Why Congress Should Pass the ECPA Amendment Act

Thanks to an outdated law, anything stored online for more than 180 days doesn't get the protections of the Fourth Amendment. Congress has the chance to fix the problem, but will it?

By Ben Jacobs, reporter for Newsweek/Daily Beast.

July 30th, 2013

Is Congress about to pass the first significant privacy-protection legislation since 9/11?

Right now if you store any information in "the cloud" for longer than 180 days, the government does not need a warrant to search it, only a subpoena, which does not require judicial approval. This means all those emails in your inbox from last year, the Google Docs that you've been working on for a while, and everything you have saved in your Dropbox are essentially not covered by the Fourth Amendment to the Constitution.

How this is possible? It's because when the law governing this, the Electronic Communications Privacy Act (ECPA), was written in 1986, five years before Tim Berners-Lee had even invented the Internet, and has not been updated since. It was written at a time when no one ever conceived that email or data would be stored online; after all you had to connect via a dial-up modem to get information displayed in one of 16 colors available on your computer monitor. If information was left online for an extended period, it had likely been forgotten or abandoned. But today, the ECPA allows that, in theory, law enforcement need not go through a judge in order to go through your inbox.

The disconnect between statute books and modern life has led to a bipartisan push to update the law. The ECPA Amendment Act, co-sponsored by Sens. Patrick Leahy (D-VT) and Mike Lee (R-UT), would extend the warrant requirement to communications stored online for more than 180 days. The bill is not perceived to be terribly controversial—after all, as one Senate aide points out, it is not intended to radically change the law, but simply to restore the balance that Congress originally intended when it passed ECPA in 1986.

As Julian Sanchez, a research fellow at the Cato Institute, points out, the bill codifies policy that many big Internet companies already follow. "We know Google, Microsoft, and Yahoo are requiring warrants, and the Department of Justice has accepted that." Sanchez warned, though, that "local law enforcement is sometimes getting information from local ISPs with just a

subpoena, and there still may be many cases" where law enforcement is getting emails and other data without a warrant. However, there is no way to tell how often this happens, because there is no requirement for law-enforcement agencies to keep track of and report the number of these subpoenas.

Despite being co-sponsored by a Vermont liberal and a Utah conservative and backed by major tech companies and the Department of Justice, the ECPA amendment's advocates still face an uphill battle. Even if the bill sails through the Senate as expected, it still has to pass the tumultuous House of Representatives. This may be more difficult. So far, the 113th Congress has passed only 22 laws, several of which have simply been renamed bridges or issued commemorative gold coins. One aide on the House Judiciary Committee insisted, "We are working on a bipartisan basis to draft an ECPA reform bill."

Sanchez is optimistic about the ECPA amendment's prospects and insists that its passage is a matter of common sense. "It doesn't matter how long the wire connecting your monitor to your hard drive is," he said. "Your personal files and emails should be protected by Fourth Amendment."