



Written by [Michael Tennant](#) on February 13, 2015

Lawmakers Move to Shield Americans' E-mails From Government Snooping

Remember that e-mail you got from your significant other six months ago — the one you read, replied to, and deleted? Probably not, but if it's still stored on a server somewhere, as it may well be, Uncle Sam thinks it's fair game for his agents' prying eyes — and they don't even need to get a warrant to sneak a peek.

Under the Electronic Communications Privacy Act (ECPA) of 1986, electronic communications left on remote servers — “in the cloud,” in today's parlance — for more than 180 days are considered abandoned and therefore not protected by the Fourth Amendment's requirement that government agents obtain a warrant before searching and seizing them. This might not have been so unreasonable in the era of eight-bit computers and 300-baud modems, when the cost of online time and remote e-mail storage was so high that most messages were downloaded to users' computers for reading and storage. (The government must still get a warrant to search locally stored messages.)



Today, however, the law simply doesn't make sense. Few people download e-mails or other electronic communications, such as text messages or private social-media posts, on a regular basis. Most are stored in the cloud for retrieval whenever, wherever, and by whatever means (desktop or laptop PC, smartphone, tablet, etc.) the parties to the communication desire. It is therefore quite unreasonable to assume that cloud messages over 180 days old have been abandoned and thus can be searched by the government on a whim.

Nevertheless, that is the self-serving way the federal government interprets the ECPA to this day, helped along by the fact that, as CNET's [Declan McCullagh](#) put it, the law “is so notoriously convoluted, it's difficult even for judges to follow.” The judges of the Sixth Circuit Court of Appeals in 2010 ruled that the government has to get a warrant to access e-mails, with the result that some data-storage companies have begun enforcing that rule themselves. But there is no guarantee that another court won't decide differently.

“We believe that it's crucial that such a thin reed not protect some of the most sensitive information we have,” blogged [Chris Calabrese](#), senior policy director for the Center for Democracy and



Written by [Michael Tennant](#) on February 13, 2015

Technology. “After all, privacy in communications is central to our democracy. Journalists need it to talk to their sources, advocates need it to organize protests, and normal folks need the freedom to complain about their government without fear of retribution.”

Fortunately, a significant number of folks in Congress — who might well be on the receiving end of some of those complaints — are trying to secure Americans’ right to electronic privacy, at least to some extent. Senators Mike Lee (R-Utah) and Patrick Leahy (D-Vt.) recently introduced the Electronic Communications Privacy Amendments Act of 2015. Representatives Kevin Yoder (R-Kan.) and Jared Polis (D-Colo.) have introduced companion legislation in the House of Representatives.

“The government is essentially using an arcane loophole to breach the privacy rights of Americans,” Yoder told [McClatchy Washington Bureau](#). “They couldn’t kick down your door and seize the documents on your desk, but they could send a request to Google and ask for all the documents that are in your Gmail account. And I don’t think Americans believe that the Constitution ends with the invention of the Internet.”

The bill would require government agents to obtain a search warrant based on probable cause before rummaging through someone’s e-mail. “Agencies also would have to notify users within three business days of accessing their email or other digital communications, though law enforcement would have 10 days to provide notice,” reported McClatchy. “Courts could grant delays on the notification requirement to prevent the destruction of evidence or intimidation of witnesses, or in cases in which people’s safety was deemed to be at risk.”

“There is no reason we should still be operating under a law written in the analog age when we’re living in a digital world,” Lee said in a [statement](#). “Yet that’s exactly what has happened with the Electronic Communications Privacy Act, which has remained virtually unchanged since it was first enacted in 1986. In the nearly three decades since ECPA became law, technology has advanced rapidly and beyond the imagination of anyone living in 1986. The prevalence of email and the low cost of electronic data storage have made what were once robust protections insufficient to ensure that citizens’ Fourth Amendment rights are adequately protected.”

Similar legislation has been introduced in recent years but stalled. Outrage over the National Security Agency’s spying on Americans, however, may give the 2015 version the boost it needs to become law.

“When I discuss this with constituents at home, they’re frankly stunned to know that in this day and age government still believes they can sift through and spy on Americans’ email correspondence without any sort of due process,” Yoder told McClatchy. “I would say many members of Congress were not aware of this and are becoming aware and the momentum is growing.”

If anything, that’s an understatement. The House version of the bill already has 228 additional cosponsors; the Senate version has nine. The bill also enjoys the support of a wide variety of civil-liberties groups such as the American Civil Liberties Union; think tanks such as the Heritage Foundation; and technology companies such as Amazon, Facebook, and Google.

“Privacy crosses political aisles, especially when we see the government expanding domestic spying in secret in so many different ways,” Lee Tien, a senior staff attorney for the Electronic Frontier Foundation (EFF), told McClatchy.

Still, the bill could be better. In particular, it doesn’t address the issue of government collection of metadata. “Even if the bill becomes law,” noted McClatchy, “customers’ names, locations, addresses, routing information and subscriber network addresses still could be subpoenaed without a warrant and



Written by [Michael Tennant](#) on February 13, 2015

without notice, although accessing the content of their conversations would require the authorization of a judicial magistrate or judge.”

The good news is that even if the bill dies or becomes law in a watered-down form, Americans can still secure their digital privacy to some degree through their state governments. State Senator Mark Leno (D), for instance, has introduced the California Electronic Communications Privacy Act (CalECPA), which would require state law-enforcement officers to get a warrant before searching mobile devices or stored electronic communications.

“States can and should impose stronger privacy protections and CalECPA is exactly that: a comprehensive digital privacy bill that is consistent with the strong protection in the California constitution,” EFF senior staff attorney Hanni Fakhoury told [Sputnik News](#). “CalECPA allows the state to take its digital privacy in its own hands instead of waiting for Congress to act.”

Leno’s bill, too, is supported by a diverse group of organizations and companies and may stand a greater chance of passage than the federal bill, especially given the intense opposition among federal officials, who have warned of the dire consequences of forcing them to abide by the Constitution.

“States may want to protect their citizens more aggressively than a blanket Federal Statute would provide,” Chicago-Kent College of Law legal fellow Adam Rouse told *Sputnik*. “I believe that passage of laws like [CalECPA] are a very big step forward in the fight for freedom from government intrusion on private communications.”



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe