

The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data

BY CAMILLE FISCHER | FEBRUARY 8, 2018



This week, Senators Hatch, Graham, Coons, and Whitehouse introduced a bill that diminishes the data privacy of people around the world.

The Clarifying Overseas Use of Data ([CLOUD](#)) Act expands American and foreign law enforcement’s ability to target and access people’s data across international borders in two ways. First, the bill creates an explicit provision for U.S. law enforcement (from a local police department to federal agents in Immigration and Customs Enforcement) to access “the contents of a wire or electronic communication and any record or other information” about a person regardless of where they live or where that information is located on the globe. In other words, U.S. police could compel a service provider—like Google, Facebook, or Snapchat—to hand over a user’s content and metadata, even if it is stored in a foreign country, without following that foreign country’s privacy laws.[\[1\]](#)

Second, the bill would allow the President to enter into “executive agreements” with foreign governments that would allow each government to acquire users’ data stored in the other country, without following each other’s privacy laws.

For example, because U.S.-based companies host and carry much of the world’s Internet traffic, a foreign country that enters one of these executive agreements with the U.S. to could potentially wiretap people located anywhere on the globe (so long as the target of the wiretap is not a U.S. person or located in the United States) without the procedural safeguards of U.S. law typically given to data stored in the United States, such as a warrant, or even notice to the U.S. government. This is an enormous erosion of current data privacy laws.

This bill would also moot legal proceedings now before the U.S. Supreme Court. In the spring, the Court will decide whether or not current U.S. data privacy laws allow U.S. law enforcement to serve warrants for information stored outside the United States. The case, [United States v. Microsoft](#) (often called “Microsoft Ireland”), also calls into question principles of international law, such as respect for other countries territorial boundaries and their rule of law.

Notably, this bill would expand law enforcement access to private email and other online content, yet the [Email Privacy Act](#), which would create a warrant-for-content requirement, has still not passed the Senate, even though it has enjoyed [unanimous support](#) in the House for the past [two years](#).

The CLOUD Act and the US-UK Agreement

The CLOUD Act’s proposed language is not new. In 2016, the Department of Justice [first proposed](#) legislation that would enable the executive branch to enter into bilateral agreements with foreign governments to allow those foreign governments direct access to U.S. companies and U.S. stored data. Ellen Nakashima at the *Washington Post* [broke](#) the story that these agreements (the first iteration has already been negotiated with the United Kingdom) would enable foreign governments to wiretap any communication in the United States, so long as the target is not a U.S. person. In [2017](#), the Justice Department re-submitted the bill for Congressional review, but added a few changes: this time including broad language to allow the extraterritorial application of U.S. warrants outside the boundaries of the United States.

In September 2017, EFF, with a coalition of 20 other privacy advocates, sent a [letter](#) to Congress opposing the Justice Department’s revamped bill.

The executive agreement language in the CLOUD Act is nearly identical to the language in the DOJ’s 2017 bill. None of [EFF’s concerns](#) have been addressed. The legislation still:

- Includes a weak standard for review that does not rise to the protections of the warrant requirement under the 4th Amendment.
- Fails to require foreign law enforcement to seek individualized and prior judicial review.
- Grants real-time access and interception to foreign law enforcement without requiring the heightened warrant standards that U.S. police have to adhere to under the Wiretap Act.
- Fails to place adequate limits on the category and severity of crimes for this type of agreement.
- Fails to require notice on any level – to the person targeted, to the country where the person resides, and to the country where the data is stored. (Under a separate provision regarding U.S. law enforcement extraterritorial orders, the bill allows companies to give notice to the foreign countries where data is stored, but there is no parallel provision for company-to-country notice when foreign police seek data stored in the United States.)

The CLOUD Act also creates an unfair two-tier system. Foreign nations operating under executive agreements are subject to minimization and sharing rules when handling data belonging to U.S. citizens, lawful permanent residents, and corporations. But these privacy rules do not extend to someone born in another country and living in the United States on a temporary visa or without documentation. This denial of privacy rights is unlike other U.S. privacy laws. For instance, the [Stored Communications Act](#) protects all members of the “public” from the unlawful disclosure of their personal communications.

An Expansion of U.S. Law Enforcement Capabilities

The CLOUD Act would give unlimited jurisdiction to U.S. law enforcement over any data controlled by a service provider, regardless of where the data is stored and who created it. This applies to content, metadata, and subscriber information – meaning private messages and account details could be up for grabs. The breadth of such unilateral extraterritorial access creates a dangerous precedent for other countries who may want to access information stored outside their own borders, including data stored in the United States.

EFF argued on this basis (among others) against unilateral U.S. law enforcement access to cross-border data, in our Supreme Court [amicus brief](#) in the Microsoft Ireland case.

When data crosses international borders, U.S. technology companies can find themselves caught in the middle between the conflicting data laws of different nations: one nation might use its criminal investigation laws to demand data located beyond its borders, yet that same disclosure might violate the data privacy laws of the nation that hosts that data. Thus, U.S. technology companies lobbied for and received provisions in the CLOUD Act allowing them to move to quash or modify U.S. law enforcement orders for extraterritorial data. The tech companies can quash a U.S. order when the order does not target a U.S. person and might conflict with a foreign government’s laws. To do so, the company must object within 14 days, and undergo a complex “comity” analysis – a procedure where a U.S. court must balance the competing interests of the U.S. and foreign governments.

Failure to Support Mutual Assistance

Of course, there is another way to protect technology companies from this dilemma, which would also protect the privacy of technology users around the world: strengthen the existing international system of Mutual Legal Assistance Treaties (MLATs). This system allows police who need data stored abroad to obtain the data through the assistance of the nation that hosts the data. The MLAT system encourages international cooperation.

It also advances data privacy. When foreign police seek data stored in the U.S., the MLAT system requires them to adhere to the Fourth Amendment’s warrant requirements. And when U.S. police seek data stored abroad, it requires them to follow the data privacy rules where the data is stored, which may include important “[necessary and proportionate](#)” standards. Technology users are most protected when police, in the pursuit of cross-border data, must satisfy the privacy standards of both countries.

While there are concerns from law enforcement that the MLAT system has become too slow, those concerns should be addressed with improved resources, training, and streamlining.

The CLOUD Act raises dire implications for the international community, especially as the [Council of Europe](#) is beginning a process to review the MLAT system that has been supported for the last two decades by the Budapest Convention. Although Senator Hatch has in the past introduced [legislation](#) that would support the MLAT system, this new legislation fails to include any provisions that would increase resources for the U.S. Department of Justice to tackle its backlog of MLAT requests, or otherwise improve the MLAT system.

A growing chorus of privacy groups in the United States opposes the CLOUD Act’s broad expansion of U.S. and foreign law enforcement’s unilateral powers over cross-border data. For example, Sharon Bradford Franklin of [OTI](#) (and the former executive director of the U.S. Privacy and Civil Liberties Oversight Board) objects that the CLOUD Act will move law enforcement access capabilities “in the wrong direction, by sacrificing digital rights.” [CDT](#) and [Access Now](#) also oppose the bill.

Sadly, some [major U.S. technology companies](#) and legal scholars support the legislation. But, to set the record straight, the CLOUD Act is not a “[good start](#).” Nor does it do a “[remarkable job](#)” of balancing these interests in ways that promise long-term gains in *both* privacy and security.” Rather, the legislation reduces protections for the personal privacy of technology users in an attempt to mollify tensions between law enforcement and U.S. technology companies.

Legislation to protect the privacy of technology users from government snooping has long been overdue in the United States. But the CLOUD Act does the opposite, and privileges law enforcement at the expense of people’s privacy. EFF strongly opposes the bill. Now is the time to strengthen the MLAT system, not undermine it.

[\[1\]](#) The text of the CLOUD Act does not limit U.S. law enforcement to serving orders on U.S. companies or companies operating in the United States. The Constitution may prevent the assertion of jurisdiction over service providers with little or no nexus to the United States.

RELATED ISSUES:

INTERNATIONAL

LAW ENFORCEMENT ACCESS

RELATED CASES:

IN RE WARRANT FOR MICROSOFT EMAIL STORED IN DUBLIN, IRELAND

TAGS:

PRIVACY

MLAT REFORM

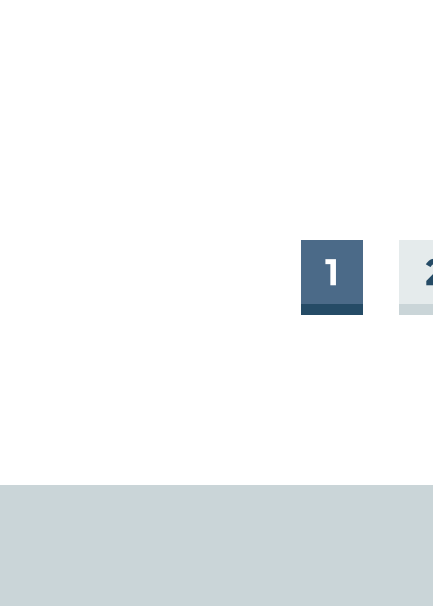
CROSS-BORDER


JOIN EFF LISTS

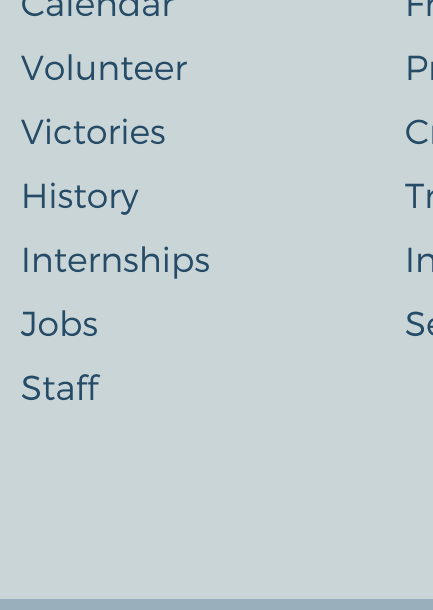
Join Our Newsletter! Email updates on news, actions, events in your area, and more.


SUBMIT

RELATED UPDATES

- 

DEEPLINKS BLOG BY DAVID RUIZ | MARCH 13, 2018
A New Backdoor Around the Fourth Amendment: The CLOUD Act
There’s a new, proposed backdoor to our data, which would bypass our Fourth Amendment protections to communications privacy. It is built into a dangerous bill called the CLOUD Act, which would allow police at home and abroad to seize cross-border data without following the privacy rules where the data is...
- 

DEEPLINKS BLOG BY DAVID RUIZ | MARCH 11, 2018
EFF and 23 Groups Tell Congress to Oppose the CLOUD Act
EFF and 23 other civil liberties organizations sent a letter to Congress urging Members and Senators to oppose the CLOUD Act and any efforts to attach it to other legislation. The CLOUD Act ([S. 2383](#) and [H.R. 4943](#)) is a dangerous bill that would tear away global privacy...
- 

DEEPLINKS BLOG BY JILLIAN C. YORK, KAREN GULLO | MARCH 6, 2018
Offline/Online Project Highlights How the Oppression Marginalized Communities Face in the Real World Follows Them Online
People in marginalized communities who are targets of persecution and violence—from the Rohingya in Burma to Native Americans in North Dakota—are using social media to tell their stories, but finding that their voices are being silenced online. This is the tragic and unjust consequence of content moderation policies...
- 

DEEPLINKS BLOG BY JYOTI PANDAY | FEBRUARY 27, 2018
Can India’s Biometric Identity Program Aadhaar Be Fixed?
The Supreme Court of India has commenced final hearings in the long-standing challenge to India’s massive biometric identity apparatus, Aadhaar. Following last August’s ruling in the Puttaswamy case rejecting the Attorney General’s contention that privacy was not a fundamental right, a five-judge bench is now weighing in on...
-

DEEPLINKS BLOG BY JEREMY MALCOLM | FEBRUARY 13, 2018
How Have Europe’s Upload Filtering and Link Tax Plans Changed?
Although we have been opposing Europe’s misguided link tax and upload filtering proposals ever since they first surfaced in 2016, the proposals haven’t been standing still during all that time. In the back and forth between a multiplicity of different Committees of the European Parliament, and two other institutions...
-

DEEPLINKS BLOG BY CINDY COHN | DECEMBER 22, 2017
What It Means to Fight for Technology Users in 2017
EFF fights for technology users. We believe that empowering and protecting users should be baked into laws, policies, and court decisions, as well as into the technologies themselves. Since our founding in 1990, we have paired this goal with the common-sense recognition that in order to properly consider these questions...
-

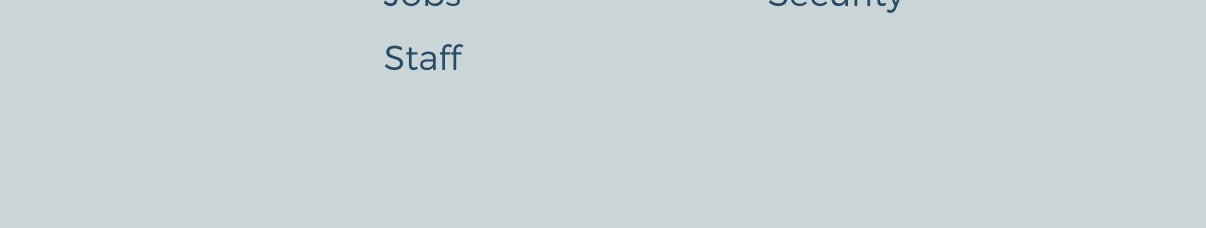
DEEPLINKS BLOG BY JEREMY MALCOLM | NOVEMBER 27, 2017
EFF at Cyberspace Events in Delhi: Protecting the Public Core of the Internet
Last week EFF attended the [Global Conference on Cyberspace](#) (GCCS) in New Delhi, India, as one of a small handful of nonprofit organizations invited to participate. This was the fifth in a series of conferences sometimes called the London Process, after the first event that was held in London...
-

DEEPLINKS BLOG BY JEREMY MALCOLM | NOVEMBER 22, 2017
European Law Claims to Protect Consumers... By Blocking the Web
Last week the European Parliament passed a new [Consumer Protection Regulation](#) [PDF] that allows national consumer authorities to order ISPs, web hosts and domain registries to block or delete websites... all without a court order. The websites targeted are those that allegedly infringe European consumer law. But European consumer...
-

DEEPLINKS BLOG BY JEREMY MALCOLM | OCTOBER 24, 2017
Public Money, Public Code: Show Your Support For Free Software in Europe
The global movement for [open access](#) to publicly-funded research stems from the sensible proposition that if the government has used taxpayers’ money to fund research, the publication of the results of that research should be freely-licensed. Exactly the same rationale underpins the argument that software code that the government...
-

DEEPLINKS BLOG BY JEREMY MALCOLM | OCTOBER 23, 2017
Portugal Bans Use of DRM to Limit Access to Public Domain Works
At EFF, we’ve become all too accustomed to [bad news on copyright coming out of Europe](#), so it’s refreshing to hear that Portugal has recently passed a law on copyright that helps to strike a fairer balance between users and copyright holders on DRM. The law doesn’t abolish legal...

FOLLOW EFF:



CONTACT

General
Legal
Security
Membership
Press

ABOUT

Calendar
Volunteer
Victories
History
Internships
Jobs
Staff

ISSUES

Free Speech
Privacy
Creativity & Innovation
Press Releases
Transparency
International
Security

UPDATES

Blog
Events
Press Materials
Whitepapers

PRESS

Press Contact
Press Materials

DONATE

Join or Renew Membership Online
One-Time Donation Online
Shop
Other Ways to Give