



May 25, 2016

The Honorable Charles Grassley
Chairman, Senate Judiciary Committee
U.S. Senate
Washington, D.C. 20510

The Honorable Patrick Leahy
Ranking Member, Senate Judiciary Committee
U.S. Senate
Washington, D.C. 20510

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH 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

RE: Senate Judiciary Committee Markup of S. 356, the Electronic Communications Privacy Act Amendments Act.

Dear Chairman Grassley, Ranking Member Leahy, and Members of the Committee,

The American Civil Liberties Union (ACLU) strongly supports S. 356, the Electronic Communications Privacy Act Amendments Act, sponsored by Senators Leahy and Lee, and we are pleased that the Judiciary Committee is holding a markup of this bill.

The ACLU – along with a broad coalition of companies, privacy groups, and other stakeholders – strongly supports ECPA reform.¹ Almost a quarter of the Senate has cosponsored S.356, and the House voted overwhelmingly, 419-0, to pass H.R. 699, their ECPA reform bill.

We believe that S.356 contains critical provisions necessary to ensure that Americans' adoption of modern technologies – like email and cloud storage – does not require sacrificing Fourth Amendment privacy protections. Specifically, the bill would impose a warrant requirement for access to electronic content (with limited exceptions), consistent with the Sixth Circuit's decision in *U.S. v. Warshak*.² As a result, the bill would end the outdated "180-day rule" in ECPA, which permits law enforcement to access email communications older than 180 days without a warrant. Similarly, the bill will also require a warrant for opened emails—rejecting the Department of Justice's interpretation that ECPA does not require a warrant in such instances. This is consistent with the current policies of the FBI³ and major service providers, which generally require a warrant before consumers' content information can be turned over to law enforcement officials.

¹ Coalition Letter from Privacy Groups and Companies to the House of Representatives in Support of H.R. 699, the Email Privacy Act, (April 13, 2016), <https://cdt.org/files/2016/04/Coalition-Letter-Supporting-HR-699-As-Amended-final041316-1.pdf>.

² *United States v. Warshak*, 769 F.3d 372 (6th Cir. 2014).

³ Rep. Susan DelBene, *Rep. DelBene Questions FBI Director James B. Comey*, YOUTUBE (June 11, 2014), <https://www.youtube.com/watch?v=Okle6t7bHi4&feature=youtu.be>.

Though we prefer S.356, the ACLU supports H.R. 699, which modified S.356's companion bill in the House and passed by a unanimous vote. By codifying a warrant-for-content rule with limited exceptions, H.R. 699 represents a significant step forward in updating outdated provisions of ECPA. However, we acknowledge that H.R. 699 does not achieve all of the reforms we believe are needed: it eliminates key notice provisions contained in the original version of the bill, lacks a strong suppression remedy, and does not address geolocation information. We will continue to work for these important protections.

H.R. 699 was the product of extensive negotiations between Congressional staff, companies, civil society, and other stakeholders. There were significant privacy concessions made during that process. Significant substantive changes to the bill would disrupt the compromise forged in the House, and undermine the broad coalition of support behind the bill. Thus, the ACLU urges members of the Committee to oppose any weakening amendments, including those that would:

- 1) Expand the government's surveillance authority by allowing the government to obtain information regarding Americans' online communications through National Security Letters (NSLs);
- 2) Create concerning mandatory emergency exceptions; or
- 3) Create overbroad exceptions to the warrant requirement in cases where the user may not have appropriately provided consent.

The ACLU would oppose the bill if the amendments referenced above were adopted, without modification.

NSL Statute Expansion

The ACLU urges the committee to oppose amendments, which would expand the types of information the FBI can obtain using an NSL.

Cornyn Amendment 1 would dramatically expand the government's surveillance authority by allowing the government to use an NSL to obtain sensitive information from companies regarding Americans' online communications. Current law limits the use of NSLs to collect only the "name, address, length of service, and local and long distance toll billing records of a person or entity" from an electronic communication service provider. Other types of electronic communication transaction record (ECTR) data, such as email logs, cell site data, or even browser history, cannot be obtained by the FBI absent a court order. This amendment would remove the requirement for a court order and open the door for FBI access into deeply sensitive information, with few checks on abuse.

Indeed, the FBI has a long history of abusing the NSL statute for warrantless access of American's private information.⁴ Between 2003 and 2005, the FBI issued over 140,000 NSLs, all of which included gag orders against disclosing what information was being requested.⁵ The information collected from NSLs is retained indefinitely and shared within the intelligence community. An audit by the Office of the Inspector General at Department of Justice (DOJ) found numerous instances of NSLs intentionally being

⁴ Letter from the American Civil Liberties Union to the House Judiciary Committee, (last visited May 25, 2016), available at, <https://www.aclu.org/letter/aclu-statement-abuse-national-security-letters-submitted-house-judiciary-committee/>.

⁵ *National Security Letters*, EPIC (last visited May 25, 2016), <https://epic.org/privacy/nsl/>.

abused to gain access to private information in cases that were not relevant to an FBI investigation.⁶ And, NSLs have also been used in the past for the bulk collection of thousands of records.

Given the troubling use of NSL's, Congress should reject any attempt to expand the already overbroad authorizing statute. Such an expansion would grant the FBI access to intimate details of Americans without appropriate judicial oversight or accountability.

Mandatory Emergency Exception

The ACLU urges the committee to oppose amendments which would *require* providers to disclose electronic records and communications, even in cases where the provider does not have a good faith belief that an emergency does in fact exist. Such a change is unnecessary and would create increased opportunities for abuse.

Under both current law and the ECPA reform legislation, law enforcement has the ability to go to a communications provider and ask for the voluntary disclosure of electronic records and communications. The provider may disclose information in response to such a request if they, “in good faith,” believe that “an emergency involving danger of death or serious physical injury” requires disclosure.⁷

Providers routinely respond to such requests. For example, from January to June 2015, Google reported that it received 236 emergency requests, and produced data in 69% of these cases.⁸ Similarly, for the same period, Facebook reports that it received 855 requests and produced data in response to 74% of the cases.⁹ However, allowing provider the discretion to deny requests that are not adequately supported acts as an important check against law enforcement abuse in cases where police seek to circumvent the warrant requirement or otherwise misuse emergency requests. Indeed, there are numerous examples of such emergency exceptions being misused. For example:

- In a comprehensive 2010 investigation, the Inspector General at the DOJ found that, in the years following the 9/11 attacks, the FBI repeatedly misused so-called “exigent letters” and other informal requests to compel the production of telephone records and other material. In many cases, the FBI presented the request as exigent when it was not, in fact, an emergency.¹⁰
- In a case in Anderson, California, police coerced a person seeking a restraining order into saying she had been held against her will for six hours, and then sent a false emergency request for location information to the purported kidnapper’s cellular service provider.¹¹

⁶ Mike German, *ACLU Roadmap of Justice Department Inspector General’s Review of the FBI’s Use of National Security Letters*, ACLU (March 19, 2007), <https://www.aclu.org/letter/aclu-roadmap-justice-department-inspector-generals-review-fbis-use-national-security-letters>.

⁷ 18 U.S.C. § 2702(b)(8), (c)(4) (2012). Indeed, the standard by which providers may disclose communications and records was lowered in 2006 in the USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 107(b)(1)(B), 120 Stat. 192 (2006) to allow disclosure with a “good faith” belief.

⁸ *Transparency Report: United States*, GOOGLE, (last visited May 25, 2016), <https://www.google.com/transparencyreport/userdatarequests/US/> (last visited April 11, 2016).

⁹ *United States Law Enforcement Requests for Data*, FACEBOOK (last visited May 25, 2016), <https://govtrequests.facebook.com/country/United%20States/2015-H2/>.

¹⁰ DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, *A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 257–72* (2010), *available at* <https://oig.justice.gov/special/s1001r.pdf>.

¹¹ *Jayne v. Sprint PCS*, No. CIVS072522LKKGGHP, 2009 WL 426117, at *2 (E.D. Cal. Feb. 20, 2009).

- In Reno Nevada, a law enforcement training manual warned that emergency tracking had been “misused” and that continued misuse would “undoubtedly backfire.”¹²
- Police in Baltimore repeatedly made emergency requests for cellphone information from companies, even when true emergencies did not exist.¹³

By making emergency disclosure mandatory, Sessions Amendment 1 and 2 would increase the opportunities for the types of abuses cited above. In addition, these amendments lack critical back-end protections such as after-the-fact judicial review, notice, suppression, standing for providers to challenge improper requests, and a civil remedy for individuals whose information is improperly disclosed. As a result, individuals would lack any meaningful remedy or recourse in cases where law enforcement incorrectly obtains their information through the proposed emergency provisions.

Consent Exception

The ACLU urges the committee to oppose amendments that contain unnecessary exceptions to the warrant clause in cases in cases where a user may not have provided meaningful consent.

Currently, if a user consents to government access of their information, they can provide that information directly to the government. Indeed, major providers are increasingly taking steps to ensure that users are able to access their information and provide it to any party of their choosing. In cases where a user may no longer be able to access their information, the appropriate course is for the provider to provide the information *directly to the user* (who may then provide the information to the government). Sessions Amendment 1 and Cornyn Amendment 2 flip this logic on its head. Instead, the proposed amendments would allow providers to give information directly to the government without adequate protections to ensure that a user has provided meaningful consent and is fully aware of the scope of information that may be given to the government. Such an amendment is unnecessary and opens the door to improper disclosures resulting from abuse or human error.

Additionally, the ACLU urges members to oppose amendments that seek to expand the activities covered by the Computer Fraud and Abuse Act ("CFAA") and create new authority for the government to hack computers.

The Senate Judiciary Committee has the opportunity to amend our outdated laws to ensure that Americans' Fourth Amendment rights are protected in the digital age – through a bill that passed unanimously in the House and has the support of broad coalition spanning companies and civil liberties organizations. We urge the Committee to pass this bill, without weakening amendments, and bring the law in-line with Americans' expectations of privacy.

If you have any questions, please feel free to contact Legislative Counsel Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

¹² Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. Times, Mar. 31, 2012, <http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html>; see also Response to ACLU Public Records Request from the Reno, Nevada, Police Department (Aug. 5, 2011), available at <https://www.aclu.org/cell-phone-location-tracking-documents-nevada?redirect=protecting-civil-liberties-digital-age/cell-phone-location-tracking-documents-nevada#Reno>.

¹³ Devlin Barrett, *U.S. Will Change Stance on Secret Phone Tracking*, W.S.J., May 3, 2015, <http://www.wsj.com/articles/u-s-will-change-stance-on-secret-phone-tracking-1430696796>.

Sincerely,

A handwritten signature in cursive script, appearing to read "Karin Johanson".

Karin Johanson

Director, Washington Legislative Office

A handwritten signature in cursive script, appearing to read "Neema Singh Guliani".

Neema Singh Guliani

Legislative Counsel