April 6, 2011

The Honorable Patrick J. Leahy
Chairman
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Charles E. Grassley
Ranking Member
United States Senate Committee on the Judiciary
152 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Grassley:

As public interest groups dedicated to limited, Constitutional government, we write to urge Congress to extend the Fourth Amendment's protections to Internet-based "cloud" and mobile location services. Specifically, Congress should amend outdated U.S. laws originally intended to protect citizens against unwarranted law enforcement access to their private information held electronically by third parties. The laws protecting such information, while robust at the time of their enactment, have been eroded by technological change. By closing the resulting gaps in legal protection, Congress can restore Americans' individual liberties in the digital age and ensure the Internet remains a powerful engine of economic growth, while preserving the tools needed by law enforcement investigations and removing legal uncertainty that may hamper law enforcement's effectiveness.

Bringing the Fourth Amendment into the Digital Age

Among the chief causes of the American Revolution was widespread outrage at the use of "general warrants" and "writs of assistance" by British officers to conduct searches and seizures without judicial oversight.[1] George Mason's Virginia Declaration of Rights, adopted mere months before the U.S. Declaration of Independence,[2] set forth the basic warrant requirements for lawful searches that were ultimately enshrined in the Fourth Amendment—which protects our "persons, papers and effects" from such arbitrary invasion by requiring law enforcement to obtain warrants issued by a court upon a showing of probable cause.

The Fourth Amendment's protection of the "right of the people to be secure … against unreasonable searches and seizures" is the crown jewel of our constitutional liberties and our greatest bulwark against tyranny. Yet most U.S. courts have declined to extend Fourth Amendment protection to digital "papers" stored with third parties, even those reasonably expected to remain private. In 1986, Congress attempted to fill this gap with the Electronic Communications Privacy Act (ECPA), which remains the primary federal law governing law enforcement access to electronic communications.

For its time, ECPA was a forward-looking, liberty-enhancing statute. But new technologies have changed how individuals and businesses communicate in profound ways unforeseeable in 1986. For example, with storage costs plummeting,[3] more and more sensitive information once stored locally (and protected by the Fourth Amendment) is being stored remotely (where it is only partially protected by ECPA). Mobile phones track users' movement to support a variety of beneficial services and applications—yet under ECPA, this locational data may be obtained by law enforcement without a search warrant.

Congress has tried—unsuccessfully—on several recent occasions to update ECPA to keep pace with technological change. In October 2000, for instance, the Republican-controlled House Judiciary Committee voted 20-1 to approve reforms very similar to what we propose here.[4] Unfortunately, that legislation never made it to a floor vote.

ECPA Reform Would Enhance U.S. Economic Competitiveness

Cloud computing has already been a boon for global commerce and communication.[5] In coming years, this revolutionary shift is expected to generate massive efficiency gains, and cultivate economic growth worldwide.[6] Cloud computing substantially lowers overall IT costs, allows companies to switch from large and infrequent capital expenditures to consistent recurring operating expenditures, and can easily accommodate fluctuations in computing needs.[7] This makes cloud computing especially valuable to start-ups and small businesses—the dynamos of our economy.

But because most information stored with third-party cloud providers often enjoys no Fourth Amendment protection—unlike data stored on first-party (*i.e.*, local) computers[8]—even IT professionals are worried about the privacy of information stored with cloud computing providers,[9] and thus hesitate to embrace cloud computing.

Cloud computing and mobile service providers receive thousands of governmental demands for private user information annually.[10] Despite the sensitive nature of the information sought, many of these demands were made without meaningful judicial review, or any review at all—due to ECPA's inadequate protections.[11]

Protecting Cell Locational Data Will Safeguard Liberty & Foster Burgeoning Mobile Ecosystems

Most smartphones sold today include GPS transceivers and support network-based location (*i.e.*, triangulation by cell towers) when no GPS signal is available. Under ECPA, however, the standards governing law enforcement access to mobile locational information are not explicitly spelled out. Many courts have authorized such demands without requiring a search warrant—contrary to our Fourth Amendment heritage.[12]

Our proposed reforms would not only protect our constitutional liberties, but also promote the growth of the mobile ecosystem. Mobile apps increasingly use location-based functionality to deliver a variety of services to users, from navigation to localized ads to location-based social networking. These services are expected to generate $12.7 billion in revenues by 2014.[13]

ECPA Reform Will Bring Needed Clarity to Law Enforcement Investigations

Law enforcement has effectively fought crime within the constraints of the Fourth Amendment—largely because those constraints are generally clear, predictable and well-understood. By contrast, ECPA's rules governing access to electronic information are a confusing, byzantine mess. Compounding this complexity, a series of conflicting court decisions has resulted in dramatically different standards between jurisdictions for law enforcement demands for electronic information. The resulting legal uncertainty impedes law enforcement efforts and greatly complicates the training of computer crime investigators.[14]

Our proposed ECPA reforms would resolve these ambiguities by creating a single set of nationwide standards that are consistent with the Fourth Amendment. Moreover, unlike ECPA's existing rules, the rules we propose would map readily to cloud and mobile services and reflect users' reasonable privacy expectations in the digital age. Our proposed reforms would not affect the tools used by intelligence agencies and law enforcement authorities to track terrorists and spies.[15]

The Time for Reform is Now

Major decisions regarding the future architecture of cloud computing are being made right now. If Congress fails to enact ECPA reform, cloud computing services may be designed to rely on servers outside the U.S. Not only would this harm U.S. competitiveness, it could also, ironically, deny U.S. law enforcement access to cloud data—even with a lawful warrant.

We urge Congress to act immediately to amend ECPA to extend the Fourth Amendment's protections against the unreasonable search and seizure of digital documents and other electronic information. Specifically, Congress should require that law enforcement:

1. Obtain a search warrant before it can obtain private content stored online;
2. Obtain a search warrant before it can track the location of a mobile communications device;
3. Persuade a court that demands for information about the parties with whom an individual has communicated are relevant and material to a criminal investigation; and
4. Demonstrate to a court that the information it seeks through a bulk data request pertaining to an entire class of users is needed for a criminal investigation.

Indeed, at least one federal appellate court has found a key part of ECPA inconsistent with the Fourth Amendment, just as we argue.[16] By making ECPA consistent with the Fourth Amendment, Congress can avoid protracted litigation in other circuits and clarify proper procedures for law enforcement to obtain access to information with a warrant, just as the Founders intended.

In liberty,

TechFreedom

Competitive Enterprise Institute

Americans for Tax Reform's Digital Liberty Project

FreedomWorks

Campaign for Liberty

Washington Policy Center

Liberty Coalition

Center for Financial Privacy and Human Rights

Less Government

The Committee for Justice

CONTACTS:

Berin Szoka, bszoka@techfreedom.org

Ryan Radia, rradia@cei.org

Kelly Cobb, kcobb@atr.org

[1] Cuddihy, William J. "'A Man's House is His Castle': New Light on an Old Case", review of The Writs of Assistance Case by M. H. Smith. Reviews in American History 7, no. 1 (March 1979), 64–69.
[2] Virginia Bill of Rights, § 10. *available at* http://www.constitution.org/bcp/virg_dor.htm
[3] Chip Walter, *Kryder's Law*, SCIENTIFIC AMERICAN, July 25, 2005, available at http://www.scientificamerican.com/article.cfm?id=kryders-law.
[4] *Cf.* Electronic Communications Privacy Act of 2000**,** H.R. 5018, http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.05018: and Digital Due Process, *Our Principles*, http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163
[5] Gartner, *Gartner Says Cloud Computing Will Be As Influential As E-business*, June 26, 2008, http://www.gartner.com/it/page.jsp?id=707508
[6] IDC, Worldwide and Regional Public IT Cloud Services 2010–2014 Forecast, June 2010, http://www.idc.com/research/viewdocsynopsis.jsp?containerId=223549&sectionId=null&elementId=null&pageType=SYNOPSIS. ("The cloud model will propel IT market growth and expansion for the next 20 years and will help the industry to more rapidly develop and distribute a new generation of killer apps.")
[7] Ben Kepes, Diversity Limited, *Moving your Infrastructure to the Cloud: How to Maximize Benefits and Avoid Pitfalls*, Dec. 20, 2010, http://www.rackspace.com/hosting_knowledge/whitepaper/moving-your-infrastructure-to-the-cloud-how-to-maximize-benefits-and-avoid-pitfalls/.
[8] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, *available at* http://www.minnesotalawreview.org/sites/default/files/Couillard_MLR.pdf.
[9] Andrew R Hickey, Cloud Computing Security Risks Outweigh Benefits: Survey, CRN, Apr. 9, 2010, http://www.crn.com/news/security/224202475/cloud-computing-security-risks-outweigh-benefits-survey.htm ("nearly half of IT professionals in the U.S. say the risk of cloud computing eclipses the perceived benefits")
[10] *See, e.g.*, Google Transparency Report, http://www.google.com/transparencyreport/governmentrequests/ (Noting 4,287 data requests from 1/1/10 to 6/30/10); *see also* Jon Stokes, Sprint fed customer GPS data to cops over 8 million times, ArsTechnica, http://arstechnica.com/telecom/news/2009/12/sprint-fed-customer-gps-data-to-leos-over-8-million-times.ars; *see also* Nick Summers, Walking the Cyberbeat, Newsweek, May 1, 2009, http://www.newsweek.com/2009/04/30/walking-the-cyberbeat.html ("Facebook … says it tends to cooperate fully and, for the most part, users aren't aware of the 10 to 20 police requests the site gets each day.")
[11] Tracy Mitrano, *Taking the Mystique out of the USA-Patriot Act: Information, Process and Protocol*, May 2002, http://www.cit.cornell.edu/policies/esurveillance/article.cfm ("Prior to the Patriot Act, law enforcement required a traditional subpoena in order to acquire 'routing' information, information that by and large is in the realm of telephonic communications and would not require a high level of authorization. Since the Patriot Act, a new method of what some observers have called 'rubber stamp' subpoenas has replaced that traditional authorization standard.").
[12] Orin Kerr, Third Circuit Rules That Magistrate Judges Have Discretion to Reject non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records, Volokh Conspiracy, September 8, 2010, http://volokh.com/category/cell-site-information/. ("The Third Circuit… ruled that… the government can obtain historical cell-site records under 2703(d) without getting a warrant.")
[13] Giselle Tsirulnik, Total mobile LBS revenues to reach $12.7B by 2014, Mobile Marketer, May 20, 2010, http://www.mobilemarketer.com/cms/news/search/6309.html
[14] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); *see also* In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, No. 08-4227 (3d Cir. Sept. 7, 2010).
[15] The Digital Due Process proposals would leave unchanged the Foreign Intelligence Surveillance Act and the amendments to ECPA contained in the USA PATRIOT Act of 2001.
[16] U.S. v. Warshak II at 23, http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf (6th Cir. Dec 14, 2010).