Testimony and Statement for the Record of

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

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

Before the

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

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

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

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

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

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

---

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

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

I. The Electronic Communications Privacy Act

A. Background on Privacy Laws

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

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

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

Other privacy bills include similar requirement.[7]

B. The Electronic Communications Privacy Act

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

---

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

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

C. "Data Retention" and "Data Preservation"

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

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

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

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

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

---

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

D. Disclosures of records by service providers

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

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

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

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

II. Current Industry Practices

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

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

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

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

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

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

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

---

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

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

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

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

III. Proposed Legislative Changes and Potential Problems

A. Data Retention Obligation

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

B. Immunity Provisions

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

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

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

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

[28] 18 U.S.C. § 2703(c)(2)

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

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

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

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

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

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

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

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

IV. The Importance of Data Minimization Practices

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

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

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

---

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

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

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

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

V. The European Experience with Data Retention Requirements

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

VI. Recommendations:

A. Remove Sections 4, 5, and 6

---

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

[50] *Id.*

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

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

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

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

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

B. New Reporting Requirement for Access to Transactional Data

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

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

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

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

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

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

This committee should consider similar reporting requirements for law enforcement requests to Internet providers similar to those that were considered by this Committee in 2000.[55]

Conclusion

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

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

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