WASHINGTON
LEGISLATIVE OFFICE

March 22, 2018

Dear Representative/Senator,

We anticipate that as early as today Congress will vote on H.R. 1625, the "Consolidated Appropriations Act, 2018," which includes a modified version of the "Clarifying Lawful Overseas Use of Data Act (CLOUD Act)." **The ACLU opposes H.R 1625, and urges you to vote "NO." The ACLU has a number of concerns with the bill, but the CLOUD Act provisions alone pose such a grave threat to civil liberties that they alone are significant enough to warrant a "NO vote."**

The CLOUD Act represents a sea change in our laws governing privacy and electronic data. It threatens human rights, jeopardizes the Fourth Amendment interests of individuals inside the U.S., and provides an alarming level of discretion to the executive branch at the expense of congressional authority. Despite its implications, the CLOUD Act has been the subject of no markups, public hearings, or floor debate. It is alarming that a bill of this magnitude has been tacked onto H.R. 1625 in the eleventh hour.

While there were minor changes to the original version of the CLOUD Act, these amendments fail to address many core concerns. Specifically, among other concerns, the CLOUD Act provisions in H.R. 1625 would:

- grant the executive branch the ability to enter into foreign agreements without congressional approval or other adequate checks to prevent abuse;
- permit foreign governments to obtain information about people in the U.S. without meeting U.S. legal standards, which could then be used by these countries to arrest, detain, or engage in other activities against Americans;
- allow foreign governments to engage in real-time intercepts (wiretaps) on U.S. soil for the first time and under standards that do not comport with the Wiretap Act; and
- eliminate protections that help to prevent U.S. technology companies from providing information to foreign governments that facilitate serious human rights abuses.

The ACLU urges you to vote "NO" on H.R. 1625 because the CLOUD Act provisions jeopardize Americans' privacy, threaten human rights, and grant the executive branch broad discretion with inadequate checks to prevent abuse.

Under current law, foreign government requests to U.S. companies for stored content (i.e. emails, texts, documents, etc.) are generally governed by Mutual

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Legal Assistance Treaties (MLATs), which allow for the exchange of information between the U.S. and foreign governments. MLAT agreements are generally ratified by the Senate, stipulate that foreign government requests must be vetted by the Department of Justice, and require that a U.S. judge issue a warrant based on probable cause before data can be handed over. As part of this process, the DOJ and a U.S. judge can consider human rights concerns and take steps to protect Americans' privacy. Current MLAT agreements do not permit foreign governments to engage in real-time intercepts (wiretaps) on U.S. soil with the assistance of U.S. technology companies.

The CLOUD Act would change current law to (1) allow the executive branch to enter into agreements with foreign government that would permit them to obtain content and wiretaps directly from U.S. technology companies without further review by any U.S. government entity; and (2) clarify that the DOJ can obtain data stored by U.S. technology companies overseas pursuant to U.S. process, which the parties will likely use to claim moots the pending *United States v. Microsoft Corporation* (commonly referred to as the *Microsoft v. Ireland)* case. However, the new framework created by the bill fails to adequately protect the rights of individuals inside and outside the U.S. We urge you to oppose H.R. 1625 because these provisions would:

Grant the executive branch the power to enter into foreign agreements without congressional approval or the opportunity for judicial review. 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 approval from Congress. The bill bars judicial or administrative review of this decision. This contrasts with the current MLAT process, which generally requires that the Senate ratify individual agreements.

Allow foreign governments to engage in wiretaps on U.S. soil for the first time and without meeting the requirements of the Wiretap Act. The bill would allow foreign governments to go directly to U.S. providers and obtain assistance with wiretaps without adhering to Wiretap Act standards such as 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.

Permit foreign governments to use "incidentally" collected information of people in the U.S. to prosecute, arrest, or take other actions against Americans. The bill allows foreign governments to eavesdrop and collect stored communications, which may contain the sensitive information of individuals in the U.S. in communication with foreigners. The bill does not bar foreign governments from using such information to prosecute, arrest, or take action against Americans, even in cases where such actions are unrelated to the direct purpose for which the information was collected.

Create a new backdoor that permits foreign governments to share information about Americans collected under standards lower than what the Constitution requires. The bill permits broad information sharing between the U.S. and foreign governments, extending far beyond cases where such information is necessary to protect life or safety. This information sharing would

provide the U.S. government ample opportunity to obtain information about Americans and others while evading the requirements of the Fourth Amendment.

Fail to ensure that the executive branch does not enter into agreements with countries that commit human rights abuses. The human rights standards that countries must meet to be eligible for an agreement are vague, weak, and unclear. For example, among other concerns, the bill does not explicitly prohibit agreements with countries that have a pattern or practice of engaging in human rights violations, nor does it require an assessment of whether a country has effective control of intelligence or law enforcement units. In addition, the bill states that countries must respect "universal international human rights", without definition or clarity regarding how to assess this (this is not a recognized term in U.S. or international law). Moreover, it states that countries must protect freedom of expression, without stating whether free expression is defined under U.S. law, international law, or a country's own domestic law. Such ambiguity is particularly concerning given that the bill eliminates any further vetting of requests by a US government entity.

Does not clarify that DOJ must obtain a warrant for content or comply with constitutional notice obligations when seeking data stored overseas by U.S. companies. 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.

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

Sincerely,

Faiz Shakir
National Political Director

Neema Singh Guliani
Legislative Counsel