Cybersecurity Amendments Would Modernize 25-Year-Old Privacy Law

by Greg Nojeim [1]
August 1, 2012

[Editors Note: This is one in a of series of blog posts from CDT on the Cybersecurity Act, S. 3414, a bill co-sponsored by Senators Lieberman and Collins that is slated to be considered on the Senate floor soon.]

Two amendments to the Senate cybersecurity bill now being debated would require government agents to get a warrant before reading a person's email or secretly tracking someone through their mobile phone. The amendments, if adopted, would be a huge privacy gain and address a long-standing civil liberties goal of modernizing the Electronic Communications Privacy Act [2], the 25-year old law setting rules for when government agents can access our electronic communications and other private data.
The amendments, one from Senator Leahy [3] and another from Senator Wyden [4], would implement reforms sought by a diverse coalition [5] from across the political spectrum. Supporters [6] include AT&T, Google, the ACLU, Americans for Tax Reform, EFF, and IBM, among others.

Including these reforms in the Cybersecurity Act is appropriate: the information sharing, monitoring and countermeasures provisions of the bill all effectively amend ECPA and the Wiretap Act, permitting companies to share user information notwithstanding privacy protections in those laws. Congress should strengthen the underlying laws to counterbalance these changes.

ECPA Reform Is Long Overdue

The amendments respond to the dramatic technological changes in the 25 years since ECPA became law. Digital communications services are now ubiquitous in modern life. The government has a huge appetite for the data generated when we use the Internet and our mobile phones. Last year, government agencies made over 1.3 million demands [7] for text messages, location data and other information about mobile subscribers alone.

ECPA was forward-looking when adopted. Court decisions of this outdated law now create a crazy patchwork of rules for government collection of communications and location data. This lack of clarity serves no one. It confuses users and law enforcement, as well as the companies in the middle that have to respond to government demands while protecting users. One federal appeals court has held part of the statute unconstitutional.

Leahy Amendment

The Leahy amendment [3] requires government agents to get a search warrant, based on probable cause, before they are allowed access to the content of users' private communications or documents stored "in the cloud," except in some circumstances.

Americans today routinely use some sort of electronic communication for confidential correspondence ranging from business deals to personal letters. Most people save their emails indefinitely, with much of the data stored on the computers of communications service providers. Tens if not hundreds of millions of people store calendars, draft documents, private photos and videos online. Senator Leahy's amendment would eliminate the outdated rule in ECPA that permits the government read someone's stored documents and email without a warrant.

The Leahy amendment also would cure a constitutional defect in ECPA. In December 2010, the Sixth Circuit ruled [8] in *U.S. v. Warshak* that the provision of ECPA allowing the government to access email over 180 days old with a subpoena is unconstitutional. In response, many providers –

including providers in other court circuits – now require a warrant before granting law enforcement access to communications content. By requiring warrants for content, Senator Leahy's amendment would make the law clearly constitutional and put companies and prosecutors back on firm legal footing.

The amendment also modifies the Video Privacy Protection Act to make it easier for online video services to get consent from consumers to share data about movie rentals. A similar tweak [9] was adopted last year in the House of Representatives.

A diverse coalition [10] of groups and companies supports the Leahy amendment.

Wyden Amendment

The cell phones that we carry with us all the time are tracking devices [11]. Even when no call is being made, mobile devices placed in pockets, purses and on night stands constantly signal their location to service providers. The government is increasingly collecting location data from service providers in order to track citizens. GPS is only a part of this invasive surveillance: data indicating which cell towers a device is near at any given time can be readily available to the government.

Senator Wyden's amendment [12] would require a warrant if the government wants to track someone using that person's mobile phone, except in emergencies or when a person calls 911. The amendment mirrors the GPS Act introduced in both the House and the Senate by a bipartisan group [4] of lawmakers, introduced [13] last year. Under Wyden's amendment, the government would need a court-approved warrant, based on probable cause, to obtain information about a person's location that is generated by use of a mobile device such as a cell phone. Similar to Senator Leahy's amendment, Wyden's location amendment would replace complex and constitutionally-suspect rules with a clear warrant requirement.

Senator Wyden's location tracking amendment would also implement a reform supported by [5] companies, trade associations, and groups from across the political spectrum.

-
- privacy
- location data
- gps
- ECPA

Copyright © 2013 by Center for Democracy & Technology.
The content on this website is original to CDT and may be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://cdt.org/blogs/greg-nojeim/0108cybersecurity-amendments-would-modernize-25-year-old-privacy-law

Links:
[1] https://cdt.org/personnel/greg-nojeim
[2] https://www.cdt.org/issue/wiretap-ecpa
[3] https://www.cdt.org/files/pdfs/Leahy-ECPA-Amendment-S3414.pdf
[4] http://www.gpo.gov/fdsys/pkg/BILLS-112s1212is/pdf/BILLS-112s1212is.pdf
[5] http://www.digitaldueprocess.org
[6] http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163
[7] http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2
[8] https://www.cdt.org/blogs/joshua-gruenspecht/courts-boldly-go-fourth-rulings-validate-digital-due-process

[9] https://www.cdt.org/blogs/justin-brookman/712house-tweaks-video-privacy-law-frictionless-sharing
[10] https://www.cdt.org/files/pdfs/ECPA-Letter-Cybersecurity-Legislation.pdf
[11] http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html
[12] http://www.gpo.gov/fdsys/pkg/BILLS-112s3414pcs/pdf/BILLS-112s3414pcs.pdf
[13] https://www.cdt.org/blogs/joshua-gruenspecht/bill-introduced-protect-location-privacy?issue=75