November 30, 2015

The Honorable Charles Grassley
Chairman, Committee on the Judiciary

The Honorable Bob Goodlatte
Chairman, Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary

United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

United States House of Representatives
2426 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Grassley, Chairman Goodlatte, Ranking Member Leahy, Ranking Member Conyers, and Members of the Committees:

We, the undersigned, write in support of a simple principle: that law enforcement must convince a judge to issue a warrant before obtaining emails and the contents of other private online communications. This principle, enshrined in the Fourth Amendment — and before that, in the June, 1776 Virginia Declaration of Rights — is the crown jewel of American civil liberties. Yet it is not given effect in the Electronic Communications Privacy Act (ECPA), the 1986 law that governs law enforcement access to digital communications.

For over five years, support has been growing in Congress to reform ECPA to protect Americans' privacy. The Email Privacy Act (H.R. 699), and its Senate counterpart, the ECPA Amendments Act (S. 356), would impose a consistent warrant requirement for stored content. The House bill has the support of 304 Representatives: a veto-proof majority. Such overwhelming support for significant legislation is extraordinary in Congress.

Yet efforts to update the woefully outdated ECPA have stalled due to the stubborn insistence from some regulators that they should be exempt from a warrant requirement. They want to be able to compel a third party that hosts an investigative target's content (e.g., a cloud email provider) to disclose it *without* a warrant based upon a showing of probable cause. This would allow a wide range of regulatory agencies — including the IRS, EPA, SEC, FTC and an endless number of state agencies — to obtain sensitive personal information unrelated to an investigation and protected by privilege since service providers are in no position to assess the relevance of the materials requested or assert privilege (as targets generally do). This could include, for example, personal emails sent on work email addresses. This burden would fall most heavily on the owners and employees of small businesses, who are far more likely to rely on cloud email services (while large companies often host their own email). It is difficult to imagine how Congressional Republicans could consider granting such new power to regulators, given the vast (and increasing) overreach of the regulatory state.

Regardless, there is no need for such a carve-out. Administrative agencies can already serve a subpoena, enforceable in court, and demand production of relevant materials. The courts have regularly compelled individuals and companies to disclose their data and imposed sanctions those who don't comply.

Instead of allowing regulatory agencies to compel email and other cloud service providers to produce private data without a warrant, Congress should codify the trend of courts confronted with such situations: that the *targets* of regulatory investigations themselves remain subject to administrative subpoenas — and if they refuse to comply, they will be subject to appropriate sanctions.[1] This, in turn, will encourage targets' compliance with legitimate requests.

In addition, some law enforcement agencies are calling for an "emergency situation" exception amendment to force service providers to disclose the contents of communications — again, without a warrant. Current law already permits a provider to disclose the contents of a communication or customer records when the provider has a "good faith" belief that disclosure is necessary to avoid the death or serious physical injury of any person.[2] Law enforcement requests the content of communications only sparingly, and providers already comply overwhelmingly.[3]

This exception was written at a time (1986) when courts were frequently unavailable. But today, Article III judges are available around the clock to issue warrants, if only by telephone. So there is no need to bypass the courts. Law enforcement simply has not shown that there

---

1. *See, e.g.*, Mintz v. Mark Bartelstein & Assocs., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Defendants may request documents reflecting the content of Plaintiff's relevant text messages, consistent with the [Stored Communications Act], by serving a request for production of documents on Plaintiff pursuant to Rule 34. … Of course, Plaintiff may raise privacy or other objections to any Rule 34 document request … ."); O'Grady v. Superior Court (Apple Computer, Inc.), 44 Cal. Rptr. 3d 72, 88 (2006) ("Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions.").
2. 18 U.S.C. § 2702(b)(8), (c)(4).
3. In the second half of 2014, for instance, Google received 171 emergency data requests and produced data in 80% of those cases. These emergency requests made up about 1.7% of the total requests Google reported in its latest transparency report, which is available at http://www.google.com/transparencyreport/userdatarequests/US/. Verizon reported receiving 26,237 during the same period, the overwhelming majority of which were for user records and not message content.

is a problem that needs solving. Requiring disclosure in "emergency situations" will incentivize agencies to cry "wolf" in order to avoid judicial oversight.

We would oppose any amendments that would weaken the core privacy protections in this bill. But in particular, any amendment to circumvent the warrant requirement — whether by adding a carve-out for regulatory agencies or turning emergency requests into emergency orders — would likely be a poison pill for ECPA reform in general.

We urge you to finally move forward on bipartisan legislation to reform ECPA — *without these unnecessary and troubling exceptions to warrant protection for Americans' private digital content.*

Respectfully,

TechFreedom
60 Plus Association
American Commitment
American Consumer Institute
Americans for Tax Reform
Center for Financial Privacy and Human Rights
Citizen Outreach
Competitive Enterprise Institute
Council for Citizens Against Government Waste
Digital Liberty
FreedomWorks
Frontiers of Freedom
Heritage Action for America
Institute for Liberty
Institute for Policy Innovation
Less Government
Liberty Coalition
National Taxpayers Union
Niskanen Center
R Street
Taxpayers Protection Alliance
The Rutherford Institute

Bob Barr, Member of Congress, 1995–2003 (GA-7), and President, Liberty Guard*
Bartlett D. Cleland, Madery Bridge Consulting*
Hance Haney, Discovery Institute*
Julian Morris, Reason Foundation*

*Institutional affiliation listed for identification purposes only