

PROTECTING CHILDREN FROM INTERNET
PORNOGRAPHERS ACT OF 2011

NOVEMBER 10, 2011.—Committed to the Committee of the Whole House on the
State of the Union and ordered to be printed

Mr. SMITH of Texas, from the Committee on the Judiciary,
submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 1981]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill
(H.R. 1981) to amend title 18, United States Code, with respect to
child pornography and child exploitation offenses, having consid-
ered the same, report favorably thereon with an amendment and
recommend that the bill as amended do pass.

CONTENTS

	Page
The Amendment	2
Purpose and Summary	5
Background and Need for the Legislation	5
Hearings	21
Committee Consideration	22
Committee Votes	22
Committee Oversight Findings	30
New Budget Authority and Tax Expenditures	30
Congressional Budget Office Cost Estimate	30
Performance Goals and Objectives	32
Advisory on Earmarks	32
Section-by-Section Analysis	32
Changes in Existing Law Made by the Bill, as Reported	35
Dissenting Views	43

The Amendment

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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

“(a) IN GENERAL.—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) EXCLUSION FROM OFFENSE.—This section does not apply to a financial transaction conducted by a person in cooperation with, or with the consent of, any Federal, State, or local law enforcement agency.”

(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”; and

(2) by inserting “1960A (relating to financial facilitation of access to child pornography),” before “section 2113”.

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.—

“(1) A commercial provider of an electronic communication service shall retain for a period of at least one year a log of the temporarily assigned network addresses the provider assigns to a subscriber to or customer of such service that enables the identification of the corresponding customer or subscriber information under subsection (c)(2) of this section.

“(2) Access to a record or information required to be retained under this subsection may not be compelled by any person or other entity that is not a governmental entity.

“(3) The Attorney General shall make a study to determine the costs associated with compliance by providers with the requirement of paragraph (1). Such study shall include an assessment of all the types of costs, including for hardware, software, and personnel that are involved. Not later than 2 years after the date of the enactment of this paragraph, the Attorney General shall report to Congress the results of that study.

“(4) In this subsection—

“(A) the term ‘commercial provider’ means a provider of electronic communication service that offers Internet access capability for a fee to the public or to such classes of users as to be effectively available to the public, regardless of the facilities used; and

“(B) the term ‘Internet’ has the same meaning given that term in section 230(f) of the Communications Act of 1934.”

(b) SENSE OF CONGRESS.—It is the sense of Congress—

(1) to encourage electronic communication service providers to give prompt notice to their customers in the event of a breach of the data retained pursuant to section 2703(h) of title 18 of the United States Code, in order that those effected can take the necessary steps to protect themselves from potential misuse of private information; and

(2) 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.

(c) **TRANSITION RULE.**—The amendment made by this section shall not apply until 180 days after the date of the enactment of this Act to a provider of an electronic communications service that does not, on that date of enactment, have in effect a system of retention of records that complies with the requirements of that amendment.

(d) **STUDY.**—

(1) The Attorney General, not later than 2 years after the date of the enactment of this Act, shall complete a study of providers affected by section 2703(h) of title 18, United States Code.

(2) Such study shall include—

(A) the privacy standards and considerations implemented by those providers as they comply with the requirements of section 2703(h); and

(B) the frequency of any reported breaches of data retained pursuant to section 2703(h).

(3) The Attorney General shall, upon the completion of the study, report the results of the study to Congress.

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,” 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”;

(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)”;

(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 reported to law enforcement as a missing person), or is part of a government-authorized effort to locate a fugitive or person of interest in a criminal, antiterrorism, or national security investigation.”.

SEC. 9. SENTENCING GUIDELINES.

Pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements to ensure—

(1) that the guidelines provide an additional penalty increase above the sentence otherwise applicable in Part J of Chapter 2 of the Guidelines Manual if the defendant was convicted of a violation of section 1591 of title 18, United States Code, or chapters 109A, 109B, 110, or 117 of title 18, United States Code; and

(2) if the offense described in paragraph (1) involved causing or threatening to cause physical injury to a person under 18 years of age, in order to obstruct the administration of justice, an additional penalty increase above the sentence otherwise applicable in Part J of Chapter 2 of 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 not 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
 - (3) in paragraph (10), by striking “paragraph (1)(A)(ii)” and inserting “paragraph (1)(A)(iii)”.

Purpose and Summary

H.R. 1981 provides additional investigative and prosecutorial tools and enhanced penalties to combat the proliferation of Internet child pornography and child exploitation offenses and other Internet-based crimes.

Background and Need for the Legislation

I. THE PROLIFERATION OF CHILD PORNOGRAPHY AND CHILD EXPLOITATION ON THE INTERNET

According to the Justice Department, trafficking of child pornography images was almost completely eradicated in America by the mid-1980’s. Purchasing or trading child pornography images was risky and almost impossible to undertake anonymously.

The advent of the Internet reversed this accomplishment. Internet child pornography is among one of the fastest growing crimes in America, increasing at an average of 150% per year. These disturbing images litter the Internet and pedophiles can purchase, view, or exchange this material with virtual anonymity.

The Department reports that “the expansion of the Internet has led to an explosion in the market for child pornography, making it easier to create, access, and distribute these images of abuse. . . . The child victims are first sexually assaulted in order to produce the vile, and often violent, images. They are then victimized again when these images of their sexual assault are traded over the Internet in massive numbers by like-minded people across the globe.”¹

The National Center for Missing and Exploited Children (NCMEC) created the CyberTipline 13 years ago. To date, more than 51 million child pornography images and videos have been reviewed by the analysts in NCMEC’s Child Victim Identification Program.² As NCMEC’s president and CEO, Ernie Allen, explained at a hearing before the Crime, Terrorism and Homeland Security Subcommittee on July 12, 2011, “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

¹ *The National Strategy for Child Exploitation Prevention and Interdiction, A Report to Congress*, U.S. DEPT. OF JUSTICE, Aug. 2010, available at <http://www.projectsafefchildhood.gov/docs/natstrategyreport.pdf> (hereinafter *National Strategy*).

² *Testimony of Mr. Ernie Allen, President and CEO of the National Center for Missing and Exploited Children*, Hearing on H.R. 1981 before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, 112th Congress, July 12, 2011, at 2.

CyberTipline include images of sexual assault of toddlers and even infants.”³

A recent Federal investigation demonstrates the ease with which pedophiles can exchange pornography via the Internet and the horrific nature of this crime. Operation Delego, initiated by Immigration and Customs Enforcement (ICE) agents, uncovered an international child pornography ring that operated an Internet forum known as “Dreamboard.”⁴ The forum was based in the United States, but had nearly 600 participants who spanned across five continents.

U.S. Attorney General Eric Holder described that “[i]n order to become part of the Dreamboard community, prospective members were required to upload pornography portraying children under 12 years of age or younger Once given access, the participants had to continually upload images of child sexual abuse in order to maintain membership. The more content they provided, the more content they were allowed to access. Members who created and shared images and videos of themselves molesting children received elevated status and greater access. . . . Some of the children featured in these images and videos were just infants and in many cases, the children being victimized were in obvious and also intentional pain, even in distress and crying, just as the rules for one area of the bulletin board mandated. They had to be in distress and crying.”⁵ To date, roughly 100 members of Dreamboard have been arrested in the United States and abroad. Nearly 500 members, including the top administrator of the forum, remain at large and free to continue abusing children.⁶

II. FINANCIAL FACILITATION OF INTERNET CHILD PORNOGRAPHY

Internet child pornography has become a commercial enterprise worth billions of dollars annually.⁷ In April 2007, executives from the online payment service E-Gold were indicted for permitting known child pornographers to use their service to complete illegal money transfers.⁸ The circumstances surrounding the E-Gold indictment typify the reasons why many online payment services, which offer anonymity and lack thorough regulation, are attractive to money launderers and criminals.

Unlike banks, which must follow national and international banking regulations, online payment services bypass compliance rules that require identification of the payer and payee.⁹ For example, individuals using the E-Gold payment system were required to provide only an email address. Account holders were then free to

³*Id.* at 3.

⁴Terry Frieden, *72 charged in online global child porn ring*, CNN, Aug. 3, 2011, available at http://articles.cnn.com/2011-08-03/justice/us.child.porn.ring_1_sexual-abuse-bulletin-board-images-and-videos?_s=PM:CRIME.

⁵*Id.*

⁶Staff Briefing by Officials from U.S. Immigration and Customs Enforcement, U.S. Dept. of Homeland Security, Aug. 16, 2011.

⁷Jelani Jefferson Exum, *Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses*, XVI RICH. J.L. & TECH. 8, p.6 (2010), <http://jolt.richmond.edu/v16i3/article8.pdf>.

⁸*Digital Currency Business E-Gold Indicted For Money Laundering and Illegal Money Transmitting*, U.S. DEPT. OF JUSTICE, Apr. 27, 2007, available at <http://www.justice.gov/criminal/cybercrime/egoldIndict.htm>.

⁹*Trends in Migration, Hosting and Payment for Commercial Child Pornography Websites*, FINANCIAL COALITION AGAINST CHILD PORNOGRAPHY (2008), available at http://www.missingkids.com/en_US/documents/FCACPTechnologyChallengesWhitePaper5-08.pdf.

access their accounts over the Internet and conduct anonymous transactions with parties around the world.¹⁰

E-Gold also seemed to encourage illegal-activity in other ways. The payment service's user agreement did not prohibit criminal activity and E-Gold only assigned one employee to monitor accounts for indications of criminal activity. When the criminal activity of E-Gold users was discovered, E-Gold advised the users to relocate their funds to different E-Gold accounts.¹¹

As traditional credit card and payment services such as MasterCard, Visa, American Express, and Bank of America take steps to "virtually eliminate" their use in child pornography transactions, child pornographers will increasingly rely on online payment systems.¹²

Mr. Allen of NCMEC testified that "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."¹³

In 2006, NCMEC created the Financial Coalition Against Child Pornography. "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."¹⁴ The Coalition's goals are to "increase the risk of running a child pornography enterprise and to eliminate the profitability."¹⁵

H.R. 1981 targets the commercial Internet child pornography industry by establishing a new Federal offense for the financial facilitation of Internet child pornography. The offense makes it a crime punishable by fine or up to 20 years in prison to conduct a financial transaction knowing that it will facilitate access to child pornography. To encourage the continued efforts of NCMEC's Financial Coalition, H.R. 1981 exempts from the new offense those transactions conducted in cooperation with law enforcement agencies.

III. UNIFORM RETENTION OF CERTAIN DATA IS PARAMOUNT TO COMBATING INTERNET CHILD PORNOGRAPHY AND OTHER INTERNET CRIMES.

The Internet has revolutionized modern-day commerce and communications. Individuals can transmit emails in a split second, download movies and TV shows to their computers, or purchase a plane ticket—all thanks to the Internet. The Internet has also revolutionized modern-day crime and crime fighting. Today, the Internet is used to facilitate a myriad of criminal enterprises, including

¹⁰ See *supra* note 8.

¹¹ Brian Krebs, *U.S.: Online Payment Network Abetted Fraud, Child Pornography*, WASH. POST, May 01, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/01/AR2007050101291_pf.html.

¹² Ernie Allen, *In Child Pornography, Fight Harder*, CHRISTIAN SCI. MONITOR, Nov. 26, 2007, available at <http://www.csmonitor.com/2007/1126/p09s01-coop.html>.

¹³ *Supra* note 2 at 3.

¹⁴ *Id.* at 4.

¹⁵ *Id.*

drug trafficking, terrorism, cybercrime, fraud, human trafficking, and child pornography and exploitation.

America's communication systems are, for the most part, privately owned and operated. Telecommunications companies own and maintain the vast fiber optic, cable, and satellite networks that facilitate all landline and cellular telephone calls—including Voice over Internet Protocols (VOIP), email, instant messaging, chat rooms, bulletin boards, and the ever-expanding Internet. As a result, law enforcement agents are dependent upon these companies to store certain customer and transmission information and, when appropriate, disclose it to investigators.

The Internet is an ideal place to engage in criminal activity. It allows for almost instantaneous transmission of information and affords criminals a great deal of anonymity. The old days of police officers patrolling the streets are, to a great extent, gone. Now, law enforcement officials must patrol the Internet for crime.

When investigators encounter criminal activity on the Internet, such as a website peddling pain killers without a prescription or a chat room for pedophiles to exchange child pornography images, they are often unable to identify the perpetrators. Criminals use fake email addresses or log in names to disguise their true identities. What investigators do find is a numerical code, known as an Internet Protocol (IP) address, which is assigned to the person by an Internet provider as a way of connecting them to the Internet or transmitting their emails.

Often the only mechanism for identifying criminals on the Internet is for investigators to trace the IP address back to the Internet provider, who can link the IP address to a customer and provide investigators the criminal's true identity. Law enforcement agents, through a subpoena, will request from the provider the name and address of the user of the IP address. However, ISPs regularly purge these records—sometimes within a matter of days or weeks—making it impossible for investigators to identify the criminal. Without this information, the investigation ends and the criminal remains at large.

Opponents of data retention have adopted the odd refrain that retaining IP addresses will do nothing to help combat the proliferation of child pornography on the Internet or other Internet crimes.¹⁶ This rhetoric is resoundingly rejected by the Justice Department, the FBI, and other law enforcement entities.

Both Democratic and Republican Administrations have been calling on Internet providers to retain information for a decade. In 1999, then-Deputy Attorney General Eric Holder said that “certain data must be retained by ISPs for reasonable periods of time so that it can be accessible to law enforcement.”¹⁷ Attorney General Alberto Gonzales told the Senate Banking Committee in 2006: “This is a problem that requires Federal legislation.” “We need information. Information that helps us make cases.”¹⁸

¹⁶ See, e.g., *Remarks of Rep. Conyers*, Markup of H.R. 1981, House Committee on the Judiciary, July 28, 2011 at 60.

¹⁷ *Remarks of U.S. Deputy Attorney General Eric Holder, International Conference on “Combating Child Pornography on the Internet,”* Vienna, Austria, Sept. 29, 1999, available at <http://www.justice.gov/criminal/cybercrime/dagecos.html>.

¹⁸ *Testimony of Attorney General Alberto R. Gonzales*, Hearing on the Sexual Exploitation of Children on the Internet before the Senate Committee on Banking, Housing, and Urban Affairs, United States Senate, 109th Congress, Sept. 19, 2006.

FBI Director Robert S. Mueller told the House Judiciary Committee in April 2008, “It’s important that we have access to the records, and record retention by ISPs would be tremendously helpful in giving us the historical basis to make a case in a number of these child predators who utilize the Internet to either push their pornography or to lure persons in order to meet them.”¹⁹ The FBI has identified this matter as one of its top legislative priorities.

The International Association of Chiefs of Police (IACP) adopted a resolution on October 17, 2006 expressing its “support for data retention in aid of the investigation of crimes facilitated or committed through the use of Internet and telephony-based communication services.” Among other things, the resolution declared that “the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations, such as computer intrusion investigations and child obscenity and exploitation investigations, although law enforcement has generally acted expeditiously in processing lawful requests to Internet providers.”²⁰

In January 2011, the Justice Department testified before this Committee that “the problem of investigations being stymied by a lack of data retention is growing worse. One mid-size cell phone company does not retain any records, and others are moving in that direction. A cable Internet provider does not keep track of the Internet protocol addresses it assigns to customers, at all. Another keeps them for only 7 days—often, citizens don’t even bring an Internet crime to law enforcement’s attention that quickly. These practices thwart law enforcement’s ability to protect the public. When investigators need records to investigate a drug dealer’s communications, or to investigate a harassing phone call, records are simply unavailable.”²¹

A. *H.R. 1981 Standardizes Current Data Retention Practices*

H.R. 1981 brings uniformity to the existing data retention practices of domestic Internet providers. “Most responsible providers are already collecting the data that is most relevant to criminal and national security-related investigations. In many cases, they have to collect it in order to provide service to begin with. In other cases, they collect it for the company’s security, or to research how their service is being used. They simply do not retain that data for periods that are sufficient to meet the needs of public safety.”²²

Current law does not require Internet providers to retain the records of the IP addresses they assign to their customers. In order

¹⁹ *Testimony of FBI Director Robert S. Mueller, III*, Hearing on the Oversight of the Federal Bureau of Investigation before the Committee on the Judiciary, United States House of Representatives, 110th Congress, Apr. 23, 2008.

²⁰ International Association of Chiefs of Police, Resolution in Support for Data Retention in Aid of the Investigation of Crimes Facilitated or Committed Through the Use of the Internet and Telephony-Based Communication Services, Adopted at the 113th Annual Conference, Oct. 17, 2006, available at: http://www.iacp.org/resolution/index.cfm?fa=dis_public_view&resolution_id=294&CFID=70738225&CFTOKEN=44837577.

²¹ *Testimony of Mr. Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Dept. of Justice*, Hearing on “Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes” before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, 112th Congress, Jan. 25, 2011 at 3.

²² *Id.* at 6.

to accomplish uniform retention of certain data by providers, H.R. 1981 amends an existing law known as the Stored Communications Act (SCA).²³ The SCA was enacted in 1986 as a part of the larger Electronic Communication Privacy Act or ECPA. ECPA provides a statutory framework for the types of information law enforcement agents are authorized to request from cable and telephone providers and the types of disclosures these providers must make to investigators.

The SCA requires law enforcement agents to present Internet providers with certain types of compulsory process, depending upon the type of information requested. For example, if investigators wish to access the content of communications, such as the ability to listen to a person's phone calls or read emails, they must first obtain a warrant. To obtain other types of subscriber records that do not contain content, such as IP addresses or telephone numbers, agents must serve the provider with a subpoena or court order. It is important to note that ECPA does not simply apply to Federal law enforcement agencies, but to state and local agencies as well.

An existing SCA provision, 18 U.S.C. 2703(f), requires a provider of wire or electronic communication services or a remote computing service to *preserve* certain customer records, including IP addresses assigned to the customer, at the request of law enforcement for 90 days. Law enforcement can extend this request for an additional 90 days. A section 2703(f) request functions like a snapshot. Providers preserve what records they have in their possession at the time of the request. If they do not have the records, they cannot and do not preserve them.

This is where section 2703(f) falls short. Because providers either do not retain IP address-assignment records or do so only for short periods of time, the provider has often already purged the records by the time law enforcement has discovered the Internet child pornography or other Internet crime and made the request under section 2703(f). If the records have not been retained, then there is nothing to preserve. And, as noted above, if investigators cannot make the initial step of identifying the perpetrator, the case runs cold.

The Justice Department testified in January 2011 that the section 2703(f) preservation "approach has had its limitations. The investigator must realize he needs the records before the provider deletes them, but providers are free to delete records after a short period of time, or to destroy them immediately. If, as has sometimes been the case, a provider deletes the relevant records after just a few seconds or a few days, a preservation request can come too late."²⁴

H.R. 1981 adds a new subsection (h) to section 2703 to establish a uniform retention period of 1 year for IP address assignment records. This provision standardizes the retention period for all providers and ensures that these records are available for a sufficient period of time. This new requirement will dramatically increase the number of Internet crimes in which investigators can take the first step in their investigation—identifying the suspect.

²³ Electronic Communication Privacy Act, Pub. L. No. 99-508, Title II, 18 U.S.C § 2702 et seq., 100 Stat. 1860 (1986).

²⁴ *Supra* note 21 at 5.

H.R. 1981 amends existing provisions in the law that provide liability protection to providers (subsection (e) of section 2703 and subsection (e) of section 2707) to include this new retention requirement in the list of activities for which providers are already afforded protection. These current liability provisions, even as amended by H.R. 1981, do not afford providers absolute immunity. Providers may still be liable for knowing or intentional violations of the law.

H.R. 1981 does not alter the existing SCA structure for the compulsory process required to obtain the data. The data retained by providers under the new subsection (h) of section 2703 created by the bill will only be accessible to investigators via subpoena or court order.

B. H.R. 1981 Balances the Needs of Law Enforcement Agencies and Service Providers and the Privacy Interests of Consumers

Investigators do not become aware of a crime, particularly one committed over the Internet, at the moment it happens. When dealing with a crime on the Internet, which can easily cross state or even international jurisdictions, weeks or months may pass before law enforcement discovers or is tipped off to a crime. Therefore, the retention period for the new mandate must be long enough to serve a legitimate law enforcement function while still accommodating providers' cost concerns and limiting the potential for a breach of the information.

H.R. 1981 as introduced imposed an 18-month retention period on providers. This period mirrors an existing Federal Communications Commission (FCC) regulation that requires telephone companies to retain for 18 months telephone 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.²⁵

The 1-year retention period adopted as part of the manager's amendment is even shorter than this long-standing FCC regulation and accordingly will reduce costs for providers, while still assisting law enforcement officers with apprehending some of the most dangerous criminals.

Civil liberties and privacy groups contend that data retention threatens consumer privacy. They base this contention on the misplaced belief that Internet users are endowed with a 4th Amendment expectation of privacy in the non-content records held by providers. To be sure, the 4th Amendment to the Constitution affords individuals a right to be free from unreasonable searches and seizures of their persons, houses, papers, and effects.²⁶ By and large, this protection extends to items the person owns or has possession of; for instance—papers in a file cabinet in one's home or conversations one has over the telephone.

Individuals do not, however, possess "a reasonable expectation of privacy in information disclosed to a third party. The Fourth

²⁵47 C.F.R. § 42.6 (1986) ("Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier").

²⁶U.S. CONST. amend IV.

Amendment simply does not apply.”²⁷ As the Supreme Court noted in *United States v. Miller*,²⁸

[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.²⁹

Therefore, the records maintained by a business, such as billing records or the records required to be retained under H.R. 1981, are not afforded constitutional protection under the 4th Amendment.³⁰ Indeed, the FCC requirement to retain telephone toll records is long-standing and non-controversial. The new requirement in H.R. 1981 is no different.

In enacting ECPA in 1986, Congress, however, chose to impose statutory requirements for the acquisition by the government of certain third-party business records, namely the requirement that law enforcement officials present a subpoena or court order to obtain these records from providers. The retention provision of H.R. 1981 in no way disrupts or undermines this requirement.

As the Justice Department explained in January 2011, “retained data is held by the provider, not the government. Federal law controls when providers can disclose information related to communications, and it requires investigators to obtain legal process, such as a subpoena or court order, in order to compel providers to disclose it.”³¹

Unfortunately, opponents of H.R. 1981 chose to ignore this well-established precedent and intentionally mischaracterize the bill’s retention provision “requiring ISPs to keep the digital data for every American that will be submitted to the Federal Government without a warrant whenever we ask.”³² This characterization is grossly inaccurate. As noted previously, many providers already retain this type of data in their ordinary course of business as it is their prerogative to do so. Law enforcement agencies also currently request and receive this data—via compulsory process as required by Federal law—in conjunction with their investigations. And, as the preceding discussion explains, a subpoena or court order, not a warrant, is required to obtain these non-content records.

H.R. 1981 provides perhaps the narrowest type of data retention possible. The bill does not require the retention of any email or telephone content. It only requires providers to retain a log of the IP addresses they assign to their customers, and the information necessary to link that information to a specific customer. There is any number of records or other information that this legislation could have included in the retention mandate. Rather, H.R. 1981 has a singular, narrow focus—retention of records needed to identify a criminal suspect.

²⁷Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

²⁸425 U.S. 435 (1976).

²⁹*Id.* at 443.

³⁰*See, generally, supra* notes 23 and 27.

³¹*Supra* note 21 at 6.

³²*Remarks of Rep. Lofgren*, Markup of H.R. 1981, Committee on the Judiciary, 112th Congress, July 28, 2011 at 138–39.

Instead of threatening customer privacy, data retention can help to protect it. Both Congress and the Administration are currently addressing the issue of cyber security. As technology advances, so too does the opportunity to exploit it. Whether through a cyber attack by a foreign government or a data breach by identity thieves, “data retention can help mitigate those threats by enabling effective prosecution of those crimes. Cyber criminals, often anonymously, hack into computer networks of retailers and financial institutions, stealing millions of credit and debit card numbers and other personal information.”³³ It is the retention of IP address information that allows law enforcement to identify these serious criminals.

C. Retention Should Not be Limited to Only Child Exploitation Offenses

Opponents of H.R. 1981 contend that data retention provision is overly-broad because it does not limit retention or access to only Internet child exploitation offenses. This criticism is unfounded.

Some have suggested that the data retention provision requires providers to retain only those records pertaining to child pornography. Such a limitation is both technologically impossible and presents a far greater threat to consumer privacy than the standardized retention proposed by H.R. 1981.

The assignment of IP addresses to customers is computerized, instantaneous, and continuous. This is not like the early days of telephones, when you called the operator and asked to be connected to your friend across town. The Internet is operated by a system of computers and networks that transmit all of the information via numerical codes.

Currently, providers retain customer IP address information through an automated computerized system. Providers cannot discern from the records what function they were used for (i.e., sending an email, logging onto a chat room, visiting a website) or the subject matter of the Internet transaction.

To require providers to comb through their IP address assignments records in order to identify those records connected only to child pornography has four significant flaws: (1) providers cannot discern what a customer did on the Internet simply by looking at the IP address they assigned to a customer to access the Internet; (2) even if they could do this, providers would still be required to collect all records of all IP address assignments in order to dissect them all and determine what to retain; (3) this would require providers to investigate the Internet usage of every single customer, including the vast majority of law-abiding customers—a much more significant privacy intrusion than is contemplated by H.R. 1981; and (4) such a mandate would be financially untenable for the providers—well beyond simply retaining a log of all IP address assignments.

In addition to proposing limiting *retention* to just child pornography investigations, some have also proposed limiting law enforcement *access* to the records to only child pornography investigations. This limitation too is flawed—and was rejected by the Committee at markup.

³³ *Supra* note 21 at 6.

The Internet is not simply home to child pornography crimes. It is a virtual world where thousands of crimes are carried out every day—including telemarketing fraud, drug trafficking, human trafficking, cyber attacks, and terrorist plots. The lack of a uniform data retention mandate affects these types of investigations as well.

According to the Justice Department, “Internet and cell phone companies’ records are crucial evidence in cases involving a wide array of crimes, including child exploitation, violent crime, fraud, terrorism, public corruption, drug trafficking, online piracy, computer hacking and other privacy crimes. What’s more, these records are important not only in Federal investigations, but also in investigations by state and local law enforcement officers.”³⁴

The Committee rejected an amendment to limit access to IP address data to only certain crimes against children and related offenses. Opposition to this limitation was based in large part on the belief that subpoenas or court orders served on providers as part of a legitimate law enforcement investigation should not be precluded simply because they seek evidence for an investigation of criminal activity outside this narrow category of offenses.³⁵

Limiting the new retention requirement in H.R. 1981 to only child pornography cases would significantly lessen what law enforcement agents are *currently* able to obtain from providers. Investigators are now able to request records for any crime, so long as they comply with the requirements of the law. The laws that set forth the types of duties imposed on providers or the types of compulsory process required by law enforcement agents make no distinction or limitation based on particular types of crime. Neither should the data retention mandate in H.R. 1981.

D. Transition to Internet Protocol Version 6 (IPv6)

Internet Protocol Version 6 (IPv6) is the new standard protocol (infrastructure) of the Internet that will transition it from IPv4, the current protocol. These protocols provide IP addresses to providers. In non-technical terms, IP addresses are “the ‘phone numbers’ for the Internet that are responsible for identifying computers and devices so they can communicate.”³⁶

The current protocol, IPv4, was developed in the late 1970’s during the developmental years of the Internet.³⁷ IPv4 uses 32-bit addresses and each address is a “collection of four “dotted quads” of numbers between 0 and 255, such as 7.91.248.30.”³⁸ “Each of the numbers is eight binary bits long, and there are four of them.”³⁹

³⁴ *Testimony of Mr. Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Dept. of Justice*, Hearing on “Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes” before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, 112th Congress, Jan. 25, 2011 at 2.

³⁵ *See Remarks of Mr. Sensenbrenner*, Markup of H.R. 1981, Committee on the Judiciary, U.S. House of Representatives, 112th Congress, July 27, 2011 at 78–79.

³⁶ *Microsoft Internet Protocol Version 6*, MICROSOFT TECHNET, available at <http://technet.microsoft.com/en-us/network/bb530961>.

³⁷ Robert Cannon, *Potential Impacts on Communications From IPv4 Exhaustion & IPv6 Transition*, FCC Staff Working Paper 3 (Dec. 2010), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1230/DOC-303870A1.pdf.

³⁸ Charles Arthur and Josh Halliday, *Internet almost out of space with allocation of last addresses*, THE GUARDIAN, (Feb. 1, 2011), available at <http://www.guardian.co.uk/technology/2011/feb/01/Internet-last-addresses-ipv4-ipv6>

³⁹ *Id.*

IPv4 holds a capacity about 4 billion unique addresses.⁴⁰ This “inherently limits the number of devices that can be given a unique, globally routable address on the Internet.”⁴¹ At that time, 4 billion addresses appeared to be sufficient since no one envisioned the future rapid growth of the Internet. However, by the 1990’s, Internet engineers recognized that the supply of addresses was relatively limited compared to likely future demand.⁴² Considering that the earth’s population is approximately 6.6 billion people, under the current IPv4 protocol it is not possible to give a single IP address to every person on the earth.⁴³

In response, IPv6 was developed to expand the address space on the Internet from 32 to 128 bits.⁴⁴ This increase enables essentially an unlimited number of IP addresses (340 trillion trillion addresses),⁴⁵ and subsequently an unlimited number of devices that can be directly connected to the global Internet.⁴⁶ In addition, “IPv6 is designed to solve many of the problems of IPv4, including mobility, autoconfiguration, and overall extensibility.”⁴⁷

So far, the adoption to IPv6 has been slow and IPv6 traffic makes up only about 10% of all Internet traffic.⁴⁸ Due to the increase in mobile technological devices, e.g. Smart phones, laptops, etc., there has been an increased address consumption rate.⁴⁹ In fact on Feb. 3, 2011, the Internet Assigned Number Authority (IANA) assigned the last batch of 32 bit address blocks to the Regional Internet Registries.⁵⁰ It is expected that the U.S. will exhaust its supply of IPv4 addresses by early-to mid-2012.⁵¹

The transition of the global Internet from IPv4 to IPv6 will not be instantaneous, but is expected to span many years. Since IPv6 is not backwards compatible, both networks will exist for some time. Therefore during this period of transition, there will be an issue for how devices on IPv4 and IPv6 networks are able to interact with each other.⁵² There are two main solutions to solve this issue, “dual stack” and “tunneling.”

With the dual stack solution, a host runs both an IPv4 and an IPv6 stack side by side. “Traffic which reaches the host using ei-

⁴⁰ *Supra* note 37.

⁴¹ *IPv Transition Guidance*, FEDERAL CIO COUNCIL ARCHITECTURE AND INFRASTRUCTURE COMMITTEE, (Feb. 2006).

⁴² *Supra* note 37.

⁴³ *Supra* note 41.

⁴⁴ *IPv6 Fact Sheet*, ICANN.org, available at <http://www.icann.org/en/announcements/factsheet-ipv6-26oct07.pdf>.

⁴⁵ *IPv6 Address Added for Root Servers in Root Zone*, ICANN, (Feb. 4, 2008), available at <http://www.icann.org/en/announcements/announcement-04feb08.htm>.

⁴⁶ *Microsoft Internet Protocol Version 6*, MICROSOFT TECHNET, available at <http://technet.microsoft.com/en-us/network/bb530961>.

⁴⁷ *Id.*

⁴⁸ *Lagging Security Features, Vulnerabilities Could Hamper Transition to a New Network*, SECNAP NETWORK SECURITY (Jun 8, 2011), available at <http://www.secnap.com/support/whitepapers/ipv6-status.html>.

⁴⁹ Carolyn Duffy Marson, *Asian Carriers Grab IPv4 Addresses at Record Rate*, PC WORLD, April 23, 2010, available at http://www.pcworld.idg.com.au/article/344143/asian_carriers_grab_ipv4_addresses_record_rate/

⁵⁰ Larry Greenemeier, *Out with the Old: As Internet Addresses Run Out, the Next Generation Protocols Set Up*, SCIENTIFIC AMERICAN, Feb 4, 2011, available at <http://www.scientificamerican.com/article.cfm?id=ipv4-to-ipv6-transition>.

⁵¹ *Working Group Launched to Ensure Seamless IPv6 Transition*, CONSUMER ELECTRONIC ASSOCIATION, Sept. 01, 2011, available at <http://www.ce.org/RSS/default.asp>.

⁵² *Outcomes of the Consultation held on the Transition from IPv4 to Ipv6 in Mauritius and the Recommendations Thereon*, ICTA OF MAURITIUS, July 2011, at 36, available at http://www.icta.mu/documents/Outcome_%20IPv6_Consultation.pdf.

ther network protocol can interact with the host.”⁵³ In contrast, tunneling is a solution utilized when there is no native IPv6 connectivity between different points on the network.⁵⁴ “It encapsulates one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks.”⁵⁵

In the current IPv4 network, commercial wireline providers, with a few exceptions, assign dynamic IP addresses (or temporarily assigned network addresses) to their customers on a “one-to-one basis,” meaning that an individual IP address from a public block of addresses is assigned to an individual customer on a temporary basis. During the transition to the IPv6 network, commercial providers may rely on what is known as a Network Address Translation (NAT) box.

The FCC provides the following description of a NAT system:

A NAT box is a host on the Internet with an IP address that has behind it a network of privately addressed computers. A specific block of addresses has been set aside for private use and is not advertised by networks to the public Internet. Since these addresses only work internally and cannot be used to communicate on the public Internet, they can be reused over and over again behind NATs.

An example of a NAT might be an off-the-shelf Wi-Fi access point that a residential user might use for home Internet access. The ISP assigns to that subscriber an IP address which is assigned to whatever computer the subscriber attaches at the end of the network. The subscriber attaches the Wi-Fi router. Behind the Wi-Fi router could be all of the computers in the house; the router assigns them IP addresses from the private IP address space. In this way, a subscriber with one public IP number can have multiple computers attached to the Internet. Commercial ISPs may utilize private IP numbers for their subscribers, and corporate LANs (such as the FCC internal network) may also utilize private IP addresses.

Network operators utilize NATs for various objectives. First, NATs are used to conserve the scarce numbering resource; one public address maps to multiple private addresses. Second, NATs are also used for network management and security, creating single points of entry into networks.⁵⁶

⁵³Robert Cannon, *Potential Impacts on Communications From IPv4 Exhaustion & IPv6 Transition*, FCC Staff Working Paper 18 (Dec. 2010), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1230/DOC-303870A1.pdf.

⁵⁴*Id.*

⁵⁵*IPV Transition Guidance*, FEDERAL CIO COUNCIL ARCHITECTURE AND INFRASTRUCTURE COMMITTEE (Feb. 2006) at 36.

⁵⁶*Supra* note 53 at 22 (internal citations omitted).

Utilization of a NAT box during IPv6 transition will have the effect of changing the “one-to-one” IP address assignment process to a “one-to-many” process, in that one public IP address will be sent to a router or proxy which will, in turn, assign private IP addresses to a group of customers to access the Internet.

Law enforcement officials or other governmental entities, private entities, and individuals that currently compel retained data from commercial providers typically proffer the IP address, date and time information, and perhaps other information to facilitate the provider identifying its customer or subscriber. The providers inform the Committee that during IPv6 transition, particularly if a NAT or proxy system is utilized, additional information from the requesting entity will likely be necessary to identify the individual customer or subscriber. This may include the private and public network source port numbers associated with the assigned subscriber IP address, which would be essential when providers are utilizing a carrier-grade NAT/Port Address Translation (PAT) solution. It would also be important for the requesting entity to be able to provide the private and public network destination port numbers in order to further correlate the customer or subscriber to the destination.

The data retention mandate in Section 4 of H.R. 1981 is intended to apply before, during and after⁵⁷ IPv6 transition. The Committee appreciates, however, that during IPv6 transition, this mandate could impose additional technical and cost burdens on some commercial providers who utilize a NAT or proxy server system to assign private IP addresses to customers rather than public IP addresses. Therefore, provider compliance with a subpoena or court order for retained data from a NAT system will likely require additional information from the requesting entity. The Committee strongly encourages those commercial providers and federal, state and local law enforcement agencies, and other affected entities to work cooperatively to seek technically feasible and economically reasonable solutions for retaining private addresses and the information necessary to identify those addresses with subscriber information.

IV. ADMINISTRATIVE SUBPOENA AUTHORITY FOR APPREHENSION OF FUGITIVE SEX OFFENDERS

The U.S. Marshals Service serves a unique function among Federal law enforcement agencies. As authorized by 28 U.S.C. § 566, the Marshals’ primary mission is “to provide for the security and to obey, execute, and enforce all orders of the United States District Courts, the United States Courts of Appeals, the Court of International Trade, and the United States Tax Court, as provided by law.”

The Marshals Service also executes all writs, process, and orders issued under the authority of the United States, and provides personal protection of Federal judges, court officers, witnesses, and others.⁵⁸

⁵⁷ *Id.* at 23. “After the transition to IPv6, with the dramatically increased address space, NATs would no longer be necessary in order to deal with the scarce numbering resource. It is expected that with IPv6 the use of NATs will likely decrease although it may not disappear.”

⁵⁸ 28 U.S.C. §§ 566(c), (e)(1)(A).

The Marshals Service is also the Federal Government's primary agency for fugitive apprehension.⁵⁹ The agency holds all Federal arrest warrants until they are executed or dismissed. In fiscal year 2010, the Marshals apprehended more than 36,100 Federal fugitives, clearing approximately 39,100 felony warrants.⁶⁰

The Adam Walsh Child Protection and Safety Act of 2006⁶¹ requires the Attorney General to use the Justice Department law enforcement resources to assist jurisdictions in locating and apprehending sex offenders who fail to comply with registration requirements. The Marshals is the primary agency charged with this responsibility.

Under the Adam Walsh Act, the Marshals Service assists state, local, tribal and territorial authorities in the location and apprehension of non-compliant sex offenders. It also investigates violations of the criminal provisions of the Adam Walsh Act, and identifies and locates sex offenders displaced as a result of a major disaster. In fiscal year 2010, the Marshals apprehended 11,072 sex offenders, initiated 3,025 investigations, issued 426 warrants for registration violations, and arrested 360 people for other violations of the Adam Walsh Act.⁶²

The Marshals' duties under the Adam Walsh Act require it to respond immediately to a tip regarding an absconded sex offender. However, to obtain records relevant to fugitive apprehension, the Marshals must make a request to a United States Attorney's Office to seek an "All Writs Act" order under 28 USC § 1651. This process is burdensome and time-consuming.

Administrative subpoena authority will allow the Marshals to access hotel, rental car, or airline records quickly, before the trail goes cold on a fugitive sex offender. Administrative subpoenas can only be used to obtain these types of records—they cannot be used to obtain the content of an email or wiretap a telephone.

The administrative subpoena statute, 18 USC § 3486, currently gives authority to use such subpoenas to the Attorney General and the Secretary of the Treasury for cases involving health care, child sexual exploitation, or threats against the President or other persons protected by the Secret Service. This is narrow authority is provided to the law enforcement agencies that investigate these areas of crime—the FBI and the Secret Service.

Although the Marshals Service is under the authority of the Attorney General, their unique role of providing Federal court security and fugitive apprehension does not include criminal investigations involving the sexual exploitation or abuse of children. As such, the authority granted under section 3486 does not automatically extend to the Marshals.

H.R. 1981, therefore, performs two important steps. First, it amends the general administrative subpoena authority statute—18 U.S.C. § 3486—to add investigations of unregistered sex offenders conducted by the U.S. Marshals Service. Second, it amends section 566 of title 28 to give the Marshals express administrative sub-

⁵⁹ 28 U.S.C. § 566(e)(1)(B).

⁶⁰ *Fact Sheets: Sex Offender Operations*, U.S. MARSHALS SERVICE, Feb. 25, 2011, available at http://www.usmarshals.gov/duties/factsheets/fugitive_ops-2011.html.

⁶¹ Pub. L. No. 109-248, 111 Stat. 2466 (2006).

⁶² *Supra* note 60.

poena authority—but only for fugitive investigations of unregistered sex offenders.

Unlike the administrative subpoena authority exercised by the U.S. Secret Service and the FBI under 18 USC §3486, which is used at the *beginning* of a criminal investigation, the administrative subpoena authority authorized by H.R. 1981 for the Marshals Service will only be used after the *conclusion* of a criminal investigation—i.e., after a guilty verdict for a sex offense that carries with it a registration requirement and after the sex offender has absconded and an arrest warrant has been issued by a judge.

V. ADDITIONAL PROTECTIONS FOR CHILD WITNESSES AND VICTIMS

Child pornography and exploitation prosecutions often hinge on the testimony of the child victim. Unfortunately, many children are abused by an acquaintance or even a family member and are often intimidated from telling their stories with threats that they will be punished or get in trouble if they tell.

Intimidation of minor witnesses is a persistent problem in criminal prosecutions. The most notable example was the case of DeAndre Whitehead, a Baltimore man who was sentenced to 6 years in Federal prison in 2005 for ordering the killing of an 11-year-old girl who testified in his murder trial. The U.S. Attorney for the District of Maryland had to take over the case after the state prosecutor failed to secure a conviction in the state's intimidation case. Maryland received criticism at the time for its ineffective witness intimidation laws.

The same problem has been seen elsewhere. In 2006, a Burlington Township, Pennsylvania, Truman High School class president Tyrone Lewis was prohibited from walking at his graduation or delivering his address except via video feed after the school received threats against Lewis. The threats were intended to intimidate his sister, Rachel, who was a witness in a murder case.

Surprisingly, the intimidation does not always come from the original perpetrators of the horrific act. In October 2007, a defense attorney in a child sexual-abuse case was arrested for intimidating the 16-year-old victim.⁶³ In February 2010, the father of a teen who forced a 5-year-old boy to perform sexual acts was charged with intimidating the victim's family.⁶⁴ In March 2011, a man charged with abusing two girls over a span of 9 years was accused of witness intimidation on three different occasions.⁶⁵

Current fines and contempt citations are inadequate to protect minor witnesses and victims, especially in child sex abuse cases. For example, in a case in Dublin, Ohio, a high school lacrosse coach was fined only \$1,000 after he was convicted of intimidating a player who accused the man's son, an assistant coach on the team, of sexual assault. Although Federal law provides criminal penalties for physical violence, threats, and other egregious forms of witness

⁶³ *Denver Attorney Arrested In Witness Intimidation Case*, DENVER NEWS CHANNEL, Oct. 4, 2007, available at <http://www.thedenverchannel.com/news/14269922/detail.html>.

⁶⁴ *Father of Rape Suspect Charged with Witness Intimidation*, WICKED LOCAL, Feb. 19, 2010, available at <http://www.wickedlocal.com/milford/news/x1650244989/Father-of-rape-suspect-charged-with-witness-intimidation#axzz1RoFC05we>.

⁶⁵ *Whitman Man Indicted on Child Sex-Abuse Charges*, ENTERPRISE NEWS, Mar. 09, 2011, available at http://www.enterpriseneews.com/news/cops_and_courts/x13264467/Whitman-man-indicted-on-child-sex-abuse-charges.

intimidation, more subtle forms of intimidation directed at a child remain unaddressed.

H.R. 1981 provides Federal courts with the means to control such intimidation through effective protection orders, and a new felony penalty for violation of such orders will strengthen the deterrent effect of a restraining order and prevent intimidation.

H.R. 1981 also instructs the U.S. Sentencing Commission to review, and increase if appropriate, the Sentencing Guidelines contained in Part J of Chapter 2, relating to penalties for witness intimidation in certain crimes against children offenses.

VI. ENHANCED PENALTIES FOR CHILD PORNOGRAPHY POSSESSION

Current law imposes a maximum 10-year penalty for child pornography possession offenses. Since the Supreme Court's 2005 *United States v. Booker*⁶⁶ decision, which made the Federal Sentencing Guidelines discretionary, in the Federal courts have begun to issue lower and lower sentences for child pornography offenses. From 2006 to 2010, the rate of within-Guideline range sentences for child pornography possession dropped from 62.6% to 39.6%. During that same time period, the number of possession cases receiving sentencing departures jumped from 61 (25.6%) to 394 (44.9%).⁶⁷

The decline in penalties stems, in part, from the false belief that possession of child pornography is not a serious crime, or at least is not as serious as other child exploitation offenses. This belief is dangerously flawed.

As the Justice Department noted in its August 2010 National Strategy, "many experts in the field believe that use of [the] term [child pornography] contributes to a fundamental misunderstanding of the crime—one that focuses on the possession or trading of a picture and leaves the impression that what is depicted in the photograph is pornography. Child pornography is unrelated to adult pornography; it clearly involves the criminal depiction and memorializing of the sexual assault of children and the criminal sharing, collecting, and marketing of the images."⁶⁸

The people who consume child pornography create the market for it, and thereby encourage the victimization of children. According to the Justice Department, 67 percent of reported sexual assault victims are children.

There is a growing link between the possession of child pornography and the actual molestation of children. NCMEC estimates that more than 40 percent of people convicted of possession are also guilty of victimizing a child, and there is evidence that pedophiles are increasingly only sharing their illegal images with "select" groups of people who are also able to share homemade images of child exploitation. This trend encourages further harm to children.

In 2009, a symposium of experts who studied child pornography met to share individual findings and develop an international consensus on the risks to children from child pornography. The symposium

⁶⁶ 543 U.S. 220 (2005).

⁶⁷ *Average Sentence and Position Relative to the Guideline Range for Child Pornography Possession Offenses, Fiscal Years 2005 through Preliminary 2010*, U.S. SENT. COMM'N (2010).

⁶⁸ *The National Strategy for Child Exploitation Prevention and Interdiction, A Report to Congress*, U.S. DEPT. OF JUSTICE, Aug. 2010, available at <http://www.projectsafefchildhood.gov/docs/natstrategyreport.pdf>.

sium recognized the general sense that there is a connection between child pornography and other sex related crimes.

Symposium participants . . . agreed that there is sufficient evidence of a relationship between possession of child pornography and the commission of contact offenses against children to make this a cause of acute concern. Participants did not see this necessarily as a linear relationship, but considered it a relationship that must be assessed in determining treatment and criminal justice options because, based on research using samples of individuals convicted of child pornography offenses, a significant portion of those who possess child pornography have committed a contact sexual offense against a child.⁶⁹

The belief that mere possession of child pornography images is not a serious crime also ignores the ongoing victimization that the children experience, often well into adulthood, knowing that their images continue to be shared on the Internet. As one psychologist recently testified in a child pornography possession case, “victims are constantly anxious, they walk around anxious. . . . when they go into the street they look at everyone they pass and say, ‘Did you see the pictures?’ . . . They are constantly ruminating about who have seen those pictures.”⁷⁰ These children’s lives are thrown into permanent disarray to feed the appetites of the “mere” possessors.

H.R. 1981 ensures tough penalties for those who victimize the youngest and most vulnerable of our society by increasing the maximum penalty from 10 to 20 years for offenses under sections 2252(b)(2) and 2252A(b)(2) of title 18 involving prepubescent minors or minors under the age of 12.

H.R. 1981 is supported by the National Center for Missing and Exploited Children, the National Center for Victims of Crime, the National Sheriffs’ Association, the Major County Sheriffs’ Association, the International Union of Police Associations, the Fraternal Order of Police, the International Association of Chiefs of Police, and the Federal Law Enforcement Officers Association.

Hearings

The Committee’s Subcommittee on Crime, Terrorism, and Homeland Security held 1 day of hearings on H.R. 1981 on July 12, 2011. Testimony was received from Mr. Ernie Allen, President and CEO, National Center for Missing and Exploited Children, Sheriff Michael J. Brown, Bedford County Sheriff’s Office, and Mr. Marc Rotenberg, President, Electronic Privacy Information Center, with additional material submitted by the National Sheriffs’ Association, Major County Sheriffs’ Association, the Fraternal Order of Police, the International Union of Police Associations, the National Center for Victims of Crime, and Mr. Levi C. Maaiia, Vice President, FullChannel. In addition, the Subcommittee held a hearing on January 25, 2011, to take testimony on the subject of data retention. Testimony was received from Mr. Jason M. Weinstein, Deputy As-

⁶⁹ Andrew G. Oosterbaan, *Global Symposium for Examining the Relationship Between Online and Offline Offenses and Preventing the Sexual Exploitation of Children*, U.S. DEPT. OF JUSTICE 10 (2009), available at http://www.governo.it/GovernoInforma/Dossier/G8_interno_giustizia/LEPSG_Child_Exploitation_Symposium.pdf.

⁷⁰ *United States v. C.R.*, ___ F.Supp.2d ___, 2011 WL 1901645, at *33 (E.D.N.Y. 2011).

sistant Attorney General, U.S. Department of Justice, Mr. John M. Douglass, Chief of Police, Overland Park, Kansas, Ms. Kate Dean, Executive Director, U.S. Internet Service Providers Association, and Mr. John B. Morris, Jr., General Counsel, Center for Democracy and Technology, with additional material submitted by Mr. Ernie Allen, President and CEO, National Center for Missing and Exploited Children.

Committee Consideration

On July 28, 2011, the Committee met in open session and ordered the bill H.R. 1981 favorably reported with an amendment, by a rollcall vote of 19 to 10, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee's consideration of H.R. 1981.

1. An amendment by Mr. Scott to limit the data retention period to 180 days. Defeated 12–14.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa	X		
Mr. Pence			
Mr. Forbes		X	
Mr. King			
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross			
Ms. Adams			
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee		X	
Ms. Waters	X		
Mr. Cohen			
Mr. Johnson	X		
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu	X		
Mr. Deutch		X	
Ms. Sánchez	X		

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Ms. Wasserman Schultz			
Total	12	14	

2. An amendment by Mr. Smith to add safe harbor language to Section 2 of the bill (creating a new offense for financial facilitation of access to child pornography) to exempt financial institutions assisting law enforcement investigations; to rewrite Section 4 relating to data retention; and to make other technical and conforming changes. Adopted 19–4.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Smith, Chairman	X		
Mr. Sensenbrenner, Jr.		X	
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte			
Mr. Lungren	X		
Mr. Chabot			
Mr. Issa			
Mr. Pence			
Mr. Forbes	X		
Mr. King			
Mr. Franks			
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Griffin	X		
Mr. Marino	X		
Mr. Gowdy	X		
Mr. Ross			
Ms. Adams	X		
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott		X	
Mr. Watt	X		
Ms. Lofgren		X	
Ms. Jackson Lee	X		
Ms. Waters	X		
Mr. Cohen	X		
Mr. Johnson	X		
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu	X		
Mr. Deutch			
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	19	4	

3. An amendment by Mr. Sensenbrenner to strike Section 7 and 10 (redesignated) from the underlying legislation to strike all subpoena powers granted under the bill. Defeated 10–17.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot			
Mr. Issa		X	
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams			
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee		X	
Ms. Waters	X		
Mr. Cohen	X		
Mr. Johnson	X		
Mr. Pierluisi			
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch		X	
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	10	17	

4. An amendment by Ms. Lofgren to strike Section 4 from the bill. Defeated 8–15.

ROLLCALL NO. 4

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot			
Mr. Issa			
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		

ROLLCALL NO. 4—Continued

	Ayes	Nays	Present
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross			
Ms. Adams			
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman		X	
Mr. Nadler			
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Cohen			
Mr. Johnson	X		
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch		X	
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	8	15	

5. An amendment by Mr. Scott to authorize additional funds for FBI agents, prosecutors and defenders assigned to work on child exploitation cases. Defeated 7–11.

ROLLCALL NO. 5

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble			
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren			
Mr. Chabot		X	
Mr. Issa			
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks			
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross			
Ms. Adams		X	
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters			
Mr. Cohen		X	

ROLLCALL NO. 5—Continued

	Ayes	Nays	Present
Mr. Johnson			
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu			
Mr. Deutch			
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	7	11	

6. An amendment by Ms. Lofgren to require ISPs to report nature of requests for data and costs to AOC, and also to require AOC to report to Congress yearly. Defeated 9–15.

ROLLCALL NO. 6

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa	X		
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks			
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams			
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters			
Mr. Cohen	X		
Mr. Johnson			
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch			
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	9	15	

7. An amendment by Ms. Lofgren to strike Sections 5 and 6 and to replace with language clarifying that existing protections under ECPA apply to data retained under Section 4. Defeated 7–18.

ROLLCALL NO. 7

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble			
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa		X	
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters			
Mr. Cohen	X		
Mr. Johnson			
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch			
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	7	18	

8. An amendment by Ms. Lofgren to forbid communication services from collecting any additional data that they do not already associate or collect for business reasons, and to forbid communication services from associating any information with a particular user. Defeated 7–16.

ROLLCALL NO. 8

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa			
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	

ROLLCALL NO. 8—Continued

	Ayes	Nays	Present
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Griffin		X	
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters			
Mr. Cohen			
Mr. Johnson			
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch			
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	7	16	

9. An amendment by Ms. Lofgren to retitle the bill as the “Keep Every American’s Digital Data for Submission to the Federal Government Without a Warrant Act of 2011.” Defeated 9–18.

ROLLCALL NO. 9

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa	X		
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		

ROLLCALL NO. 9—Continued

	Ayes	Nays	Present
Ms. Lofgren	X		
Ms. Jackson Lee		X	
Ms. Waters	X		
Mr. Cohen			
Mr. Johnson	X		
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu			
Mr. Deutch		X	
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	9	18	

10. Motion to report H.R. 1981 favorably, as amended. Passed 19–10.

ROLLCALL NO. 10

	Ayes	Nays	Present
Mr. Smith, Chairman	X		
Mr. Sensenbrenner, Jr.		X	
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte	X		
Mr. Lungren	X		
Mr. Chabot	X		
Mr. Issa		X	
Mr. Pence			
Mr. Forbes	X		
Mr. King	X		
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Griffin	X		
Mr. Marino	X		
Mr. Gowdy	X		
Mr. Ross	X		
Ms. Adams	X		
Mr. Quayle			
Mr. Conyers, Jr., Ranking Member		X	
Mr. Berman	X		
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee	X		
Ms. Waters		X	
Mr. Cohen			
Mr. Johnson		X	
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu			
Mr. Deutch	X		
Ms. Sánchez			
Ms. Wasserman Schultz			
Total	19	10	

Committee Oversight Findings

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 1981 the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 12, 2011.

Hon. LAMAR SMITH, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1981, the "Protecting Children from Internet Pornographers Act."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Martin von Gnechten (for Federal costs), who can be reached at 226-2860, and Marin Randall (for the impact on the private sector), who can be reached at 226-2940.

Sincerely,

DOUGLAS W. ELMENDORF,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 1981—Protecting Children from Internet Pornographers Act.

H.R. 1981 would amend current law to modify and expand Federal crimes related to child pornography. The legislation would prohibit financial transactions that facilitate access to child pornography. The legislation also would require Internet service providers to retain Internet usage information for at least 18 months and prevent legal actions against the providers related to the retention of those records. The bill also would allow the U.S. Marshals Service to issue administrative subpoenas to investigate unregistered sex offenders. Under the legislation, district courts would be required to issue protective orders to prevent harassment or intimidation of a minor victim or witness. H.R. 1981 also would direct the

U.S. Sentencing Commission to review Federal sentencing guidelines related to certain child abuse crimes.

IMPACT ON THE FEDERAL BUDGET

Enacting the legislation could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. However, CBO estimates that any net effects would be insignificant in any year. The bill could increase direct spending by extending witness protective services to certain minor witnesses and victims. Any such increases would be insignificant because of the small number of witnesses and victims likely to be affected.

In addition, because those prosecuted and convicted under H.R. 1981 would be subject to increased criminal fines, the Federal Government might collect additional fines if the bill is enacted. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the small number of cases likely to be affected.

Based on information from the Department of Justice (DOJ), CBO estimates that implementing H.R. 1981 would cost around \$1 million over the 2012-2016 period, assuming the availability of appropriated funds, mostly for DOJ to complete two studies and for changes in prison sentences. CBO estimates that H.R. 1981 would have a negligible impact on the number of offenders under Federal incarceration because many of the offenders prosecuted under H.R. 1981 can be prosecuted under current law.

IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS AND THE PRIVATE SECTOR

H.R. 1981 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on the State, local, or tribal governments.

The bill would impose private-sector mandates, as defined in UMRA, on providers of electronic communications services (such as telecommunication companies and Internet service providers) and on entities who have a right to file certain claims against those providers. The bill would require providers to retain for one year a detailed log of all electronic addresses assigned to each of their customers. To comply, providers would have to upgrade or build systems and buy hardware to collect, store, secure, and administer the required data.

CBO estimates that the total costs to private entities of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates (\$142 million in 2011, adjusted annually for inflation).

According to data from the Census Bureau, there are approximately 3,000 providers of electronic communications services. Based on information from industry experts and data technology professionals about current practices and the cost to design and install the data systems that would be required by the bill, CBO estimates that the aggregate cost of this mandate to the private sector would be more than \$200 million.

The bill also would eliminate an existing right to file claims against providers for retaining records of assigned electronic addresses. The cost of this mandate would be the forgone net value

of any awards and settlements in such claims. Based on value of awards and settlements in recent court decisions related to privacy rights and assigned electronic addresses, CBO expects that the cost of this mandate would not be large.

STAFF CONTACTS

The CBO staff contacts for this estimate are Martin von Gnechten (for Federal costs) and Marin Randall (for the impact on the private sector). The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 1981 provides additional investigative and prosecutorial tools and enhanced penalties to combat the proliferation of Internet child pornography, child exploitation offenses, and other Internet-based crimes.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 1981 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

The following discussion describes the bill as reported by the Committee.

Section 1. Short Title. This section cites the short title of the bill as the “Protecting Children from Internet Pornographers Act of 2011.”

Section 2. Financial Facilitation of Access to Child Pornography. This section creates a new Federal offense for the financial facilitation of child pornography. Any person who conducts a financial transaction knowing that it will facilitate access to child pornography will be liable under this section and may be fined or imprisoned up to twenty years. This new offense makes it a crime for someone to conduct a financial transaction knowing that such transaction will facilitate access to child pornography. Section 2 does not apply to financial transactions conducted by a person in cooperation with, or with the consent of, a federal, state or local law enforcement agency.

Section 3. Money Laundering Predicate. This section adds section 1466A of title 18 (relating to obscene visual representation of the abuse of children) and section 1960A of title 18 (relating to financial facilitation of access to child pornography) as specified unlawful activities under section 1956 of title 18, the Federal money laundering statute.

Section 4. Retention of Certain Records by Electronic Communication Service Providers. Subsection (a) requires commercial providers of an electronic communication service to retain for 1 year a log of the temporarily assigned network addresses the provider assigns to a subscriber or customer. Such log must enable the identification of the corresponding customer or subscriber information that providers are currently required to disclose pursuant to 18

U.S.C. § 2703(c)(2). The intent of this language is for these two subsections—the newly created 2703(h) and the existing (c)(2) to work in tandem with each other. Section 4 does not instruct providers on *how* they retain IP address assignment logs out of an abundance of caution to not disrupt the current retention practices of many providers. Section 4 is intended to enable the identification of a customer or subscriber to a corresponding IP address since this is often the only mechanism for identifying a criminal suspect operating via the Internet. It is envisioned that once such person's identity is determined, investigators will immediately seek disclosure of any information the provider also has under (c)(2). The types of information listed under (c)(2) are already held by most if not all providers as a necessary function of their businesses—name, address, billing information, etc. Without the required retention under the new 2703(h), there is often no way for law enforcement to request this commonly-held information under (c)(2).

Section 4 applies to both commercial wireline and wireless providers of an electronic communication service.⁷¹ The provision does not extend to commercial providers of a remote computing service since such a service does not engage in the act of assigning temporarily assigned network addresses to subscribers or customers. This section defines commercial providers in such a way as to exclude retention by a modem in a home or network in a business, free Wi-Fi services provided by bookstores, coffee shops, restaurants or other businesses, and fee-based Wi-Fi provided by hotels or other entities whose services are not available to the public. The intent is to maintain the current retention practices by telecommunication companies while not creating a new requirement on services such as those described above that may fall incidentally within the technical definition of electronic communication service.

Specifically, the definition of commercial provider excludes Internet services offered for free. Numerous businesses, city governments, and airports offer free Internet services to customers or to those within the range of service (such as Wi-Fi). By limiting the application of the bill to commercial providers who offer electronic communication services for a fee, an entity that offers free Internet service is excluded from the mandate.

Likewise, the bill also limits application of Section 4 to only commercial providers who offer electronic communication services to the public. Hotels and airlines, for example, offer fee-based Internet service to their customers, which is incidental to the primary service provided. This service also is available only to customers who first acquire the primary service of a hotel room or airline ticket. Unlike free Internet service available to all people who are in the District of Columbia or who purchase a coffee at Starbucks (and even those who do not), fee-based Internet service provided by hotels, airlines, or other similar businesses is not available to the public.

To be sure, although a member of the general public can enter a hotel lobby, that same person cannot enter a hotel room—for any

⁷¹ According to information compiled by Justice Department on the six largest wireless providers in the U.S., one major provider already retains IP session information for 1 rolling year, two wireless providers retain this data for 60 days, one provider retains non-public IP address data for 72 hours, and two providers do not retain at all. See *Retention Periods of Major Cellular Service Providers, Data Gathered by the Computer Crime and Intellectual Property Section, U.S. DEPT. OF JUSTICE* (Aug. 2010).

reason—without first paying for it or without the permission of a paying guest. To do so would be trespassing. No one would contend that the Snickers candy bar in a hotel room minibar or the wine offered for purchase on an airplane is available to any member of the public who wishes to purchase them. These are incidental services to the primary services of a hotel room or airline flight and can only be purchased once the necessary steps to acquire the primary service are completed. The same is true for fee-based Internet service in a hotel room or on an airplane. They are not available to the public but only to paying hotel room guests or airline passengers.

Subsection (a) limits access to such records to only governmental entities and directs the Attorney General to conduct a study of the costs associated with compliance by providers with the retention mandate. “Governmental entity” is defined by 18 U.S.C. §2711(4).

Subsection (b) expresses the Sense of Congress that records retained pursuant to this section should be stored securely to protect customer privacy and prevent against potential breach of the records.

Subsection (c) gives providers up to 180 days to comply with the retention requirement.

Subsection (d) directs the Attorney General to study the privacy standards implemented by providers with regard to compliance with the retention requirement and the frequency of any reported breaches of such data.

Section 5. No Cause of Action against a Provider Disclosing Information under this Chapter. This section amends section 2703(e) of title 18 to provide additional liability protections to providers who retain records pursuant to section 4 of the Act.

Section 6. Good Faith Reliance on Requirement. This section amends section 2707(e) of title 18 to add retention of records pursuant to the requirement under section 4 to the list of actions afforded liability protections.

Section 7. Subpoena Authority. This section amends section 556 of title 28 (governing the powers and duties of the U.S. Marshals Service) to authorize the U.S. Marshals Service to issue administrative subpoenas in investigations of unregistered sex offenders.

Section 8. Protection of Child Witnesses. This section amends section 1514 of title 18 (providing for protection of victims or witnesses) to expand protection of minor victims and witnesses from harassment or intimidation. The core of the section is an amendment to the current Federal protection order statute to allow courts greater flexibility in cases involving child victims and witnesses, who are more vulnerable to intimidation and manipulation. This section allows a Federal court to issue a protective order if it determines that harassment or intimidation exists specifically in the case of a minor witness and that the intimidation would affect the willingness of the witness to testify in an ongoing investigation or Federal criminal matter. Protective orders for minor witnesses can be issued for 3 years or until the witnesses’ 18th birthday, whichever is longer (protective orders for adults are capped at 3 years in length). This section also permits courts to issue protection orders to restrict the harassing or intimidating distribution of a witness’s restricted personal information on the Internet. This section also fills a gap in current law by creating criminal penalties of a fine, imprisonment up to 5 years, or both, for knowing and in-

tentional violations of any protective order issued under section 1514. Under the statute as currently written, there is no criminal enforcement capability for protective orders issued, and violators likely face nothing more than a contempt citation. This section was previously approved by both the House and Senate in the 111th Congress but not enacted into law.

Section 9. Sentencing Guidelines. This section directs the United States Sentencing Commission to review and amend Federal sentencing guidelines and policy statements to ensure that such guidelines provide an additional penalty for obstruction of justice, namely witness intimidation, associated with sex trafficking of children and other child abuse crimes. Similar language passed the House and Senate in the 111th Congress but was not enacted into law.

Section 10. Enhanced Penalties for Possession of Child Pornography. This section increases the maximum penalty from 10 to 20 years for child pornography offenses involving prepubescent minors or minors under the age of 12. This increase was approved by the House and Senate in the 111th Congress but not enacted into law.

Section 11. Administrative Subpoenas. This section makes a conforming amendment to section 3486 of title 18 (governing administrative subpoena authority) to authorize such authority for the USMS in apprehending unregistered sex offenders.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

PART I—CRIMES

* * * * *

CHAPTER 73—OBSTRUCTION OF JUSTICE

* * * * *

§ 1514. Civil action to restrain harassment of a victim or witness

(a) * * *

(b)(1) A United States district court, upon motion of the attorney for the Government, *or its own motion*, shall issue a protective order prohibiting harassment of a victim or witness in a Federal criminal case *or investigation* if the court, after a hearing, finds by a preponderance of the evidence that harassment of an identified victim or witness in a Federal criminal case *or investigation* exists or that such order is necessary to prevent and restrain an offense under section 1512 of this title, other than an offense consisting of misleading conduct, or under section 1513 of this title.

(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.

[(2)] (3) At the hearing referred to in paragraph (1) of this subsection, any adverse party named in the complaint shall have the right to present evidence and cross-examine witnesses.

[(3)] (4) A protective order shall set forth the reasons for the issuance of such order, be specific in terms, describe in reasonable detail [(and not by reference to the complaint or other document)] the act or acts being restrained.

[(4)] (5) The court shall set the duration of effect of the protective order for such period as the court determines necessary to prevent harassment of the victim or witness but in no case for a period in excess of three years from the date of such order's issuance. The attorney for the Government may, at any time within ninety days before the expiration of such order, apply for a new protective order under this section, *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.*

[(c) As used in this section—

[(1) the term “harassment” means a course of conduct directed at a specific person that—

[(A) causes substantial emotional distress in such person; and

[(B) serves no legitimate purpose; and

[(2) the term “course of conduct” means a series of acts over a period of time, however short, indicating a continuity of purpose.]

(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 reported to law enforcement as a missing person), or is part of a government-authorized effort to locate a fugitive or person of interest in a criminal, antiterrorism, or national security investigation.

* * * * *

CHAPTER 95—RACKETEERING

Sec.

1951. Interference with commerce by threats or violence.

* * * * *

1960A. Financial facilitation of access to child pornography.

* * * * *

§ 1956. Laundering of monetary instruments

(a) * * *

* * * * *

(c) As used in this section—

(1) * * *

* * * * *

(7) the term “specified unlawful activity” means—

(A) * * *

* * * * *

(D) an offense under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), section 115 (relating to influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), section 152 (relating to concealment of assets; false oaths and claims; bribery), section 175c (relating to the variola virus), section 215 (relating to commissions or gifts for procuring loans), section 351 (relating to congressional or Cabinet officer assassination), any of sections 500 through 503 (relating to certain counterfeiting offenses), section 513 (relating to securities of States and private entities), section 541 (relating to goods falsely classified), section 542 relating to entry of goods by means of false statements), section 545 (relating to smuggling goods into the United States), section 549 (relating to removing goods from Customs custody), section

554 (relating to smuggling goods from the United States), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), section 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds), section 793, 794, or 798 (relating to espionage), section 831 (relating to prohibited transactions involving nuclear materials), section 844 (f) or (i) (relating to destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), section 875 (relating to interstate communications), section 922(1) (relating to the unlawful importation of firearms), section 924(n) (relating to firearms trafficking), section 956 (relating to conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), section 1005 (relating to fraudulent bank entries), 1006 (relating to fraudulent Federal credit institution entries), 1007 (relating to Federal Deposit Insurance transactions), 1014 (relating to fraudulent loan or credit applications), section 1030 (relating to computer fraud and abuse), 1032 (relating to concealment of assets from conservator, receiver, or liquidating agent of financial institution), section 1111 (relating to murder), section 1114 (relating to murder of United States law enforcement officials), section 1116 (relating to murder of foreign officials, official guests, or internationally protected persons), section 1201 (relating to kidnaping), section 1203 (relating to hostage taking), section 1361 (relating to willful injury of Government property), section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction), 1466A (relating to obscene visual representation of the abuse of children), section 1708 (theft from the mail), section 1751 (relating to Presidential assassination), 1960A (relating to financial facilitation of access to child pornography), section 2113 or 2114 (relating to bank and postal robbery and theft), section 2252A (relating to child pornography) where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct, section 2260 (production of certain child pornography for importation into the United States), section 2280 (relating to violence against maritime navigation), section 2281 (relating to violence against maritime fixed platforms), section 2319 (relating to copyright infringement), section 2320 (relating to trafficking in counterfeit goods and services), section 2332 (relating to terrorist acts abroad against United States nationals), section 2332a (relating to use of weapons of mass destruction), section 2332b (relating to international terrorist acts transcending national boundaries), section 2332g (relating to missile systems designed to destroy aircraft), section 2332h (relating to radiological dispersal devices), section 2339A or 2339B (relating to providing material support to terrorists), section 2339C (relating to financing of terrorism), or

section 2339D (relating to receiving military-type training from a foreign terrorist organization) of this title, section 46502 of title 49, United States Code, a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (relating to aviation smuggling), section 422 of the Controlled Substances Act (relating to transportation of drug paraphernalia), section 38(c) (relating to criminal violations) of the Arms Export Control Act, section 11 (relating to violations) of the Export Administration Act of 1979, section 206 (relating to penalties) of the International Emergency Economic Powers Act, section 16 (relating to offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the Food and Nutrition Act of 2008 (relating to supplemental nutrition assistance program benefits fraud) involving a quantity of benefits having a value of not less than \$5,000, any violation of section 543(a)(1) of the Housing Act of 1949 (relating to equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, any felony violation of the Foreign Corrupt Practices Act, or section 92 of the Atomic Energy Act of 1954 (42 U.S.C. 2122) (relating to prohibitions governing atomic weapons)

* * * * *

§ 1960A. Financial facilitation of access to child pornography

(a) *IN GENERAL.*—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) *EXCLUSION FROM OFFENSE.*—This section does not apply to a financial transaction conducted by a person in cooperation with, or with the consent of, any Federal, State, or local law enforcement agency.

* * * * *

CHAPTER 110—SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN

* * * * *

§ 2252. Certain activities relating to material involving the sexual exploitation of minors

(a) * * *

(b)(1) * * *

(2) Whoever violates, or attempts or conspires to violate, paragraph (4) of subsection (a) shall be fined under this title or imprisoned not more than 10 years, or both, but if 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 such person has a prior conviction under this chapter, chapter 71,

chapter 109A, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or chapter 117, or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.

* * * * *

§ 2252A. Certain activities relating to material constituting or containing child pornography

(a) * * *

(b)(1) * * *

(2) Whoever violates, or attempts or conspires to violate, subsection (a)(5) shall be fined under this title or imprisoned not more than 10 years, or both, but, if *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 not more than 20 years, or if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.*

* * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * *

§ 2703. Required disclosure of customer communications or records

(a) * * *

* * * * *

(e) 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*, providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

* * * * *

(h) RETENTION OF CERTAIN RECORDS.—

(1) *A commercial provider of an electronic communication service shall retain for a period of at least one year a log of the temporarily assigned network addresses the provider assigns to a subscriber to or customer of such service that enables the*

identification of the corresponding customer or subscriber information under subsection (c)(2) of this section.

(2) Access to a record or information required to be retained under this subsection may not be compelled by any person or other entity that is not a governmental entity.

(3) The Attorney General shall make a study to determine the costs associated with compliance by providers with the requirement of paragraph (1). Such study shall include an assessment of all the types of costs, including for hardware, software, and personnel that are involved. Not later than 2 years after the date of the enactment of this paragraph, the Attorney General shall report to Congress the results of that study.

(4) In this subsection—

(A) the term “commercial provider” means a provider of electronic communication service that offers Internet access capability for a fee to the public or to such classes of users as to be effectively available to the public, regardless of the facilities used; and

(B) the term “Internet” has the same meaning given that term in section 230(f) of the Communications Act of 1934.

* * * * *

§ 2707. Civil action

(a) * * *

* * * * *

(e) DEFENSE.—A good faith reliance on—

(1) 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);

* * * * *

PART II—CRIMINAL PROCEDURE

* * * * *

CHAPTER 223—WITNESSES AND EVIDENCE

* * * * *

§ 3486. Administrative subpoenas

(a) AUTHORIZATION.—(1)(A) In any investigation of—

(i)(I) a Federal health care offense; or (II) a Federal offense involving the sexual exploitation or abuse of children, the Attorney General; **[or]**

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

[(ii)] (iii) an offense under section 871 or 879, or a threat against a person protected by the United States Secret Service under paragraph (5) or (6) of section 3056, if the Director of the Secret Service determines that the threat constituting the of-

fense or the threat against the person protected is imminent, the Secretary of the Treasury,

* * * * *

- (D) As used in this [paragraph, the term] *paragraph*—
 - (i) the term “Federal offense involving the sexual exploitation or abuse of children” means an offense under section 1201, 1591, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423, in which the victim is an individual who has not attained the age of 18 years [.] ; and
 - (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.).

* * * * *

(6)(A) A [United State] *United States* district court for the district in which the summons is or will be served, upon application of the United States, may issue an ex parte order that no person or entity disclose to any other person or entity (other than to an attorney in order to obtain legal advice) the existence of such summons for a period of up to 90 days.

* * * * *

(9) A subpoena issued under paragraph (1)(A)(i)(II) or [(1)(A)(ii)] (1)(A)(iii) may require production as soon as possible, but in no event less than 24 hours after service of the subpoena.

(10) As soon as practicable following the issuance of a subpoena under [paragraph (1)(A)(ii)] *paragraph (1)(A)(iii)*, the Secretary of the Treasury shall notify the Attorney General of its issuance.

* * * * *

SECTION 566 OF TITLE 28, UNITED STATES CODE

§ 566. Powers and duties

(a) * * *

* * * * *

- (e)(1) The United States Marshals Service is authorized to—
 - (A) provide for the personal protection of Federal jurists, court officers, witnesses, and other threatened persons in the interests of justice where criminal intimidation impedes on the functioning of the judicial process or any other official proceeding; [and]
 - (B) investigate such fugitive matters, both within and outside the United States, as directed by the Attorney General[.]; and
 - (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).

* * * * *

Dissenting Views

I. INTRODUCTION

H.R. 1981, the “Protecting Children From Internet Pornographers Act of 2011,” is a seriously flawed bill. Although it purports to be a bill to protect children from Internet pornographers, its reach extends well beyond this goal and is not narrowly tailored to combat child pornography. It includes an expensive and dangerous data retention mandate that would compromise the privacy of all Americans and unnecessarily burden the telecommunications industry. In addition, this legislation vastly expands administrative subpoena power, circumventing both judicial oversight and supervision by the Attorney General.

These problems, as well as additional concerns, have prompted more than 30 organizations to declare their strong opposition to H.R. 1981. These diverse organizations include religious groups, groups committed to the protection of civil liberties and privacy, advocates against domestic violence, and technology policy groups.¹ Additional organizations and think tanks have also registered their opposition stating that, “H.R. 1981 . . . follows in the footsteps of repressive governments such as China, which recently enacted a similar retention mandate . . . to facilitate its suppression of dissidents.”²

For these reasons, and those discussed below, we respectfully dissent and urge our colleagues to reject this seriously flawed legislation.

II. H.R. 1981’S DATA RETENTION MANDATE IS INTRUSIVE, EXPENSIVE, AND INEFFECTUAL

Section 4 of H.R. 1981 provides that “[a] commercial provider of an electronic communication service shall retain for a period of at least one year a log of the temporarily assigned network addresses the provider assigns to a subscriber to [sic] or customer of such service that enables the identification of the corresponding customer or subscriber information. . . .” This principle is called “data retention.”

¹Letter from Advocacy for Principled Action in Gov’t; Am. Booksellers Fund. for Free Expression; ACLU; Am. Library Ass’n; Ass’n of Research Libraries; Bill of Rights Def. Comm.; Ctr. for Dem. & Tech.; Ctr. for Digital Dem.; Ctr. for Fin. Privacy & Human Rights; Ctr. for Media & Dem.; Ctr. for Nat’l Sec. Studies; Consumer Action; Consumer Fed. of Am.; Consumer Watchdog; Council on Am.-Islamic Relations; Defending Dissent Found.; Demand Progress; DownsizeDC.org, Inc.; Elec. Frontier Found.; Elec. Privacy Info. Ctr.; Friends of Privacy USA; Liberty Coalition; Muslim Pub. Affairs Council; Nat’l Ass’n of Crim. Def. Lawyers; Nat’l Workrights Inst.; Patient Privacy Rights; Privacy Activism; Privacy Journal, Robert Ellis Smith, Publisher; Privacy Rights Clearinghouse; and World Privacy Forum; to Rep. Lamar Smith, Chairman, and Rep. John Conyers, Jr., Ranking Member (July 27, 2011) (“Privacy Sign-On Letter”) (on file with H. Comm. on the Judiciary, Dem. Staff).

²Letter from Competitive Enter. Inst., TechFreedom, & Am. for Tax Reform’s Digital Liberty, to Rep. Lamar Smith, Chairman, and Rep. John Conyers, Ranking Member at 2 (n.d.) (“Free Enter. Coal. Letter”) (on file with H. Comm. on the Judiciary, Dem. Staff).

Data retention should be distinguished from data preservation, which is a request by law enforcement for an Internet Service Provider (“ISP”) to refrain from destroying specific data about a particular individual, on the basis of individualized suspicion that the subject of the request is involved in criminal activity.³ Data retention, by contrast, is a blanket requirement that ISPs keep data on every customer, including customers who have no connection to criminal activity. In the United States, where 70 percent of 309 million Americans have Internet access, this means approximately 230 million Americans will be subject to the bill’s data retention requirements,⁴ and almost none of these data will ever be useful in a criminal investigation.⁵ Even though section 4’s data retention mandate is intrusive, expensive, ineffectual, and bad public policy,⁶ Representative Zoe Lofgren’s (D–CA) amendment⁷ to strike this provision from the bill failed by a vote of 8 to 15.⁸

A. The Data Retention Mandate Will Not Significantly Further Law Enforcement Goals

The bill’s data retention mandate will not significantly improve law enforcement efforts, as analyzed by the Congressional Budget Office (CBO). According to the CBO, “H.R. 1981 would have a *negligible impact* on the number of offenders under federal incarceration because many of the offenders prosecuted under H.R. 1981 can be prosecuted under current law.”⁹

Nevertheless, supporters of the bill are all too willing to compromise privacy and burden industry for an untested, albeit laudable, concept. Although there is myriad anecdotal evidence and strong personal views about the critical nature of the data, there is no empirical evidence to indicate that this mandate will actually further law enforcement’s goals in any significant way.¹⁰ To the contrary, the available data reveals that the status quo is working for industry and law enforcement alike and that a data retention mandate will exacerbate the current forensic evidence backlog crisis that law enforcement is already experiencing. In addition, we cannot ignore the fact that technology will cause numerous gaps in the gathering of this data that will severely undermine the purpose of the bill. The only goal the bill will actually further is that of compromising consumer privacy.

³*Data Retention As a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the H. Comm. on the Judiciary*, 112th Cong. at 73 (2011) (“*Data Retention Hearing*”) (statement of Kate Dean, Exec. Dir., U.S. Internet Svc. Provider Ass’n).

⁴*Data Retention Hearing* at 73 (statement of John Morris, Gen. Counsel, Ctr. for Dem. & Tech.).

⁵ONLINE SAFETY AND TECHNOLOGY WORKING GROUP, YOUTH SAFETY ON A LIVING INTERNET: REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP at 100 (2010) (“OSTWG Report”), available at http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf.

⁶See generally, Memorandum from John Morris, Greg Nojeim, & Erica Newland, Ctr. for Dem. & Tech. (July 19, 2011) (“CDT Memo”) (on file with H. Comm. on the Judiciary, Dem. Staff); Letter from Laura W. Murphy, Director, D.C. Legis. Office, Christopher Calabrese, Legis. Counsel, & Jesselyn McCurdy, Senior Legis. Counsel, ACLU, to Rep. Lamar Smith, Chairman, and Rep. John Conyers, Ranking Member (July 27, 2011) (“ACLU Letter”) (on file with H. Comm. on the Judiciary, Dem. Staff).

⁷Amdt. No. 6 to the bill.

⁸*Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 75 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

⁹CONG. BUDGET OFFICE, COST ESTIMATE FOR H.R. 1981 at 1 (Oct. 12, 2011) (emphasis added).

¹⁰Free Enter. Coal. Letter at 2.

1. *The Current Data Preservation Tools Are Effective*

There is no consensus among either the law enforcement community or industry representatives that there is a need for a data retention mandate, despite a decade-long debate over data retention. Most recently, in 2008, Congress created the Online Safety and Technology Working Group (OSTWG) to, among other things, “review and evaluate . . . the practices of electronic service providers and remote computing service providers related to record retention in connection with crimes against children.”¹¹ The panel, which included industry representatives, issued a final report, concluding in part that “there is not—either within OSTWG or the broader community—consensus on whether any data retention mandates should be imposed on service providers.”¹² Indeed, while some law enforcement representatives favor the bill, the U.S. Department of Justice has not taken a position on H.R. 1981.¹³

The available data suggests that the existing procedures for individualized data preservation on a specific customer¹⁴ are sufficient to provide law enforcement officials with the evidence they need to investigate and prosecute child exploitation offenses that occur on the Internet in about 80 percent of cases¹⁵ and, in the remaining 20 percent of cases, law enforcement officials obtain the required evidence “through other means, such as by interviewing suspects at their residences or reviewing information on [suspects’] computers.”¹⁶ Moreover, industry representatives observe that data preservation tools are underutilized by law enforcement. If the preservation period is insufficient, a better solution would be to extend the data preservation period by perhaps another 180 days, rather than create a new mandate. Data preservation is an effective and, unlike data retention, targeted law enforcement tool, which is much more consistent with American values that citizens are entitled to a presumption of innocence and invasive law enforcement tools require individualized suspicion. Moreover, unlike data preservation, data retention can misdirect law enforcement efforts. While effective prosecution requires urgency and real-time investigations, this bill focuses law enforcement’s attention backward, toward mass amounts of stale, unusable information.

The bill’s effectiveness is further undermined by the carve-out for the vast majority of information that is useful to law enforcement, specifically the data needed to identify users of free social networking, email and instant message services. The bill presumes that criminal activity occurs predominantly over paid accounts. Experience and common sense tell us that this type of activity occurs more commonly on free services.

¹¹ See Pub. L. No. 110–385, 122 Stat. 4103, § 214(a)(3).

¹² OSTWG Report at 110.

¹³ *Id.* at 105, n.87.

¹⁴ See 18 U.S.C. §§ 2703(f) & 2258A(h) (requiring ISPs to preserve data on a particular customer, upon request of law enforcement, for up to 180 days).

¹⁵ GOV’T ACCOUNTABILITY OFFICE, GAO–11–334, COMBATING CHILD PORNOGRAPHY: STEPS ARE NEEDED TO ENSURE THAT TIPS TO LAW ENFM’T ARE USEFUL AND FORENSIC EXAMINATIONS ARE COST EFFECTIVE at 44–45 (2011) (“GAO Report”), available at <http://www.gao.gov/new.items/d11334.pdf>.

¹⁶ *Id.* at 45.

2. *The Biggest Challenge to Investigating Child Exploitation Offenses is Not a Lack of Data, but a Backlog in Forensic Examinations*

H.R. 1981 will exacerbate the current backlog in forensic examinations. For example, during its study of the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (“PROTECT”) Act,¹⁷ the Government Accountability Office (GAO) found that the biggest barrier to investigating and prosecuting child pornography and other online child exploitation cases was a backlog of digital forensic evaluations,¹⁸ not an inability to locate data from an ISP prior to its destruction. Considering the recent reduction in the number of investigators dedicated to child pornography and other online child exploitation cases,¹⁹ Congress would be better off dedicating more resources to law enforcement personnel.²⁰ H.R. 1981, however, fails to authorize any such additional resources. In fact, when Representative Bobby Scott (D–VA) offered an amendment to appropriate funds for an additional 200 FBI agents, 30 additional prosecutors, and 20 additional public defenders, Committee Chairman Smith argued against the amendment and it was defeated by a 7 to 11 vote.²¹

The problem is not the lack of information provided to law enforcement. For instance, ISPs provided 248,000 tips through the Cyber Tipline from January 1, 2008 to December 31, 2010,²² but federal law enforcement agencies only investigated a fraction of these tips during the same²³ period: 17,799²⁴ investigations by the FBI, 8,414²⁵ by ICE, 684²⁶ by the Postal Inspectors, and 424²⁷ by the Secret Service. Giving law enforcement even more data to sort through will not further the goal of safeguarding our children against Internet pornographers, particularly when there is no willingness to provide more personnel. As Representative Scott stated at the markup, “When the problem is finding the needles in the haystacks of information . . . , the priority should not be adding more hay.”²⁸

¹⁷ Pub.L. 108–21, 117 Stat. 650 (2003).

¹⁸ GAO Report at 36–40. This backlog was partly a result of a 3000% increase in the amount of data that law enforcement had to review, and leading to delays in the analysis of suspects’ computers of up to a year. *Id.* at 35–36.

¹⁹ *Id.* at 50, 57 (reduction in both FBI and U.S. Postal Inspectors personnel dedicated to child pornography cases). Accordingly, the number of child pornography prosecutions is also decreasing. *Id.* at 9–10.

²⁰ CDT Memo at 4–5.

²¹ *Tr. of Markup of H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 87 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

²² GAO Report at 9–10.

²³ The CyberTipline numbers are reported by calendar year (January 1 to December 31), while the investigations numbers are reported by fiscal year (October 1 to Sept 30 of the following year).

²⁴ GAO Report at 51 (computed by adding together the numbers for FY2008, FY2009, and FY2010).

²⁵ *Id.* at 55 (computed by adding together the numbers for FY2008, FY2009, and FY2010).

²⁶ *Id.* at 57 (computed by adding together the numbers for FY2008, FY2009, and FY2010).

²⁷ *Id.* at 56 (computed by adding together the numbers for FY2008, FY2009, and FY2010).

²⁸ *Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 81 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

3. *The Nature of Current Technology and Limitations Imposed by H.R. 1981 will Prevent Millions of IP Addresses from being Retained*

Even if there was a demonstrated need for data retention, the mandate imposed by H.R. 1981 is wholly ineffective. Specifically, the nature of our current technology, as well as limitations built into the bill, would cause millions of Internet users to escape the reach of the mandate.

i. *Tor*

One example of such technology is Tor²⁹—a simple, free software application originally developed as a project of the U.S. Naval Research Laboratory.³⁰ Tor routes a user’s Internet traffic through a series of secure tunnels (the “Tor network”) before passing it off to the user’s final destination, using layers of concentric encryption in such a way that obscures: (1) the destination and content of users’ traffic from the user’s ISP, and (2) the users’ identity and location from the user’s website or other Internet destination the user intends to access.³¹ Tor’s goal is to allow people to browse and communicate over the Internet without being tracked or monitored, even by their ISP or by law enforcement.

Among its many uses, Tor enables child pornography traffickers to avoid detection and identification while they trade their illicit media. Law enforcement with access to an ISP’s retained data on a Tor user can discern only one thing: that a given user connected to the Tor network. Law enforcement would not be able to discern the content of the user’s communications over the Internet (*e.g.*, whether the user’s Internet traffic contained child pornography) nor would law enforcement be able to track down the user’s ultimate destination beyond the Tor network (*e.g.*, whether the user was visiting a child pornography website). Also, law enforcement could not work backwards to discover the identity and location of a Tor-using child pornography consumer using a list of computers known to have accessed a child pornography distributor. All that law enforcement would discover is that a computer from the Tor network accessed the distributor, but could not penetrate the Tor network to determine the identity or location of the actual user trafficking the child pornography.

“Unfortunately, nobody has explained to Congress that tech-savvy criminals can easily evade detection even if ISPs are required to retain data, by using such anonymity tools as TOR [sic]. . . .”³² H.R. 1981’s data retention mandate does nothing to eliminate the ability of child pornographers to use Tor to ply their illicit trade. H.R. 1981 applies only to “commercial provider[s] of an electronic communication service,” that is, services that “offer[] Internet access for a fee,” but Tor neither provides Internet access by itself, nor charges a fee. This is a gaping hole in the data reten-

²⁹TOR PROJECT, <http://www.torproject.org>.

³⁰U.S. NAVAL RESEARCH LAB, ONION ROUTING, <http://www.onion-router.net>.

³¹The Tor Project, which provides the software and operates the network of tunnels, has a more comprehensive, illustrated explanation. TOR PROJECT, TOR: AN OVERVIEW, <http://www.torproject.org/about/overview.html.en>.

³²Julian Sanchez, *Congress out to spy on your 'puter*, N.Y. POST (July 31, 2011), available at http://www.nypost.com/p/news/opinion/opedcolumnists/congress_out_to_spy_on_your_puter_z8eadkV4ktqtKfanoon1eL.

tion regime, and would ensure that anyone could avoid the data retention mandate simply by downloading and using a simple—and free—software program.

Before Congress rushes to criminalize it, we must recognize that Tor has myriad legitimate uses. It is accessed by law-abiding users who want to utilize the Internet anonymously and avoid detection or monitoring, while still exercising their First Amendment rights.³³ Pro-democracy dissidents in China use Tor to circumvent the “Great Firewall of China” and publish pro-democracy content. Journalists use Tor to privately and securely communicate with their sources. U.S. law enforcement uses Tor to conduct Internet surveillance or Internet-based sting operations without fear that the targets will discover the law enforcement officers’ identities. Whistleblowers use Tor to call attention to wrongdoing or malfeasance in their organizations without fear that their organization will eventually track down and retaliate against the whistleblower.

Unless H.R. 1981 is applied to Tor, child pornographers will be able to anonymize their Internet usage and circumvent the goal of the bill. This false choice between targeting child pornographers and protecting the First Amendment rights of law abiding citizens perfectly illustrates why the data retention mandate is unworkable and ineffective.

ii. Complimentary Wireless Internet Access

The proliferation of free Internet usage means that millions of users will be exempted from the mandate, which requires only fee based services to retain data. A host of businesses provide free wireless Internet access to their guests as a courtesy, including coffee shops, hotels, fast food restaurants, airlines, passenger rail, public libraries, universities, and even some law firms and doctors’ offices. As reported, H.R. 1981 exempts all of these organizations from the data retention mandate, because they do not offer Internet access “for a fee.”

By only requiring ISPs that “offer Internet access capability for a fee” to retain information, the bill fails to recognize the nuance inherent in distinguishing free versus paid business models. It creates an arbitrary distinction that means two identical entities are subject to a vastly different, and costly, government mandate depending on whether they charge for use of the Internet. For example, a hotel, under this law, that directly charges a customer for Internet access would be required to retain data while a hotel that provides free access (meaning the cost is built into the room rate) would not. Not only is there no rational basis for this type of distinction, but it could motivate some businesses not to charge for their services, to avoid the burden of complying with the mandate. Similarly, universities, in-flight Internet, coffee houses, rail service and other ISP services would either fall under or be exempt from this law based only on their current business model.

Further yet, child predators eager to avoid the law’s reach will have an incentive to spend time in places where children typically congregate, such as public libraries and McDonald’s restaurants. For example, McDonald’s, which is a popular family destination,

³³ TOR PROJECT, WHO USES TOR?, <http://www.torproject.org/about/torusers.html.en>.

has 11,500 United States locations that provide free wireless internet. By placing these locations outside the reach of the data retention mandate, H.R. 1981 “will encourage sexual predators to visit McDonald’s restaurants in order to share their illicit contraband online,” even though such “restaurants [are] packed with innocent children. . . .”³⁴

B. The Data Retention Mandate Seriously Infringes on the Legitimate Privacy Interests of Everyday Consumers

The data retention mandate is a substantial infringement on privacy rights, particularly when one considers that the vast majority of people using the Internet are innocent, law-abiding individuals.³⁵ The legislation mandates the retention of extremely sensitive and detailed personal information³⁶ that could be misused, fall into the wrong hands or be inadvertently or carelessly disclosed. Despite these risks, H.R. 1981 has no significant protections to protect sensitive personal information from abuse by industry or the government.

1. The Scope of the Data Retention Mandate is Overly Broad

By requiring paid ISPs to retain all IP data that can “enable the identification of the customer,” H.R. 1981 will force companies to retain a broad swath of private data about consumers pertaining to, among other things, their private communications, location and web-surfing activity. Once retained by ISPs, law enforcement need only meet a minimal standard to obtain this data—private, personal information including IP addresses, corresponding user identifying information and transactional data—because the data is subject to subpoena, without notice to the user or any judicial action.³⁷ Furthermore, this mandate would create a treasure trove of consumer information that would be susceptible to a data breach.

The overly broad data retention mandate will also eliminate competition between companies with respect to privacy. Some consumers place a high premium on privacy and choose a telecommunications company based upon the rigor of their privacy policies, such as the ability to opt-out of having their web-surfing information tracked or stored. These policies recognize the consumer’s right to maintain control over their information and are an important tool in securing user trust. By mandating the retention of all IP addresses in an identifiable format, H.R. 1981 would take away the discretion that ISPs currently have to tailor their privacy policies to the needs of consumers.

2. The 12-Month Data Retention Period is Excessive

Some ISPs already retain data on their customers’ IP addresses for varied amounts of time as part of their normal business prac-

³⁴ Christopher Soghoian, Grad. Fellow at the Ctr. for Applied Cybersecurity Research at Ind. Univ., *Unhappy meal: Data retention bill could lure sex predators into McDonalds, libraries*, ARS TECHNICA: LAW & DISORDER BLOG (July 11, 2011), available at <http://arstechnica.com/tech-policy/news/2011/07/unhappy-meal-data-retention-bill-could-lure-sex-predators-into-mcdonalds-libraries.ars>.

³⁵ Like industry, privacy experts also believe that the approach set forth in §2703(f) is better, because it targets those suspected of wrongdoing, rather than innocent users of the Internet. See OSTWG Report at 113.

³⁶ See ACLU Letter at 2; CDT Memo at 2.

³⁷ OSTWG Report at 114; see also 18 U.S.C. § 2703(c)(2) and 18 U.S.C. § 2703(c)(3).

tics.³⁸ H.R. 1981, however, would mandate a 12-month data retention period for all ISPs, even though the National Cable and Telecommunications Association (“NCTA”) reports that no law enforcement agency has ever requested data from their members that is more than 3 months old. In fact, “in Europe—where the Data Retention Directive requires that providers retain all sorts of data for a 6–24 month period—studies have made clear that the usefulness of retained data for law enforcement investigations falls off sharply after 6 months and again after twelve months.”³⁹

Given the privacy interests implicated by such a long retention window and the fact that law enforcement practice is not to request stale data, Representative Scott offered an amendment⁴⁰ to reduce the retention period to 180 days, from 1 year. Unfortunately, the Committee defeated this amendment by a 12 to 14 vote.⁴¹

3. *The Bill Fails to Provide Even Minimal Transparency for a Major Expansion of Law Enforcement Surveillance Powers*

This sweeping new data retention mandate also raises the possibility of government overreach and abuse, far beyond what is necessary to stop child exploitation. However, H.R. 1981 lacks any safeguards or reporting requirement that would ensure that both Congress and the public have a way to know how often the government is demanding Internet user data and whether those demands are being put to uses beyond tracking child pornographers.

Representative Zoe Lofgren offered an amendment that would have guaranteed a minimum of transparency for this major expansion of law enforcement surveillance powers. The amendment would have required a report on law enforcement’s requests for historical information from providers that includes the number of requests that law enforcement made, the types of cases, and the results of such requests. This report would have been similar to the annual Wiretap Report that the Administrative Office compiles, on the volume and nature of government wiretap applications.⁴² The Committee defeated Representative Lofgren’s amendment⁴³ by a vote of 9 to 15.⁴⁴

C. *The Data Retention Mandate Imposes Significant Costs on the Private Sector*

The costs of complying with H.R. 1981 will be onerous for the private sector. In fact, the Congressional Budget Office estimates that the aggregate cost of the mandate on the private sector would be more than \$200 million.⁴⁵ This amount exceeds the threshold set by the Unfunded Mandates Reform Act for private sector man-

³⁸ OSTWG Report at 103.

³⁹ CDT Memo at 4.

⁴⁰ Amdt. No. 1 to the Manager’s Amdt.

⁴¹ *Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 69 (July 27, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2027%2011%20HR%202633%20HR%201981.pdf>.

⁴² *Cf.* 18 U.S.C. § 2519 (Reports concerning Intercepted Wire, Oral, or Electronic Communications).

⁴³ Amdt. No. 8 to the bill.

⁴⁴ *Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 100 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

⁴⁵ CONG. BUDGET OFFICE, COST ESTIMATE FOR H.R. 1981 at 2 (Oct. 12, 2011).

dates. Much, if not all, of this cost will likely be passed on to consumers by ISPs in the form of fees or higher rates.⁴⁶

Industry representative argue that the actual cost to the private sector and consumers may be much higher than the CBO estimates. The cost of compliance with the data retention mandate could be \$1.6 billion because of the transition from using IPv4 to IPv6⁴⁷ and the greater difficulty in maintaining data about customers under IPv6⁴⁸ than under the currently-used IPv4, the cost of compliance with the data retention mandate could be \$1.6 billion. The U.S. Internet Service Provider Association (“USISPA”) estimates that the cost of implementing and operating H.R. 1981’s retention requirement over 5 years would be \$500 million. The European Union’s experience is also telling. According to Finland’s Ministry of the Interior, if the original proposal had been adopted it would have involved costs of about \$5.5 billion Euro for his country.⁴⁹

H.R. 1981 would require ongoing costs, in addition to the “costs the provider would incur to design and install the data systems that would be required by the bill.”⁵⁰ For example, AOL considered a smaller ISP with only about 4 million customers, estimates that it issues more than 50 million IP addresses per day. AOL’s costs under H.R. 1981 will not only include creating, maintaining, and securing⁵¹ the infrastructure to store the 50 million specific IP addresses created per day, and all of the related required information, but also creating and maintaining similar infrastructure to sort and search through all that data with the speed and precision law enforcement will demand.

H.R. 1981’s unfunded private sector mandate will hit small and rural providers especially hard, driving some of them out of business and leaving some rural residents without any Internet provider.⁵² According to National Telecommunications Cooperative Association (“NTCA”), rural Internet providers “are small businesses that operate on thin margins and lack the economies of scale to absorb a large, sudden cost,” in part because they “serve areas where there is no business case for service and where others refuse to serve.”⁵³ If the high cost of H.R. 1981’s regulatory mandate drives rural providers out of business,⁵⁴ “there [will] typically be no pro-

⁴⁶Free Market Coalition Letter at 1 (“[C]onsumers themselves [will] ultimately bear most of the costs incurred by companies in complying with the data retention mandate.”).

⁴⁷See generally ROBERT CANNON, FCC, FCC WORKING PAPER 3, POTENTIAL IMPACTS ON COMM’NS FROM IPV4 EXHAUSTION & IPV6 TRANSITION (Dec. 2010).

⁴⁸See *id.* at 25 (“These solutions [to various problems arising due to the transition to IPv6], however, break end-to-end connectivity and make it difficult to map specific IP numbers to individual end users. IP numbers may map to carrier grade NAT boxes which may have behind them many households, neighborhoods, or even towns, making it difficult to know to whom an IP address belongs.”).

⁴⁹“Data Retention Directive: reactions related to the costs involved,” 18 January, 2006, available at <http://www.edri.org/edrigram/number4.1/dataretentioncosts> (last accessed October 14, 2011)

⁵⁰CONG. BUDGET OFFICE, COST ESTIMATE FOR H.R. 1981 at 2 (Oct. 12, 2011).

⁵¹See OSTWG Report at 111 (noting that data retained under the bill “would present new and unparalleled risks to privacy and security”); see also Free Enter. Coal. Letter at 2.

⁵²See Letter from Shirley Bloomfield, CEO, National Telecommunications Cooperative Association to Rep. Lamar Smith, Chair (July 26, 2011) (“NTCA Letter”) at 1; see also Letter from Levi C. Maaia, Vice President of Full Channel (July 8, 2011).

⁵³NTCA Letter at 1.

⁵⁴See, e.g., CDT Memo at 3.

vider ready to step in and provide the kind of area-wide service that the local and national economies rely on.”⁵⁵

To help ISPs deal with an unfunded mandate that could range from \$200 million to \$1.6 billion, Representative Lofgren offered an amendment⁵⁶ to clarify that the bill would not require any ISP to collect any information which it was not already collecting for business purposes. The committee defeated this amendment by a vote 7 to 16.⁵⁷

D. The Data Retention Mandate Endangers Victims of Domestic Violence, Sexual Assault, and Stalking

For domestic violence victims and other victims of stalking and sexual assault, the data retention mandate increases their risk of further abuse.⁵⁸ Cindy Southworth, founder of the Safety Net Technology Project at the National Network to End Domestic Violence, cites the example of a domestic violence victim whose abuser subpoenaed her cell-phone records, after the victim went into hiding across the country.⁵⁹ Armed with these cell phone records, the abuser found out where the victim lived, worked, and which friends and family she called for support.⁶⁰ H.R. 1981’s data retention mandate creates another trove of information for abusers to mine for information on their victims, putting victims at risk.⁶¹

Although the bill, as reported, provides that only “governmental entities” may access the retained data, this will not prevent malicious abusers and stalkers from illegally obtaining the data by impersonating a law enforcement agent and conning ISP employees into turning over the confidential data to the stalker or abuser. In fact, Congress has already recognized that this so-called “pretexting” is a problem when it comes to phone call records.⁶² In response, the Law Enforcement and Phone Privacy Protection Act of 2006⁶³ was enacted to criminalize this conduct and provide increased penalties. There is no reason to suggest that the stalkers and abusers of domestic violence victims will have any more trouble obtaining Internet records than phone records. Once armed with this information, a stalker or abuser can locate their intended victim, even after that victim has gone into hiding. Accordingly, the mere existence of this retained data is a threat to victims of domestic violence and stalking.

E. Despite its Stated Purpose, H.R. 1981 Is Not Limited to Child Pornography Offenses

While the stated goal of H.R. 1981 is to combat Internet-based child pornography and other child exploitation cases, it is not limited to such cases. There is nothing in the bill to prevent law en-

⁵⁵ NTCA Letter at 1.

⁵⁶ Amdt. No. 38 to the bill.

⁵⁷ *Tr. of Markup of H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 137 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

⁵⁸ Letter from National Network to End Domestic Violence to Representative Lamar Smith, Chairman, and Representative John Conyers, Jr., Ranking Member at 1 (July 26, 2011) (on file with H. Comm. on the Judiciary, Dem. Staff).

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² See H.R. Rep. 109–395 at 2–3 (2006) (discussing “pretexting”).

⁶³ Pub. L. No. 109–476, 120 Stat. 3568 (codified at 18 U.S.C. § 1039).

forcement from using the data for investigations of any crime from terrorism⁶⁴ to the unlawful interstate transport of water hyacinths,⁶⁵ and even in intelligence gathering operations, which generally do not require disclosure to the target.

This kind of “mission creep” is hardly unprecedented. When Congress passed the “sneak and peak” provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (“USA PATRIOT”) Act of 2001⁶⁶ in the wake of the September 11th terrorist attacks, it intended for the provision to be used in terrorism investigations. And yet, of the 763 “sneak and peak” warrants issued between October 1, 2007 and September 30, 2008, only 3 were terrorism-related;⁶⁷ the biggest category was narcotics investigations, for which 474 sneak-and-peak warrants were issued.⁶⁸

Knowing that law enforcement will have such broad access to their personal data, with no restrictions on the reason for obtaining it, Internet users may alter their usage habits, even if entirely legal. A gay or lesbian student may not want to find a support group to help him or her through bullying; a woman who felt a lump in her breast may avoid looking up medical information on breast cancer; a political activist may avoid organizing supporters online out of the fear that complete strangers may discover their perfectly legitimate, but private, activities.

Even the bill’s short title is misleading.⁶⁹ Representative Zoe Lofgren (D–CA) sought to amend the title to reflect what the bill actually does, “Keep Every American’s Digital Data for Submission to the Federal Government Without a Warrant Act of 2011.” This amendment, however, was rejected by the Committee by a vote of 9 to 18.⁷⁰

F. H.R. 1981 Contains An Unconstitutional Limitation on Access to Personal Data

The bill, as reported, includes a provision limiting access to the data retained under section 4 to “governmental entities.”⁷¹ This language was added in an attempt to address concerns that, once ISPs are required to maintain this data, private parties, such as divorce lawyers, insurance companies, bill collectors, or marketing companies, could also access the data. The limitation on access to

⁶⁴ See 18 U.S.C. § 2332b.

⁶⁵ See 18 U.S.C. § 46.

⁶⁶ Pub. L. No. 107–56 § 213, 115 Stat. 272, 286, codified at 18 U.S.C. § 3103a.

⁶⁷ See JAMES C. DUFF, DIRECTOR, ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMIN. OFFICE OF THE U.S. COURTS ON APPLICATIONS FOR DELAYED-NOTICE SEARCH WARRANTS & EXTENSIONS (2009) at 6, available at <http://big.assets.huffingtonpost.com/SneakAndPeakReport.pdf>.

⁶⁸ *Id.*

⁶⁹ “If Congress had to name laws honestly, [H.R. 1981] would be called the ‘Forcing Your Internet Provider to Spy On You Just In Case You’re a Criminal Act of 2011’. . . .” Julian Sanchez, *Congress out to spy on your ‘puter*, N.Y. POST (July 31, 2011), available at http://www.nypost.com/p/news/opinion/opedcolumnists/congress_out_to_spy_on_your_puter_z8eadkV4ktqtKfanoon1eL; see also Jim Harper, *Moral Panic & Your Privacy*, CATO@LIBERTY (July 11, 2011), available at <http://www.cato-at-liberty.org/moral-panic-and-your-privacy>.

⁷⁰ Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary, 112th Cong. at 148 (July 28, 2011), available at <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

⁷¹ “As used in [inter alia, 18 U.S.C. § 2703, the U.S. Code section amended by H.R. 1981 § 4], the term ‘governmental entity’ means a department or agency of the United States or any State or political subdivision thereof.” 18 U.S.C. § 2711.

“governmental entities,” however, would also preclude criminal defendants from accessing this information because they are not “governmental entities.” Under the Constitution, however, criminal defendants are entitled to receive all evidence favorable to them and a restriction on access to that data violates the defendants’ right to due process.⁷² This limitation will not withstand judicial scrutiny.

III. H.R. 1981 CONTAINS AN UNNECESSARY AND BROAD EXPANSION OF ADMINISTRATIVE SUBPOENA POWER

Section 11 of H.R. 1981 grants the United States Marshals Service (“USMS”) administrative subpoena power in cases involving unregistered sex offenders.⁷³ This unprecedented expansion of administrative subpoena power circumvents the normal, judicially-supervised subpoena process and grants the USMS unfettered authority to investigate cases that do not even deal with child pornography.⁷⁴

Under current law, the Attorney General already has the authority to issue administrative subpoenas in investigations of “a Federal offense involving the sexual exploitation or abuse of children. . . .”⁷⁵ Section 11 would allow the USMS to issue administrative subpoenas, not to investigate actual offenses against children, but to investigate nonregistration of former offenders “even if [the nonregistered offender] is not suspected of any new sex crime,”⁷⁶ and even though there is no difference in recidivism rates between former offenders who comply with registration requirements and former offenders who do not.⁷⁷

Further, this bill would allow the USMS itself to issue subpoenas without oversight from either the Attorney General or the courts. This broad delegation of unsupervised power to lower-level executive officials is without precedent. As a result of this provision, the USMS would have even more authority than the Secret Service when confronted with an imminent threat against a President, when there is simply no exigency warranting such extraordinary power. As Assistant Attorney General Robert Rabin explained in 2000:

The administrative subpoena power . . . reflects a delicate balancing of law enforcement, oversight, and privacy needs and issues, all within the limited context of health care

⁷²“Under the Due Process Clause of the Fourteenth Amendment, criminal prosecutions must comport with prevailing notions of fundamental fairness. We have long interpreted this standard of fairness to require that criminal defendants be afforded a meaningful opportunity to present a complete defense. To safeguard that right, the Court has developed ‘what might loosely be called the area of constitutionally guaranteed access to evidence.’” *California v. Trombetta*, 467 U.S. 479, 485 (1984) (quoting *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 (1982)).

⁷³Persons convicted of certain sex-related federal crimes are required to register with the federal government. See Adam Walsh Child Protection and Safety Act of 2006, Title I, Pub. L. No. 109-248, 120 Stat. 587 (codified at 42 U.S.C. 16901 *et seq.*).

⁷⁴“Administrative subpoenas are an improvisation to accommodate the massive power of the bureaucracy, and they’ve become another end-run around the Fourth Amendment.” Jim Harper, *Moral Panic and Your Privacy*, CATO@LIBERTY (July 11, 2011 5:02pm), available at <http://www.cato-at-liberty.org/moral-panic-and-your-privacy>.

⁷⁵18 U.S.C. § 3486(a)(1)(A)(i)(II).

⁷⁶ACLU Letter at 5.

⁷⁷*Reauthorization of the Adam Walsh Act: Hearing Before the H. Comm. on the Judiciary*, Serial No. 112-12, 112th Cong., at 63 (Feb. 15, 2011) (statement of Dawn Doran, Dep. Dir., Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) Office, U.S. DOJ).

fraud investigations. This [provision] . . . was part of a special health care fraud and abuse initiative. . . . [It] was not anticipated to serve as a vehicle by which to expand administrative subpoena authority to other Cabinet officers for special types of investigations unrelated to health care fraud.⁷⁸

Even if it could be demonstrated that the USMS needed this extraordinary power, the appropriate way to grant this authority would be to have the cabinet-level Attorney General—not the lower-level director of the USMS—issue these administrative subpoenas, as is done with the Secret Service. Unfortunately, when Representative Scott offered an amendment⁷⁹ to accomplish this result, the Committee defeated it by voice vote.⁸⁰ And when Mr. Sensenbrenner offered an amendment⁸¹ to strike both sections containing the subpoena authority, the Committee defeated it by a vote of 10 to 17.⁸²

X. CONCLUSION

H.R. 1981 contains numerous problematic provisions, many of which—including the data retention mandate—will do little to further the goal of apprehending child pornographers. Instead, this legislation would compromise the privacy of all Americans and unnecessarily burden the telecommunications industry, all under the guise of protecting children. The bill contains an intrusive and expensive data retention mandate that threatens the privacy of Internet users everywhere. In addition, H.R. 1981 dramatically expands administrative subpoena power, circumventing judicial oversight. For these reasons, we respectfully dissent.

JOHN CONYERS, JR.
ROBERT C. “BOBBY” SCOTT.
ZOE LOFGREN.
HENRY C. “HANK” JOHNSON, JR.

○

⁷⁸ Letter from Robert Raben, Ass’t Att’y Gen., to Rep. Henry Hyde, Chairman, H. Comm. on the Judiciary (June 9, 2000), *quoted in* H.R. REP. 106-669, at 14–15 (2000).

⁷⁹ Amdt. No. 11 to the bill.

⁸⁰ *Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 122 (July 28, 2011), *available at* <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.

⁸¹ Amdt. No. 3 to the bill.

⁸² *Tr. of Markup on H.R. 1981: Before the H. Comm. on the Judiciary*, 112th Cong. at 42 (July 28, 2011), *available at* <http://judiciary.house.gov/hearings/pdf/7%2028%2011%20HR%201981%20HR%201433.pdf>.