March 12, 2018

Dear Member/Senator,

The undersigned privacy, civil liberties, and human rights organizations strongly oppose S.2383/H.R. 4943, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Some technology companies have suggested that the CLOUD Act represents "notable progress to protect consumers' rights."[1] We disagree. We believe the CLOUD Act undermines privacy and other human rights, as well as important democratic safeguards.

The legislation purports to provide clarity regarding the legal standards that should apply in cases where governments seek data that is not stored within their jurisdiction. Under current U.S. law, such requests for stored information are generally governed by Mutual Legal Assistance Treaties (MLATs), which allow for the exchange of information between the U.S. and foreign governments. The CLOUD Act proposes allowing the U.S. and foreign governments to bypass the MLAT framework.

However, the alternative framework created by the bill fails to protect the rights of Americans and individuals abroad, and would place too much authority in the hands of the executive branch with few mechanisms to prevent abuse. As described in more detail below, among other things, the legislation would:

- **Allow foreign governments to wiretap on U.S. soil under standards that do not comply with U.S. law;**
- **Give the executive branch the power to enter into foreign agreements without Congressional approval;**
- **Possibly facilitate foreign government access to information that is used to commit human rights abuses, like torture; and**
- **Allow foreign governments to obtain information that could pertain to individuals in the U.S. without meeting constitutional standards.**

Foreign Government Requests for Data

Many of the undersigned groups have written previously[2] regarding our concerns with proposals similar to the CLOUD Act, which would allow the executive branch to enter into bilateral agreements with foreign governments to bypass the MLAT process. These agreements would permit foreign governments to obtain wiretaps and stored communications, including those that could contain information about Americans, directly from U.S. technology companies without review by the Department of Justice (DOJ) or approval from a U.S. judge. While this framework creates numerous problems, below are some of our most prominent concerns:

The bill would strip Congress of power and places authority in the hands of the executive branch. Unlike the existing MLAT process, the CLOUD Act would give broad discretion to the Attorney General, with the concurrence of the Secretary of State, to enter into agreements with foreign governments without the advice and

[1] Letter from Apple, Facebook, Google, Microsoft, and Oath to CLOUD Act bill sponsors (Feb. 6, 2018), *available at* https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf

[2] Privacy and Civil Liberties Coalition Letter opposing cross-border legislation (September 20, 2017), *available at* https://www.aclu.org/letter/coalition-letter-opposing-cross-border-data-transfer-proposal

consent of Congress, and would bar judicial or administrative review of their decision. MLAT agreements are generally negotiated by the executive branch and must be approved by a two-thirds vote of the Senate. In contrast, the CLOUD Act would allow the executive branch to enter into agreements with foreign governments—without congressional approval. The bill stipulates that any agreement negotiated would go into effect 90 days after Congress was notified of the certification, unless Congress enacts a joint resolution of disapproval, which would require presidential approval or sufficient votes to overcome a presidential veto.

The bill would give the executive branch discretion to enter into agreements with countries that do not protect human rights, allowing them to obtain sensitive user information without further review by any U.S. government entity. The CLOUD Act would not require that foreign governments meet even vague, malleable standards to request and receive data from U.S. companies. For example, the AG must consider whether, but does not need to affirmatively find that, a country "adheres to applicable human rights obligations" or "demonstrates respect for international human rights." The legislation also would not require that foreign governments obtain *prior* approval from an independent decision-maker when making data requests, nor would they be required to show probable cause. This contrasts with the MLAT process, where foreign government requests are reviewed by the DOJ, and a U.S. judge must find probable cause and may consider human rights impacts.

The bill would permit foreign governments to obtain real-time intercepts (wiretaps) in the U.S. pursuant to standards under which the U.S. government is prohibited from wiretapping. For the first time, this agreement would allow foreign governments to obtain the assistance of U.S. companies for obtaining real-time intercepts of their users' communications. It would do so without requiring foreign governments to adhere to Wiretap Act standards, including notice, probable cause, or set duration limits. This would adversely impact not just non-Americans who may be targeted by wiretaps, but also Americans who are parties to such communications.

The bill would fail to protect the constitutional rights of citizens and others residing inside the U.S. The bill would allow searches and seizures within the U.S. that do not meet the standards set out in the Fourth Amendment. It would also permit foreign governments to share incidentally collected data about Americans with U.S. governmental entities, even when obtained under standards lower than what the Constitution requires. In addition, while the bill states that foreign governments must take steps to minimize the retention of "U.S. persons'" information, these provisions are inadequate because they require only that government policies "meet the definition" of Foreign Intelligence Surveillance Act requirements to the "maximum extent possible." Such language also excludes protections for non-citizens in the U.S. who are not green-card holders.

<u>U.S. Government Requests for Data</u>

The CLOUD Act also proposes permitting the DOJ to obtain data stored abroad without going through the MLAT process. But in doing so, the bill fails to ensure that such requests adequately protect individual rights and some of our most prominent concerns are:

The bill does not specify that the DOJ must obtain a warrant for content or comply with constitutional notice obligations. The CLOUD Act fails to include a warrant-for-content requirement for communications that are over 180 days old. This could open the door to U.S. government demands for this information without meeting constitutional standards. In addition, the bill would not ensure that users whose information is demanded are notified, so that they may challenge improper requests.

The bill may cut off users' ability to intervene in cases where a U.S. government demand does not meet the bill's requirements. The CLOUD Act allows companies to move to quash a disclosure demand in cases where disclosure would violate the laws of the foreign government where the information is located and the US has entered into a data agreement with the foreign government. It makes this motion the exclusive means by which a conflict of laws claim may be raised. This fails to explicitly state that users have standing to raise this claim. In addition, it does not require that a U.S. judge, as a matter of course in all cases, assess whether a demand raises conflict of law concerns.

We urge you to oppose the CLOUD Act, and efforts to attach it to other pieces of legislation.

If you have questions, please contact ACLU Legislative Counsel, Neema Singh Guliani, at 202-675-2322 or nguliani@aclu.org.

Sincerely,

Access Now
Advocacy for Principled Action in Government
American Civil Liberties Union
Amnesty International USA
Asian American Legal Defense and Education Fund (AALDEF)
Campaign for Liberty
Center for Democracy & Technology
CenterLink: The Community of LGBT Centers
Constitutional Alliance
Defending Rights & Dissent
Demand Progress Action
Electronic Frontier Foundation
Equality California
Free Press Action Fund
Government Accountability Project
Government Information Watch
Human Rights Watch
Liberty Coalition
National Association of Criminal Defense Lawyers
National Black Justice Coalition
New America's Open Technology Institute
OpenMedia
People For the American Way
Restore The Fourth