GlobalResearch
Center for Research on Globalization

Responsibility Deflected, the CLOUD Act Passes. Will Erode Privacy Protections Worldwide

Make no mistake—you spoke up. You emailed your representatives. You told them to protect privacy and to reject the CLOUD Act, including any efforts to attach it to must-pass spending bills. You did your part. It is Congressional leadership—negotiating behind closed doors—who failed.

By David Ruiz
Global Research, March 24, 2018
Electronic Frontier Foundation 22 March 2018

Region: USA
Theme: Intelligence, Law and Justice, Police State & Civil Rights

UPDATE, March 23, 2018: President Donald Trump signed the $1.3 trillion government spending bill—which includes the CLOUD Act—into law Friday morning.

"People deserve the right to a better process."

Those are the words of Jim McGovern, representative for Massachusetts and member of the House of Representatives Committee on Rules, when, after 8:00 PM EST on Wednesday, he and his colleagues were handed a 2,232-page bill to review and approve for a floor vote by the next morning.

In the final pages of the bill—meant only to appropriate future government spending—lawmakers snuck in a separate piece of legislation that made no mention of funds, salaries, or budget cuts. Instead, this final, tacked-on piece of legislation will erode privacy protections around the globe.

This bill is the CLOUD Act. It was never reviewed or marked up by any committee in either the House or the Senate. It never received a hearing. It was robbed of a stand-alone floor vote because Congressional leadership decided, behind closed doors, to attach this un-vetted, unrelated data bill to the $1.3 trillion government spending bill. Congress has a professional responsibility to listen to the American people's concerns, to represent their constituents, and to debate the merits and concerns of this proposal amongst themselves, and this week, they failed.

On Thursday, the House approved the omnibus government spending bill, with the CLOUD Act attached, in a 256-167 vote. The Senate followed up late that night with a 65-32 vote in favor. All the bill requires now is the president's signature.

Make no mistake—you spoke up. You emailed your representatives. You told them to protect privacy and to reject the CLOUD Act, including any efforts to attach it to must-pass spending bills. You did your part. It is Congressional leadership—negotiating behind closed doors—who failed.

Because of this failure, U.S. and foreign police will have new mechanisms to seize data

across the globe. Because of this failure, your private emails, your online chats, your Facebook, Google, Flickr photos, your Snapchat videos, your private lives online, your moments shared digitally between only those you trust, will be open to foreign law enforcement without a warrant and with few restrictions on using and sharing your information. Because of this failure, U.S. laws will be bypassed on U.S. soil.

As we wrote before, the CLOUD Act is a far-reaching, privacy-upending piece of legislation that will:

- Enable foreign police to collect and wiretap people's communications from U.S. companies, without obtaining a U.S. warrant.
- Allow foreign nations to demand personal data stored in the United States, without prior review by a judge.
- Allow the U.S. president to enter "executive agreements" that empower police in foreign nations that have weaker privacy laws than the United States to seize data in the United States while ignoring U.S. privacy laws.
- Allow foreign police to collect someone's data without notifying them about it.
- Empower U.S. police to grab any data, regardless if it's a U.S. person's or not, no matter where it is stored.

And, as we wrote before, this is how the CLOUD Act could work in practice:

London investigators want the private Slack messages of a Londoner they suspect of bank fraud. The London police could go directly to Slack, a U.S. company, to request and collect those messages. The London police would not necessarily need prior judicial review for this request. The London police would not be required to notify U.S. law enforcement about this request. The London police would not need a probable cause warrant for this collection.

Predictably, in this request, the London police might also collect Slack messages written by U.S. persons communicating with the Londoner suspected of bank fraud. Those messages could be read, stored, and potentially shared, all without the U.S. person knowing about it. Those messages, if shared with U.S. law enforcement, could be used to criminally charge the U.S. person in a U.S. court, even though a warrant was never issued.

This bill has large privacy implications both in the U.S. and abroad. It was never given the attention it deserved in Congress.

As Rep. McGovern said, the people deserve the right to a better process.

*

Featured image is from the author.

Articles by: David Ruiz