, Mr. Conyers talked about other access, other criminal penalties, or other criminal situations. By preserving the 18-month rule, do you see any issue involved in also civil litigation, where some lawyer on one side or the other of a divorce is going to want to subpoena that information as well, because it is now available would be available for 18 months?

Mr. ROTENBERG. Well, I certainly think it is something that a good attorney would think about, because there is now information available that might be useful in the case or the complaint. So yes, there would be the opportunity for someone to request it.

Mr. POE. Sheriff, you talked about needing more resources. Other than the 18-month retention, what else do you need? Just give me a few. Don't give me a whole list.

Mr. BROWN. I've got a list.

Mr. POE. On this issue, how can we do a better job? Last question, just answer it briefly.

Mr. BROWN. Probably the overriding is the funding for additional personnel in the task forces.

Mr. POE. Thank you.

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

The gentleman from Tennessee, Mr. Cohen?

Mr. COHEN. Thank you, Mr. Chairman.

I have a desire to work with Chairman Smith and Ms. Wasserman Schultz on the bill, because it is a serious issue and it is one that I've worked on in the past.

But I am concerned about the sentencing structure, and I maybe should direct this question to the Chairman. But I have a concern.

First of all the question to Mr. Allen that I think Chairman Smith asked about the mere possession, and the Chairman was answered—the response to his question was that you believe, based on prison data, that 40 percent of the people who view child pornography will engage in at some point. Is that correct?

Mr. ALLEN. Well, I don't want to say 40 percent, because it is very hard to prove.

Mr. COHEN. It is hard to prove. That seemed very high to me, but you said 40.

But the thing is, to make this a higher penalty, and even from your data, which I think is real high, 60 percent of the people would not have engaged and they are being punished more severely because of the 40 percent. It seems like in our system, where you let one guilty person go or 10 guilty people or that one innocent person be convicted or whatever. It seems like that—those figures are damning to the idea of mere possession folks getting these sentences.

Mr. ALLEN. First, Mr. Cohen, we are not arguing for sentence disparity. We recognize in the existing sentence structure, distribution is more serious than possession, production is more serious than just distribution.

Our argument is that there is a tendency in this country today to trivialize and minimize the possession of child pornography. "Oh, well, he just looked at the pictures." Our argument is that possession, in and of itself, is a serious crime. It is not victimless crime.

These are crime scene photos. These are images of the sexual abuse.

Mr. COHEN. I understand that. And I agree with you, but I think that there is still a level—do anyone of the three of you believe that the sentences should be doubled, as are proposed in this law, even though 71 percent of the judges said they should be lessened? Anyone of you think they should be doubled? And I want you to tell me how you think that is going to be an effective deterrent.

Mr. ROTENBERG. We have no position on that issue.

Mr. COHEN. Sheriff?

Mr. BROWN. The Sheriffs' Association—I, personally, I don't believe it needs to be doubled. We need to get judges—all due respect; well, he just left—we need to get them to impose the sentences as are directed to them. We have so many judges that they really don't understand is what is happening to children around this country in this arena.

So, no, I would not say that they need to be doubled, but I would just like to see the judges give them what is due.

Mr. COHEN. Well, I would hope that the Chairman would look at that in this bill.

You know, generally, the Sentencing Commission does this and not the Congress. And the sentencing has gone on 1,500 percent since 1990 or something. Judges have indicated they feel the guidelines are already too high and an increased maximum sentence, such as in section 10, is not being requested. Seventy-one percent of judges to 70 percent in all these areas felt that they shouldn't be increased. And I think that is just a mistake.

I have a friend, not that good of a friend, but I knew him in elementary school and I have known him since. He was an attorney in Memphis, and he was convicted of having child pornography on his computer. He got the 5-year sentence.

And while what he did was wrong, no question about it, I think there could have been alternative ways to handle his crime. And there was no proof or no suggestion that he ever tried to do anything with any children. He just had something on his—and he probably had some type of familial—that is a whole other story, because he had a brother who had some problems and something else.

But regardless, the penalty just seemed too high. And I can see where he should have gone to prison, but not necessarily for 5 years. And our justice system can't afford to put everybody away unless there is some nexus between the time and the deterrent effect, and I don't know that it was here.

So, Mr. Chairman, if you would look at it, we can talk about that. I would like to help you with the bill, but I don't think that we just doubling the sentences—I mean, it looks great. It sounds good. Does no good.

And it really hurts the budget, and it would be better to take the money that would otherwise cost to incarcerate these people and give the personnel to Sheriff Brown to convict the perpetrators.

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

Mr. SENSENBRENNER. The gentleman from California, Mr. Lungren?

Mr. LUNGREN. Thank you very much.

And I want to publicly thank the Chairman for coming out to my district when we had a hearing, or a briefing on the question of

human trafficking, in particular with respect to child trafficking. It surprises people to know that a lot of it is homegrown. I am sorry to say my own area of Sacramento, at least under FBI's statistics, is one of the top five areas in the country for this, and that there does appear to be a nexus between trafficking in children, trafficking in young women, and computer images of child pornography.

Just this week we had a man in Sacramento pleading guilty to sex trafficking in minors, and his two defendants are charged with possession and production of child pornography.

About 3 weeks ago, child porn was found on a Folsom man's lost cell phone, which depicted obscene material with children under 14. That same week, two brothers in Roseville, which is just outside my district, pleaded guilty to child pornography charges with respect to those found on their computers.

I can go on and on and just show you page after page after page. An 86-year-old man in Oroville previously convicted of sexually molesting minors pled guilty to conspiracy to possess child pornography, which was found on his computer.

There is a problem. I think we all recognize.

And, Mr. Rotenberg, you recognized it as well. Some of your concerns, it seems to me, are generic in that, at least as I understand your testimony, some problem with retention of these IP files for any period of time. I mean, the fact of the matter is they are retained for some period of time depending on the company.

What this bill says, which is a bipartisan bill, which is similar to the bill that I introduced last Congress with Chet Edwards, simply says it requires you to retain this data for at least 18 months. So what we are doing is retaining data that if it is in existence, is available to law enforcement under the circumstances articulated here.

So I guess my question, Mr. Rotenberg, is, is there a problem that you have with the access to this information by law enforcement in any event, or that the extension of time for which they are required to hold this information allows the potential for abuses in other circumstances?

Mr. ROTENBERG. My concern, Mr. Lungren, is with a government mandate that requires communication providers to keep information they wouldn't otherwise keep.

And I want to say also, you know, I have been involved with this law since before its enactment, and I have seen all the various issues that have been raised over the years. And as you say on a bipartisan basis, I think the Members of the Congress have been able to make adjustments to the law over time to deal with exigency, for example. If you can't get a warrant or you need backups or you become aware through the good work of Mr. Allen's organization that there may be particular problems, I think those techniques have developed over time in response to the concerns you have.

But this would be crossing a line. Because up to this moment, in the 25-year history of the Electronic Communications Privacy Act, there has never been a government mandate that says to ISPs, you must keep this data on all of your customers. And that is the basis of my——

Mr. LUNGREN. So that is the crossing of the line? The fact that we require them to keep information that they otherwise had with respect to regular business proceedings, but no longer need them because of the nature of those business proceedings?

Mr. ROTENBERG. They may or may not keep it. I mean, you have, for example, an 18-month requirement——

Mr. LUNGREN. Right.

Mr. ROTENBERG. I understand the current practice in the industry, you know, is somewhere between 6 and 12 months, maybe some are a bit below, maybe some are a bit——

Mr. LUNGREN. But that is what our bill provides, that it be 18 months. So why is that essentially different in nature, in terms of the action, the activity of the business and the activity of law enforcement when they have a reason to believe they would like to get this data?

Mr. ROTENBERG. It is truly a very different view of wiretap law, because up to this point in time, the general approach has been to say, we will come to you when we have some reason to believe that one of your customers is doing something wrong.

Mr. LUNGREN. Well, that is exactly what they are doing here. All they are saying is they want to make sure that the data has been retained.

Mr. ROTENBERG. No, because the way data retention works, and the distinction between data retention and the current data preservation, is data retention says at the outset you are going to keep this information on everybody because we don't know at this point in time——

Mr. LUNGREN. You are keeping information on everybody, but they are not making a request for everybody. They are coming to you with a request based on some information they have about a crime having been committed, allegedly.

Mr. ROTENBERG. Yes, so there are at least two concerns there, and this goes to the second part of your question.

The two concerns are, one, everybody, and I do mean everybody, now is looking more closely data minimization techniques, because they are realizing just how difficult it is to safeguard the information they are storing.

Mr. LUNGREN. So when you are talking about data minimization, you are talking about cutting down on the amount of information they store as opposed to criminal minimization, which we use in the——

Mr. ROTENBERG. That's correct, and that is——

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

The gentleman from Pennsylvania, Mr. Marino?

Mr. MARINO. Thank you, Chairman.

Gentlemen, thank you for being here. Mr. Allen and Sheriff, I want to thank you for your work.

I want to preface my comments and my question a little bit. I was a prosecutor for 18 years. I was a district attorney for 12 years. And I was a U.S. Attorney for 6 years. And I personally prosecuted these types of cases.

And the overwhelming factor is there is a plethora, an overabundance of this type of abuse taking place here in the United States, and it is growing. In my office, the Middle District of Pennsylvania,

it was very successful in prosecuting a sex trafficking case involving individuals over the age of 18 but below the age of 18 as well. And many, many people went to prison for a very long time.

And one of the impetuses, one of the driving factors was going back through and checking phone records, going back through and checking computer records, and capturing these images.

And unfortunately, I have had the opportunity in several cases to sit down and talk with 7- and 8- and 10-year-olds who have been exposed to this and have been photographed.

And, Mr. Rotenberg, with all due respect, and I certainly respect your opinion and your privacy issues, but I don't know if you have had the opportunity to sit down and talk to these children that have been abused, because in many situations, they are threatened. Many times it is from a person they now who is sexually abusing them and taking these photos.

And it is by accident in many cases that this information comes to fruition to another adult, or actually, to another child who goes home and tells their parents what their friends just explained to them.

And I am failing to see the concern that you have over an 18-month period, because in many of the cases that I have been exposed to and actually prosecuted, we hit stumbling blocks because some providers eliminated in 6 weeks, some providers emanated in 3 months. And many times, the child does not bring this information to somebody until a year or more later.

And if it is limited to the sexual pornography on children, and if it is limited to access in law enforcement, forgetting the argument for a moment that it is a mandate that never existed—we in law enforcement always are finding new techniques in finding perpetrators. Simply because there has never been a mandate out there, I don't understand your justification as to opposing this 18-month period.

Would you care to help enlighten me again on this?

Mr. ROTENBERG. Mr. Marino, there is absolutely no dispute about the severity of the crime or the need to prosecute effectively. But it would seem to me, and certainly listening to the statements of the other witnesses and the Members of the Committee, if that is the goal, you would began by giving resources to law enforcement so they can sift through the enormous amount of data they have. In this bill, you would extend coverage to providers of wireless services, which will become the obvious place that people will go that that you are concerned about getting after. And you would try to focus the investigations at the outset at exactly the kinds of perpetrators you are concerned about.

Data retention doesn't focus resources on the problem. It says, in effect, we just don't know what we are going to confront. We confront everything.

Mr. MARINO. But you have to realize that data retention in situations like this is critical, so as much as I would like to see the sheriff have 100 more individuals working on this, without the data retention, it is going to be futile, because data retention is critical.

I mean, I have seen too many children, I have been in hospitals with too many children and talked to them and then have them testify, to not take the step into retaining this information.

With all due respect, I really suggest that if you have the opportunity, you do more research in the area of what this is doing to these children, what they are put through, and the pathetic, the sick people that are out there exposing this. And we have to start by making it—I believe that we should double the punishment, from what I have seen and the kids that I have worked with, because nothing is going to get their lives back to what it should be as a 6-, 7-, 8-, 10-year-old.

I have seen situations where 3-month-olds have been exposed and sexually abused.

I commend you gentlemen for what you are doing.

And, Mr. Rotenberg, I respect your position, but this is a situation where I can't find any defense in not increasing this 18-month period.

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

The Chair will yield himself the final 5 minutes for questioning.

First of all, let me say that I am concerned that this bill and the data retention will allow law enforcement to use it far beyond investigating child pornography.

Let me ask you, Sheriff Brown, do you think that you need data detention for crimes other than child pornography crimes?

Mr. BROWN. Personally, no, on a local level. Again, as I have indicated, I am here for ICACs and National Sheriffs on the data retention.

I am more interested, again, the 18 months—and I think I speak for every ICAC and every department that has a cyber-unit that is doing this work, we just need a standard, a uniformed amount of time. I mean, 30 days is not enough. I don't think 6 months is. Eighteen months? I don't know. That is up to you distinguished gentlemen and women of Congress to decide.

But we would like to see a standard. Right now, there is no standard. We will go to one and it is a couple of weeks, the mom-and-pop ISP. Others it is a month. Some, I think the person to my left here is saying some are 6 months, 6 months to maybe 12 months. I don't know of any that are 12 months. It may be; I am not aware.

But I would like to see, and we would like to see, a standard.

Mr. SENSENBRENNER. Okay. I am looking at the subpoena authority in section 7, and it says the administrative subpoenas issued in accordance with the existing laws solely for the purpose of investigating unregistered sex offenders, as defined by another section of the statute, and that is amended and section 11.

From the ISP address, how do you know whether someone is a registered or unregistered sex offender, Mr. Allen?

Mr. ALLEN. Well, the premises of this is that the vast majority of these cases, 95 percent of the cases in which the Marshals are able to locate fugitive sex offenders is through communication data. Most of that as reported to us by the Marshals Service is Internet-based data.

Currently, they are required to get—what is it called?—an All Writs Act order. They go to the U.S. Attorney. The U.S. Attorney initiates a process. Typically, it takes 2 months. Two months is a lifetime when you are trying to track down a fugitive.

And again, the very nature of the fact that the offender is a fugitive means that there has been judicial review. There is a warrant for his apprehension.

So you know, the argument here is that giving them the subpoena authority enables them with the same kind of access that the FBI has, but enables them to circumvent the All Writs Act process, and be able to identify that information, obtain that information constantly.

Mr. SENSENBRENNER. Well, if most of these people are fugitives and the FBI is on the lookout for them, why does the Marshals Service need an additional administrative subpoena authority?

Mr. ALLEN. Well, because the reality, Mr. Chairman, is that it is the Marshals who are in the fugitive business. It is the Marshals who are the primary trackers and locators of criminal fugitives in this country, and particularly as it relates to sex offenders. It is the Marshals who are tasked by Congress with playing that role, in the Adam Walsh Act.

So again, our view on this——

Mr. SENSENBRENNER. Well, we will look at that in a few weeks, so it is——

Mr. ALLEN. I understand.

No, our view is that this is an essential tool needed to carry out the role that you have given them.

Mr. SENSENBRENNER. Well, you know, let me say that I have always felt negatively about administrative subpoenas. You know, I think that if you want a subpoena, it should be a judicial subpoena, because at least that way you have somebody outside of law enforcement reviewing whether this—or having the possibility of reviewing whether the subpoena should be issued.

I fought to keep administrative subpoena authority out of the Patriot Act, and I was successful on that. And what does law enforcement do? They use an existing administrative subpoena law called National Security Letters basically to get around the fact that they didn't have administrative subpoena authority as they asked for.

This is my concern, is that the administrative subpoenas given to the Marshals Service on this is going end up being used for fishing expeditions like the FBI did with National Security Letters on the Patriot Act.

And that is a concern that I think you should share, Mr. Allen, because if you don't share it, you are going to see this law being trashed just like the Patriot Act was, because law enforcement used nonjudicial review authority to be able to grab some evidence that may or may not involve an unregistered sex offender.

I think my time is up. I have spoken my piece on this.

I would like to thank the witnesses for coming today. This bill needs a lot of fixing up. It is not ready for prime time.

The gentleman from Virginia?

Mr. SCOTT. I ask unanimous consent that a letter from Full Channel showing the impact on small providers be entered into the record.

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

LEVI C. MAAIA
VICE PRESIDENT

57 EVERETT STREET
WARREN, RHODE ISLAND 02885
PHONE. 401.247.2250 FAX. 401.247.0191

July 8, 2011

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Washington, D.C.

Re: H.R. 1981 - Protecting Children From Internet Pornographers Act of 2011

To The Honorable Members of Congress:

I would like to take this opportunity to submit my thoughts and concerns on H.R. 1981, Protecting Children from Internet Pornographers Act of 2011. I was contacted by committee staff on this matter so that I could provide the perspective of a small, family-run, cable business as my family runs Full Channel here in Rhode Island. Full Channel was started in 1965 by my grandfather John Donofrio. His vision for an expansive landscape of information delivered to the living rooms and fingertips of ordinary Americans was groundbreaking. In 1982, after nearly 20 years of preparations and government hearings, he was the only individual businessperson to be awarded a cable television franchise in the State of Rhode Island. By the turn of the millennium, Full Channel remained as the only independent cable and broadband provider in the state and continues to serve the local needs of its three communities, employing local residents and supporting schools, charities and local governments.

Today Full Channel remains a valued local provider, serving homes and businesses in Bristol County, Rhode Island, by delivering digital television, broadband Internet and phone services. The company employs more than 20 local residents as sales and service representatives, technicians and engineers. Public access personnel deliver municipal government meetings, community events and other public service programming through Full Channel's three local television channels allocated to the communities. In 2009 the company was lauded as a "Top Operator" by the industry trade publication *CableFAX*. This summer, the Town of Bristol's council chairman thanked Full Channel in a written statement for bringing "greater transparency to government" by delivering local meetings to the TV sets of residents.

To be perfectly clear, I personally, and Full Channel as an organization, are champions of protecting children from all forms of abuse and exploitation, and we support the very reasonable ideals of H.R. 1981. There is no doubt that protecting our children online continues to provide a challenge in every family, and it is timely and appropriate

for Congress to consider what role the Federal government can play in that effort. However, I have serious doubts about the proposed language in that it may open a wide door to conducting electronic surveillance on every Internet-subscribing American citizen in a manner that is redundant to other statutory requirements such as the Communications Assistance for Law Enforcement Act (CALEA), may prove too costly to small businesses implement and may expand the data that companies are compiling in ways that go beyond child pornography and really touches upon broader privacy issues.

H.R. 1981 is a bill aimed at the distribution of child pornography, a sin that is on the short list of the most heinous offenses in our modern society. Intelligent, well-respected individuals may argue the merits and dangers of gun control, net neutrality, same-sex marriage and even abortion and come out unscathed relative to a witness emerging from a testimony even remotely tainted by the topic of the exploitation of children.

In 2007, Full Channel and the rest of the nation's Internet service providers began to implement CALEA, which codified the implementation of modern day digital wiretapping. CALEA gives Federal and local law enforcement protocols for the speedy access to live data from a suspect's digital connections with proper court documentation (i.e., a warrant or subpoena). When a provider is subpoenaed by a law enforcement agency to retain electronic records under CALEA they must comply.

The systems to support CALEA were expensive for small companies like Full Channel to implement; however, they have functioned seamlessly when called into action. Since its inception, Full Channel has had very few requests for information relating to crimes against children. Using these existing CALEA protocols, our staff is able to quickly respond to a subpoena and provide data. However, these instances are clearly infrequent. Adding a new statutory obligation for small businesses that will result in new costs doesn't seem merited with this in mind. I am not sure where the "problem" with existing data collection and wiretapping law exists.

With that in mind, it concerns me that this bill asks that we collect our customers' historical personally identifiable information for 18 months on the remote chance that they may have engaged in the transfer or distribution of child pornography. This seems to be an impingement on the privacy of everyday citizens.

Furthermore, H.R. 1981 discriminates between service providers, applying to those who deliver communications services via landline, but not to those who do so wirelessly, leaving gaping holes in this new so-called "security" system. In fact, the bill provides a full exemption from the data retention requirements for wireless providers like cellular giants AT&T Mobility and Verizon Wireless, publically-accessible WiFi hotspots (i.e., Starbucks, college campuses and libraries) and new WiMax installations popping up throughout the U.S. If all of the nation's providers – wireline and wireless alike – are not held to the same standard of data retention, the burden borne by small companies like

Full Channel to implement these systems will be in vane because criminal predators will easily connect to nearby cellular data networks or a neighboring resident's or business' open WiFi connection, which are all exempt from the proposed requirements.

The few brief lines in H.R. 1981 that address digital communications not only serve to create gaping holes in the bill's objective, but also serve to create a competitively unfair environment where landline providers, especially small businesses like Full Channel, are at a distinct economic disadvantage by being held to a higher standard than wireless providers. In an era when the federal government is scrambling to repurpose much of the citizens' wireless spectrum for the deployment of wireless broadband, it only seems prudent to hold traditional landline and wireless broadband providers to the same level of accountability and responsibility. To do otherwise hurts small business and will have a chilling effect on the deployment and expansion of broadband, especially in underserved and rural areas. By forcing only landline providers like Full Channel to shoulder these new regulatory burdens, it is effectively a regressive tax. This tax may be spread across millions of subscribers in larger organizations; however, small businesses like Full Channel will be hit especially hard by these financial constraints, with the profound effect of having to pass along the government implemented costs to consumers.

I urge the committee to reconsider the data retention requirements in H.R. 1981 because they are inequitable and ineffective on a number of fronts. The tools to apprehend predators are already in the hands of law enforcement under CALEA. I would argue that more resources should be devoted directly to the men and women of law enforcement dedicated to protecting children, rather than on the implementation of carte blanche data collection on the entire population of American landline Internet users.

Respectfully submitted,

Levi C. Maaia
Vice President
Full Channel TV, Inc.

LCM/

Mr. SMITH. Mr. Chairman?

Mr. SENSENBRENNER. The gentleman from Texas?

Mr. SMITH. I ask unanimous consent that a statement prepared by Congresswoman Debbie Wasserman Schultz,* the lead Democratic cosponsor of H.R. 1981, as well as letters in support of H.R. 1981 from the National Sheriffs' Association and the International Union of Police Associations be made a part of the record.

Mr. SENSENBRENNER. Well, I am glad that the gentleman from Texas is putting things in the record from the Chair of the Democratic National Committee, and without objection we will put that in the record. [Laughter.]

[The information referred to follows:]

*Prior to the printing of this hearing, a decision was made not to include the referenced material.

NATIONAL SHERIFFS' ASSOCIATION

May 26, 2011

The Honorable Lamar Smith
United States House of Representatives
Washington, D.C. 20515

The Honorable Debbie Wasserman Schultz
United States House of Representatives
Washington, D.C. 20515

Dear Congressman Smith and Congresswoman Wasserman Schultz:

On behalf of the National Sheriffs' Association (NSA) and the 3,083 elected sheriffs nationwide, I am writing to express our strong support for H.R. 1981 - the Protecting Children From Internet Pornographers Act of 2011.

The expansion and development of technology has enabled child pornography to become a worldwide epidemic. Child predators have become adept in exploiting their perversion and hiding behind the anonymity of the Internet, making it difficult for law enforcement to identify these predators. As such, unmasking child pornographers on the Internet is a painstaking and complex process for law enforcement officers and typically requires assistance from Internet Service Providers (ISP) to accurately identify the perpetrator. However, some ISPs only retain their clients' records for a short period of time, thereby hindering law enforcement's ability to identify predators when they come across child pornography.

Through the Protecting Children From Internet Pornographers Act of 2011, ISPs will be required to retain the addresses assigned to customers for 18 months. This provision will ensure that when law enforcement contacts an ISP looking for a child predator, the identifying information will still exist. Additionally, the legislation provides legal protections for ISP to further facilitate cooperation with law enforcement and help ease concerns that the ISP could be held civilly liable for sharing customer information with law enforcement during valid investigations.

H.R. 1981 also creates a new federal offense for individuals who profit from child pornography; significantly enhances penalties for possession of child pornography; provides administrative subpoena authority to the U.S. Marshals to access critical travel information and records on fugitive sex offenders; and strengthens the protections for child witnesses and victims.

As sheriffs, it is our responsibility to protect society's most vulnerable – our nation's children – from the evils of the world. Child pornography is one such evil. The provisions within H.R. 1981 provides law enforcement officers the capabilities necessary to combat child predators and child pornography. The National Sheriffs' Association strongly supports the Protection Children From Internet Pornographers Act of 2011 (H.R. 1981) and looks forward to working with you to secure passage of this critical legislation.

Sincerely,

Sheriff B.J. Roberts
President

Aaron D. Kennard, Sheriff (ret.)
Executive Director

1450 Duke St. • Alexandria, VA 22314 • 703.836.7827 phone • 703.683.6541 fax • www.sheriffs.org • nsumail@sheriffs.org

INTERNATIONAL UNION OF POLICE ASSOCIATIONS AFL-CIO

THE ONLY UNION FOR LAW ENFORCEMENT OFFICERS

SAM A. CABRAL
International President

DENNIS J. SLOCUMB
International Executive Vice President, Legislative Affairs

TIMOTHY A. SCOTT
International Secretary-Treasurer

June 16, 2011

The Honorable Lamar Smith
United States House of Representatives
Washington, D.C. 20515

Dear Congressman Smith:

On behalf of the International Union of Police Associations, AFL-CIO, I am proud to endorse your legislation, H.R. 1981, the **"Protecting Children From Internet Pornographers Act of 2011."**

We all are aware that the exploitation and victimization of children is a very serious criminal matter, both here and in other nations. Your proposed legislation would help law enforcement cope with this problem by criminalizing financial transactions that would facilitate access to, or possession of, child pornography.

This is another tool you will have provided to combat this horrible misuse of our most vulnerable and treasured citizens.

I look forward to working with you and your staff to bring this legislation forward.

Very Respectfully,

Dennis Slocumb
International Vice-President

International Headquarters • 1549 Ringling Blvd • 6TH Floor • Sarasota, Florida 34236-6772 • (941) 487-2560 • Fax: (941) 487-2570
Legislative Affairs Office • Washington, DC

Mr. SENSENBRENNER. Without objection, the Committee stands adjourned.

[Whereupon, at 11:32 a.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Subcommittee on Crime, Terrorism, and Homeland Security

First, I would like to thank Chairman Sensenbrenner and Ranking Member Scott for holding today's hearing on H.R. 1981, the "Protecting Children from Internet Pornographers Act of 2011."

I would also like the thank today's witnesses for taking time out of their schedule to share their expertise with us:

- **Mr. Ernie Allen**, President and CEO, National Center for Missing and Exploited Children
- **Sheriff Michael J. Brown**, Bedford County Sheriff's Office
- **Mr. Marc Rotenberg**, President, Electronic Privacy Information Center

H.R. 1981, the "Protecting Children from Internet Pornographers Act," focuses on sex offenses against children and includes, amongst other things, a mandate that internet service providers (ISPs) retain data for a period of 18 months, and directives to the United States Sentencing Commission to severely increase penalties for certain sex offenses.

Resolving this issue of data retention has been identified as critical for assisting federal law enforcement in online child pornography and child exploitation investigations. However, at crux of this issue is determining a balance between the necessary amount of data retention which would best serve law enforcement, the impact of added retention costs on providers, and the looming privacy concerns of the majority of law abiding Internet users.

To be sure, the issues regarding child pornography, child trafficking, and other internet crimes that may involve young people are of great concern to me. As Chairwoman of the Congressional Children's Caucus, I have focused a lot of energy on ways to combat these types of crimes. Furthermore, during the 111th Congress, this subcommittee, under the direction of then Chairman Bobby Scott, examined multiple law enforcement methods for effectively addressing these types of crimes. In January of this year, an additional hearing was held to examine data retention and its utility for prosecuting Internet crimes.

From those hearings and from many experts in this field, we are constantly hearing that one of the keys to combating these types of Internet crimes against children is access to information in a coordinated and organized manner. There are numerous organizations and tasks forces, such as the Internet Crime Complaint Center (IC3), the Innocent Images National Initiative (IINI), and the Internet Crimes Against Children Task Force (ICAC), that are in place to handle Internet crime cases, but it is necessary for there to be a coordinated response with law enforcement in order for these groups to be most effective.

A recent GAO report also points out that the biggest contributing factor to the slowed pace of child pornography and exploitation cases is the backlog of forensic evidence that awaits processing, an issue that can truly only be addressed with additional resources.

Protecting children from Internet pornographers and child exploitation rings is not a partisan issue. Both Democrats and Republicans alike would agree, as demonstrated by the bipartisan efforts to draft H.R. 1981, that something must be done to ensure that our system of protecting our children against Internet predators is a strong and effective tool. No one wants to see another child fall victim to an Internet savvy predator or trafficker. Attorney General Eric Holder has been quoted as saying that, "*certain data* must be retained by ISPs for *reasonable periods* of time

so that it can be accessible to law enforcement." I, and many of my colleagues I presume, agree wholeheartedly with the Attorney General's words.

Law Enforcement Needs:

Yes, there needs to be a consistent data retention standard in place for Internet Service Providers in order to better aide law enforcement. However, we can not ignore the issues and questions raised by the idea of data retention, especially when the standard being proposed is so broad.

H.R. 1981 proposes a retention period of 18 months, a number based on an antiquated FCC regulation that governs tolled telephone records. This amount of retention time may be unduly burdensome on some ISP's, especially those smaller regional entities. It may also lead to other issues which this bill does not address, such as privacy concerns, storage requirements, and the possibility of outsourcing of data storage to foreign entities.

Although current law requires ISP's to retain records at the request of law enforcement for at least 90 days, the current industry-wide norms go farther. According to the National Cable and Telecommunication Association, the industry norm for data retention is 6-months. In a spirit of cooperation and an effort to aide law enforcement, they would be willing to increase their data retention standard to one-year. Though there are industry norms, there is still a lot of inconsistency amongst ISPs regarding their data retention practices. For instance, AOL stores data for 7 days, which Comcast stores data for 2 years. It is imperative that a consistent industry standard be implemented, either by the industry itself or by Congress, that takes into account the aforementioned concerns.

Storage is Costly:

In the past, there have been legislative proposals that would require ISPs to retain data for all of their customers for at least 2 years—an amount of time thought to be excessive. H.R. 1981 proposes an 108-month retention period. While the idea of an 18-month data retention requirement may help to solve the problem for law enforcement if organized properly, it may also trigger some other problems to arise as well, especially for the ISPs.

Storage of such voluminous amounts of information can be extremely costly. Moreover, organization of so many terabytes of data so that it can be effectively utilized can also be very costly. For a large national ISP, absorbing these costs may not be too difficult, although I'd assume such costs would be trickled down to consumers, resulting in higher rates experienced by end users. However, for smaller ISPs, those who are regional, local or minority owned, such costs could impose hardships on their ability to compete. Furthermore, these smaller ISP's may be forced to outsource the data retention practices to a third party, which raises another concern about the protection and privacy of such information.

Privacy Concerns:

To be sure, the data retained by ISPs would contain some rather personal information of their customers. The Internet is a huge part of most people's lives, and majority of Internet users are law abiding citizens who are using the Internet in lawful ways. Storing a history of people's day-to-day online activity could certainly impose upon a person's right to privacy. Therefore, if we are to impose a data retention requirement on ISPs, we must consider the privacy concerns of users, and furthermore, how the information will be secured and protected.

Unfortunately, H.R. 1981 does not address this issue, and relies on standards already in place at the industry level. While the industry may have standards in place to govern privacy concerns, I am hesitant to support legislation which requires the retention of such private and personal information without putting necessary privacy safeguards in place.

We should be concerned about who would be handling this information and who would have access to it—both internally at ISPs and within law enforcement agencies and child Internet crime task forces and organizations. Also, we should be considering who would be liable for the privacy invasion and violation if there is ever a breach of security, or if data bases of retained information are hacked.

Lastly, we should be concerned about where the information is retained—will it be retained physically on a server? Virtually in a cloud? What happens if an ISP decides to outsource the retention services to a third party, or even more concerning, a foreign entity. These are all concerns that I believe legislation requiring the retention of personal information should address.

Despite the fact that many of these issues were raised in the January hearing held on this subject, there was still a failure to address them in this legislative proposal. It is imperative that we come to a solution that balances the needs of the law enforcement community and the privacy rights of consumers. As Chairwoman

of the Congressional Children's caucus, and a member representing the border state of Texas where child sex trafficking and exploitation is rampant, I firmly believe that something must be done to aide law enforcement efforts in combating these crimes. However, it must be done responsibly.

I look forward to working with my colleagues on both sides of the aisle to find an effective and efficient solution that will ensure the safety of children as the use the Internet, and that will effectively help law enforcement prevent the trafficking of child pornography. We can not afford to allow more children to become victims.

Again, I would like to thank the Chairman and Ranking Member for holding this hearing, and thank the witnesses for their testimony.

Major County Sheriffs' Association

1450 Duke Street, Suite 207, Alexandria, Virginia 22314

President
Sheriff Douglas C. Gillespie
Las Vegas Metropolitan Police Department
400 Stewart Ave.
Las Vegas NV 89101-2084
(702) 229-3231
(702) 382-2904 (fax)
dgillespie@lvmpdsheriff.com

Vice President
Sheriff Richard Stanek
Hennepin County Sheriff's Office
350 S. 5th St. Room 6 Courthouse
Minneapolis, MN 55415-1316
612-348-2247
612-348-8208 (fax)
rstanek@hcsheriff.org

Vice President – Government Affairs
Sheriff Michael J. Bouchard
Oakland County Sheriff's Office
1200 North Telegraph – Building 49 East
Pontiac MI 48341
248-858-5001
248-858-1806 (fax)
mbouchard@oakgov.com

Treasurer
Sheriff John Aubrey
Jefferson County Sheriff's Office
531 Court Place Suite 604
Louisville, Kentucky 40202
(502) 574-5400
(502) 574-4185 (fax)
jaubrey@louisville.com

Secretary
Sheriff Al Lamberti
Broward County Sheriff's Office
2601 West Broward Boulevard
Fort Lauderdale, FL 33312
(954) 831-8901
(954) 797-0546 (fax)
alamberti@sheriff.org

Executive Director
Joseph E. Wellinger
482 Pinecrest Drive
Tappahannock VA 22560
(804) 443-9707
(804) 445-0023 (fax)
jwellinger@msdsheriffs.org

Associate Executive Director
Michael Ferrence Jr.
Academy Leadership Associates
701 S. Carolina Street
Fredericksburg VA 22401-5610
540-890-2970
540-890-2970 (fax)
mferrence@msdsheriffs.org

July 12, 2011

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20510

The Honorable Debbie Wasserman Schultz
United States House of Representatives
Washington, DC 20510

Dear Chairman Smith and Representative Wasserman Schultz,

The Major County Sheriffs' Association (MCSA) commends you for introducing H.R. 1981, the Protecting Children from Internet Pornographers Act of 2011. Your legislation would increase public safety by protecting children from exploitation and by enhancing the ability of law enforcement to track down individuals that perpetuate this disturbing activity.

The proliferation of electronic data has made it increasingly challenging for law enforcement to investigate and identify perpetrators of child exploitation and sellers or distributors of online child pornography. The requirement in H.R. 1981 for Internet Service Providers to preserve certain data for up to 18 months will improve law enforcement's ability to investigate leads and take these criminals offline.

Additionally, making it a crime to conduct any financial transaction knowing it will lead to accessing child pornography will be a powerful prevention mechanism that will make it less appealing for purveyors of this material. It will also prevent additional harm from being done to victims of exploitation.

Your leadership in cracking down on child sex predators and expanding protections for minor victims and witnesses is greatly appreciated by the members of our association. In addition, we truly appreciate your understanding of the growing challenges law enforcement organizations face in accessing electronic evidence necessary to investigate and prosecute crimes.

The MCSA represents the interests of elected sheriffs in counties with a population of at least 500,000, totaling over 100 million Americans. We look forward to working with you to advance the Protecting Children from Internet Pornographers Act and to preserve law enforcement's ability to conduct timely and effective investigations.

Sincerely,

Douglas C. Gillespie, Sheriff

NATIONAL
FRATERNAL ORDER OF POLICE®

328 MASSACHUSETTS AVE., N.E.
WASHINGTON, DC 20002
PHONE 202-547-8189 • FAX 202-547-8190

CHUCK CANTERBURY
NATIONAL PRESIDENT

JAMES O. PASCO, JR.
EXECUTIVE DIRECTOR

The Honorable Lamar S. Smith
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

25 July 2011

Dear Mr. Chairman,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our support for H.R. 1981, the "Protecting Children from Internet Pornographers Act," which is scheduled to be considered by your Committee this week.

Trafficking in child pornography generates billions of dollars every year to criminals who conduct their business over the Internet. This legislation will greatly improve the ability of law enforcement to combat trafficking in child pornography by providing a penalty of up to ten years imprisonment for anyone who knowingly conducts a financial transaction to facilitate any access by any person to child pornography.

The bill also provides a critical tool for assisting Federal law enforcement officers conducting online child pornography and child exploitation investigations by requiring Internet Service Providers (ISPs) to retain for 18 months Internet Protocol (IP) addresses it assigns to customer accounts. In many of these investigations, the only means by which an owner or user of a child pornography website can be identified is his IP address. Under current law, law enforcement officers can subpoena the name and address of the user of the IP address from the ISP. However, ISPs regularly purge these records, making it difficult, if not impossible, for law enforcement to apprehend the distributors and consumers of child pornography on the Internet. This legislation will enable these investigations to move forward and will have a significant impact in our efforts to combat trafficking in child pornography.

On behalf of the more than 330,000 members of the Fraternal Order of Police, I urge the Committee on the Judiciary to favorably report H.R. 1981 and send it to the House floor. Thank you for your leadership and support on this issue and please do not hesitate to contact me if I can be of any additional help on this or any other issue.

Sincerely,

Chuck Canterbury
National President

—BUILDING ON A PROUD TRADITION—

BOARD OF DIRECTORS

Mark Mandell
Chair

David T. Austern
Vice Chair

Philip M. Gerson
Treasurer

G. Morris Gurley
Secretary

Alexander Auersperg
Patricia Brown
Denise Forte
Sarah Gold
Melvin Hewitt
Ala Isham
Ralph H. Isham
Donald A. Migliori
Frank M. Ochberg, M.D.
Kathleen Flynn Peterson
Stephen Rickman
Charles J. Sgro
Hon. Eric Smith
Francisco Acevedo Villarruel
David M. Zlotnick

EXECUTIVE DIRECTOR
Mai Fernandez

July 26, 2011

Congressman Lamar Smith
Chairman
Committee on the Judiciary
U. S. House of Representatives
Washington, DC 20515

Congressman John Conyers
Ranking Minority Member
Committee on the Judiciary
U. S. House of Representatives
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers:

The National Center for Victims of Crime wishes to express its support for H.R. 1981, the Protecting Children from Internet Pornographers Act of 2011.

While child pornography has been a blight on the public landscape for many decades, the exponential growth of the Internet and the ready availability of digital cameras, pocket video cameras, and cell phone cameras are working to produce a dramatic explosion in such crimes. The Internet Crimes Against Children task forces, a program funded by the Office of Juvenile Justice and Delinquency Prevention, U.S. Department of Justice, estimate a greater than 80 percent increase from 2006 through 2010 in the number of public complaints related to the possession, distribution, and manufacture of child pornography. ("Combating Child Pornography," GAO-11-334.) The harm to victims cannot be underestimated. Not only do child pornography victims suffer the harms of sexual abuse, but they suffer the added impact of living with the knowledge that a record of their abuse is in circulation for the prurient interests of others.

The Protecting Children from Internet Pornographers Act of 2011 will work to reduce roadblocks to the investigation and prosecution of child pornography. It will increase law enforcement's ability to access data held by Internet Service Providers, strengthen the ability to stop the financial transactions facilitating the trade in child pornography, and strengthen our ability to protect child victims and witnesses from intimidation and harassment.

We urge your colleagues to pass this important legislation, to help end the scourge of child pornography.

Sincerely,

Mai Fernandez

2000 M Street, NW • Suite 480 • Washington, DC 20036 • Tel. 202/467-8700 • Fax 202/467-8701 • www.ncvc.org

NNEDV

NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

2001 S STREET, NW
SUITE 400
WASHINGTON, DC 20009

www.nnedv.org

August 19, 2011

Re: HR 1981

Dear Chairman Smith:

On behalf of the National Network to End Domestic Violence (NNEDV), I write in praise of the leadership undertaken by you, and by Congresswoman Wasserman Schultz, to end the horror of child pornography. NNEDV particularly commends you for taking on the challenge of ensuring that our important system of electronic communication operates in a manner that punishes, rather than facilitates, this attack on our children and scourge on our society. Although we support this effort to eradicate child pornography, we are concerned that 18 months exceeds a safe period of time for technological storage of personal data. We are ever mindful of the fact that perpetrators of domestic violence have repeatedly demonstrated unique abilities to adapt technology for inappropriate purposes. For this reason we ask that the bill be amended to substantially shorten the storage period outlined in Section 4 of the bill.

Respectfully,

Paulette Sullivan Moore
Vice President of Public Policy

cc: Congresswoman Wasserman Schultz

November 4, 2011

The Honorable Lamar Smith
Chairman
Judiciary Committee
United States House of Representatives
Washington, D.C. 20515

Dear Representative Smith,

On behalf of Concerned Women for America Legislative Action Committee's 500,000 members nationwide, I would like to thank you for introducing the Stop Online Piracy Act, H.R. 3261. This legislation, along with your Protect Children From Internet Pornography Act, H.R. 1981, will help ensure that American property is protected from theft and our children are safe from exploitation.

The First Amendment to our Constitution allows us the freedom to express ourselves. However, this is not an unfettered right. Courts have limited this right when compelled by public safety concerns. H.R. 3261 protects the most vulnerable among us, our children, from Website operators that seek to evade our laws and peddle child pornography or illegal obscenity.

Twelve percent of all Internet sites are pornography, and 260 sites are added daily. Your legislation is needed to protect our families.

Representative Smith, we commend you for introducing the Stop Online Piracy and Protect Children From Internet Pornography Acts. We appreciate your efforts to prevent property theft and give law enforcement additional tools to keep our families safer.

Sincerely,

Penny Nance
Chief Executive Officer and President
Concerned Women for America Legislative Action Committee

○