



July 20, 2011

Chairman Lamar Smith  
U.S. House Judiciary Committee  
2138 Rayburn House Office  
Building  
Washington, DC 20515

Ranking Member John Conyers  
U.S. House Judiciary Committee  
2138 Rayburn House Office  
Building  
Washington, DC 20515

RE: ACLU Urges Opposition to H.R. 1981 on Privacy and Internet Security  
Grounds

Dear Chairman Smith and Ranking Member Conyers:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to the principles of individual liberty and justice embodied in the U.S. Constitution, we are writing today to express our opposition to H.R. 1981, the “Protecting Children From Internet Pornographers Act of 2011.” We are specifically concerned with section 4 (retention of records), sections 5 and 6 (immunity provisions) and sections 7 and 11 (subpoenas authority). Collectively these provisions invade the privacy of innocent individuals, create dangerous cybersecurity vulnerabilities and authorize overbroad information collection by law enforcement.

Sexual abuse of children is already a criminal act. All reasonable people agree that such abuse harms children to an almost unfathomable degree. Child pornography commercially exploits that harm. While H.R. 1981 may have the best of intentions, its provisions are overzealous and would harm millions of Americans while doing little to stop child pornography.

**Section 4 – Retention of Records**

Section 4 of H.R. 1981 would impose sweeping requirements on internet companies, forcing them to keep records on their customers for 18 months — impacting hundreds of millions of individuals who have no connection to the sexual exploitation of children whatsoever. As drafted the legislation requires that any “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”. There is no limitation in the law requiring that these records be used in child exploitation cases. Instead they would be available to law enforcement for any purpose.

AMERICAN CIVIL  
LIBERTIES UNION  
WASHINGTON  
LEGISLATIVE OFFICE  
915 15th STREET, NW, 6<sup>TH</sup> FL  
WASHINGTON, DC 20005  
T/202.544.1681  
F/202.546.0738  
[WWW.ACLU.ORG](http://WWW.ACLU.ORG)

LAURA W. MURPHY  
DIRECTOR

NATIONAL OFFICE  
125 BROAD STREET, 18<sup>TH</sup> FL.  
NEW YORK, NY 10004-2400  
T/212.549.2500

OFFICERS AND DIRECTORS  
SUSAN N. HERMAN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

ROBERT REMAR  
TREASURER

Temporarily assigned network addresses, also known as IP addresses, can reveal very personal and private information. These addresses are the direct link between individuals and their online activity. In essence, an IP address is a proxy for an individual's name or other identifier online. Access to this link is the lynchpin in determining the sites users visit online – what their interests are, where they bank, what online accounts they have. Such information can be used for a variety of purposes, not just criminal investigations, including by lawyers in civil lawsuits, hackers attempting to break into an individual computers, or stalkers trying to find a particular person.

Access to records of IP addresses can reveal sensitive information. For example, police in Maui recently requested IP address information from a news website in order to identify a commenter in an article describing a particular case of police abuse.<sup>1</sup> In other cases law enforcement has sought the IP addresses of every visitor to a news site on a particular day.<sup>2</sup>

Furthermore many in law enforcement have argued that it is insufficient to retain information just from companies that assign IP addresses (such as internet service providers). They argue that record retention should extend to others who provide email and data storage services like Google, Facebook, and a wide swath of other internet companies.<sup>3</sup> Such a mandate would have even more sweeping effects on privacy.

Individual search results provide a good example of how detailed and invasive these types of records can be. For example Google keeps temporarily assigned network addresses with each of its searches.<sup>4</sup> If, as some have suggested, a record retention requirement is extended to service providers like Google, such searches would have to be kept for 18 months. Embarrassing searches on subjects like incontinence or depression, work-related searches for new clients, or inquiries about sensitive political or religious issues would all have to be retained.

This proposal comes at a time when U.S. laws in the digital privacy area are woefully out of date. As the Committee explored in multiple hearings last Congress, the Electronic Communications Privacy Act has not been substantially updated since 1986 — before the creation of the World Wide Web. As the examples above demonstrate, the type and detail of records have increased dramatically since 1986. They have become much more revealing – describing reading habits, interests, personal relationships and a variety of other constitutionally protected interests – while rules for accessing and using these records have remained the same or, in the case of national security provisions, been weakened. The data retention mandate

---

<sup>1</sup> See: Jacob Shafer, *Maui Police Department Targets MauiTime's Online Commenters*, MauiTimes, May 25, 2011.

<sup>2</sup> See: <https://www.eff.org/wp/anatomy-bogus-subpoena-indymedia>

<sup>3</sup> *YOUTH SAFETY ON A LIVING INTERNET: REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP*, JUNE 4, 2010, pg 104.

<sup>4</sup> See: <http://www.google.com/intl/en/privacy/faq.html#toc-terms-server-logs>

would exacerbate these problems, making records available and identifiable for even longer periods of time.

Perhaps worst of all, record retention mandates do not address the main problems with investigating and prosecuting child pornography. In a recent report, the Government Accountability Office made clear that addressing the problem of child pornography is much more seriously hindered by:

- A lack of feedback to the National Center for Missing and Exploited Children (NCMEC) which results in incomplete or ineffective reports to law enforcement;
- The lack of a centralized “deconfliction” system that prevents multiple law enforcement entities from investigating the same crimes; and
- Backlogs in forensic analysis of digital evidence.<sup>5</sup>

An increased record retention mandate means adding even more records to a system that is already overburdened and ineffective.

## Sections 5 and 6 – Immunity Provisions

Section 5 and 6 are very expansive. These provisions create immunity for companies that retain records pursuant to section 4 and exempt this collection from civil liability. As drafted, we believe these sections could overrule state data breach laws and data security protections as well as potentially immunize companies against tort and other claims.

The new section 2703(e) of title 18 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 (new language in italics)

The breadth of this requirement is noteworthy. It applies to all records, not just IP addresses, and says that no cause of action shall lie for retaining records. Similarly, under the new section 6, a provider’s good faith reliance on the need to retain records would serve as a complete defense to any criminal or civil action, whether brought under 18 USC 2707 (the civil liability provision of the Electronic Communications Privacy Act) or any other law. In practice this means that any company that retains records

---

<sup>5</sup> *COMBATING CHILD PORNOGRAPHY Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective*, March 2011, GAO-11-334.

pursuant to this section could argue that they are immune from any liability stemming from that retention. Even if poor data security practices lead to a data breach or mistakes lead to the loss of crucial data, the company would be immunized.

The sweeping nature of these immunity provisions would decrease corporate incentives to protect records and provide adequate data security. In a time when high profile data breaches are daily news stories and identity theft is widespread, this provision seems ill-considered at best.<sup>6</sup> Greater detail on this provision can be found in the July 12, 2011 testimony of Marc Rotenberg, Director of the Electronic Privacy Information Center.

### **Sections 7 and 11 – Administrative Subpoena for “Unregistered Sex Offenders”**

Section 7 and 11 of H.R. 1981 create authority for the U.S. Marshals Service to issue administrative subpoenas “solely for the purpose of investigating “unregistered” sex offenders. We oppose granting to the Marshals Service or any executive branch agency the power to issue subpoenas which would allow it to write its own search and disclosure orders with no judicial approval.

Under current law, the government can obtain documents or testimony through its normal criminal investigative powers which include obtaining a criminal search warrant or grand jury subpoena. Criminal search warrants apply to all documents and require a judge or magistrate to find probable cause that the search will produce evidence of crime. Although grand jury subpoenas do not require probable cause, they do require a grand jury to find that the testimony or documents are relevant to an ongoing grand jury investigation of criminal activity and they can be challenged before a judge.

While administrative subpoenas are typically suited for regulatory investigations such as the administration of federal benefits programs, they have also been made available in certain criminal contexts where rigorous checks and balances provide protection against abuse. For decades, agencies such as the FBI have sought general administrative subpoena power and Congress has repeatedly been reluctant to grant it out of concern for the unchecked nature of such authority.<sup>7</sup>

---

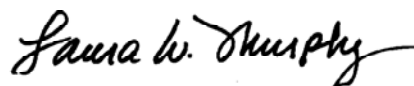
<sup>6</sup> Tate, Ryan, “Apple’s Worst Security Breach: 114,000 iPad Owners Exposed.” *Gawker* 2010, June 9, from: <http://gawker.com/5559346/>; Udo de Haes, Andreas, “Microsoft BPOS cloud service hit with data breach.” *Computer World*, December 22, 2010, from: [http://www.computerworld.com/s/article/9202078/Microsoft\\_BPOS\\_cloud\\_service\\_hit\\_with\\_data\\_breach](http://www.computerworld.com/s/article/9202078/Microsoft_BPOS_cloud_service_hit_with_data_breach); Aspan, Maria and Bartz, Diane, “Verizon customers exposed in massive U.S. data breach.” *Reuters*, April 6, 2011, from: <http://www.reuters.com/article/2011/04/06/us-verizon-epsilon-idUSTRE7350AI20110406>

<sup>7</sup> The National Security Letter provision of the Patriot Act radically expanded the FBI’s authority to demand personal customer records from Internet Service Providers, financial institutions and credit companies without prior court approval. Through NSLs the FBI can compile vast dossiers about innocent people and obtain sensitive information such as the

In addition, 18 U.S.C. 3486 currently grants the Attorney General administrative subpoena authority in any investigation of a federal offense involving sexual exploitation or abuse of children. Since simple failure to maintain registry as a sex offender can be deemed such a federal offense, H.R. 1981 would in effect allow the Marshals Service to seize computer files of an unregistered sex offender without court approval even if he or she is not suspected of any new sex crime.

Americans still have a reasonable expectation that their federal government will not gather records about their day to day activities without probable cause of a crime and without a court order. We hope that Congress will protect balance the needs of law enforcement without sidestepping our Constitution's fundamental checks and balances. H.R. 1981 purports to restrain online child pornography, but in reality it fails to achieve that worthy objective while trampling the privacy rights of almost everyone who goes online. For these, reasons we oppose H.R. 1981 and urge the members of the Committee to reject the bill or drastically reformulate Sections 4, 5, 6, 7, and 11.

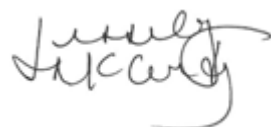
Sincerely,



Laura W. Murphy  
Director, Washington Legislative Office



Christopher Calabrese  
Legislative Counsel



Jesselyn McCurdy  
Senior Legislative Counsel

---

web sites a person visits, a list of e-mail addresses with which a person has corresponded, or even unmask the identity of a person who has posted anonymous speech on a political website. The Justice Department's Inspector General has reported that between 2003 and 2006, the FBI issued nearly 200,000 NSLs. The inspector General has also found serious FBI abuses of the NSL power.