September 20, 2017

Dear Member/Senator:

The undersigned organizations, which are dedicated to protecting privacy, civil liberties and human rights, write to outline our serious concerns regarding proposed legislation that would provide a new process for cross-border access by foreign governments to electronic communications and related data held in the United States. We urge you to oppose this legislation in its current form if it is introduced as either a stand-alone bill or as part of another legislative vehicle. We would appreciate the opportunity to discuss how best to improve the current cross-border process in a rights-protective manner.

At present, when a foreign government seeks to obtain electronic communications content held in the United States by U.S. service providers, they generally follow a process laid out in a "mutual legal assistance treaty" (MLAT) between that country and the United States. Under an MLAT, individual requests for the content of communications are evaluated by the U.S. government, and if the required standards are met, the U.S. Department of Justice (DOJ) will seek an order from a U.S. court to provide the content of communications to the foreign country. Importantly, through this review process, the DOJ and U.S. judges take additional steps to protect the rights of individuals in the United States and abroad, including requiring the minimization of data, ensuring the request does not violate the Constitution and will not cause serious human rights violations, and evaluating whether responding to the request is consistent with U.S. treaty obligations.

The current MLAT process is time consuming, and the U.S. government and foreign governments have argued that a less cumbersome procedure is needed. But rather than improve or devote more resources to the MLAT process, the proposed legislation would empower certain foreign governments to bypass it. Specifically, it would amend U.S. law to permit U.S. communications providers to respond directly to foreign government requests for stored data, and would even allow companies to conduct wiretaps (i.e. collect data in real time) for foreign governments, something that the current MLAT process does not allow. In doing so, the proposed bill eliminates many key safeguards provided under current law that protect the rights of individuals inside and outside the United States. For example, the new approach eliminates the individualized review presently conducted by the U.S. government to ensure that requests for data are not likely to be used to commit serious human rights violations. Thus, without significant amendments, this legislation poses threats to privacy, civil liberties, and human rights.

Our principal concerns with the proposed legislation are as follows:

Provides broad discretion to the Executive Branch to enter into agreements without appropriate oversight: The bill gives the Executive Branch broad discretion to enter into bilateral agreements with other countries without appropriate congressional involvement. Under

the current proposal, Congress would not need to approve, ratify, or otherwise endorse such agreements and there is no mechanism for Congress to review implementation of such agreements . Instead, similar to extradition treaties, the bill should require that Congress ratify each individual bilateral agreement, and review such agreements on a periodic basis to determine whether they should be extended. Further, the bill bars any judicial or administrative review of whether the approval requirements were met. Such unilateral power in the hands of the executive branch without congressional or judicial oversight is a recipe for arbitrariness or decisions based on political factors that do not take adequate account of the rights of people inside or outside the United States.

Allows foreign governments to obtain U.S. held data under a weak standard: The bill only requires that the order by the foreign government be based "on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation." This is a lower standard than the U.S. probable cause standard that applies to foreign requests for the content of communications under current law, impacting both the non-U.S. persons who may be targets of the foreign government requests and U.S. persons whose information may be incidentally collected. This standard may also be insufficient to meet the requirements of international human rights law. In addition, although the bill includes language stating that orders must "identify a specific person, account, address, or personal device, or any other specific identifier as the object of the Order," this language is insufficient to prevent large-scale collection. For example, an "address" could be an IP address, which can cover numerous computers, or it could include an entire apartment building.

Does not adequately protect the rights of people in the United States: Although foreign governments would not be permitted to use this cross-border process to target U.S. persons (i.e., citizens and legal permanent residents) or individuals located inside the United States, they would still be likely to obtain the communications of Americans who were in contact with foreign targets through "incidental collection." In some cases, foreign governments could then voluntarily share such information about U.S. persons with the U.S. government, even though it was collected without the safeguards that would otherwise apply under the Fourth Amendment and the Wiretap Act. Specifically, foreign governments could share any metadata for Americans' communications (such as the "to" and "from" lines of an email) with the U.S. government. Additionally, they could share the content of U.S. persons' communications if the foreign government believes the information "relates to significant harm, or the threat thereof, to the United States or U.S. persons," which is a standard lower than what would be required for the U.S. government to obtain the information on its own. Moreover, since the bill also permits foreign governments to voluntarily share collected U.S. person communications with third-party governments in certain situations, including those that do not meet baseline human rights standards, it further threatens the rights of people in the United States.

No requirement for prior individualized and independent review: Prior individualized review by an independent decisionmaker is a fundamental protection under the U.S. system of justice and under international human rights law. However, the bill only requires "review *or oversight* by a court, judge, magistrate, or other independent authority." By permitting foreign countries to

rely only on "oversight" which may be generalized, the system fails to require both the prior individualized and independent review necessary to protect individuals inside and outside the United States.

Permits real-time or prospective surveillance for the first time and without adequate safeguards: Under current law, U.S. providers may only turn over stored -- and not real-time -- content to foreign governments through the MLAT process, and when the U.S. government conducts real time or prospective surveillance, the Wiretap Act provides additional safeguards beyond those required for access to stored content. The bill, however, would permit foreign governments, for the first time, to issue orders for U.S. providers to turn over the content of communications in real time without including protections comparable to those contained in the Wiretap Act.

Fails to prevent data localization mandates or requirements for encryption back doors: The bill does not include any language to prohibit foreign countries from requiring that U.S. communications providers store their data in that country (data localization). Although efforts by countries with strong data privacy requirements to apply those protections to data held by U.S. providers may be helpful, rules that simply require data to be stored in a specific country can impede the free flow of information on the internet. Nor does the bill bar foreign countries from requiring U.S. communications providers to create back doors to circumvent encryption. The bill thus fails to protect against many of the threats that the government has suggested it is intended to forestall.

Fails to require review and establish standards for disclosure of sensitive metadata: Under current law, although foreign government requests for communications *content* are subject to the rights-protective MLAT process, U.S. providers may voluntarily turn over communications *metadata* based simply upon a request from a foreign government. This is true even for particularly sensitive metadata, such as email logs and other traffic data. In fact, it is often easier for foreign governments to obtain metadata from U.S. providers than it is for the U.S. government to do so. Any legislation governing cross-border data requests should include a requirement that foreign government requests for sensitive metadata must be subject to prior independent review, and should establish a meaningful standard for that review. The bill, however, fails to address this problem.

Does not appropriately limit the types of crimes that may justify a foreign government data request: The bill applies to data requests in connection with the prevention, detection, investigation, and prosecution of "serious crime, including terrorism," but it does not list, define, or otherwise limit the "serious crimes" that are covered. Further, unlike the current MLAT requirements, the bill fails to include a dual criminality requirement to ensure that data requests to U.S. providers would only cover the types of crimes that U.S. law also recognizes as serious criminal behavior. The bill thereby creates risks that U.S. providers will be called upon to assist in investigations and prosecutions that violate human rights and civil liberties.

Fails to ensure that the U.S. government only enters into agreements with foreign governments that meet strong human rights standards: The bill establishes requirements for the U.S. Attorney General, with the concurrence of the U.S. Secretary of State, to approve individual bilateral agreements with foreign governments under which they may seek the contents of communications directly from U.S. communications providers. However, the provisions for U.S. executive branch review and approval of such bilateral agreements only specify "factors to be considered" rather than making the listed factors mandatory for approval. For example, it should be mandatory (and not simply a factor to consider) that countries can only be approved where they adhere to applicable international human rights obligations and commitments, so that there can be no approvals for countries that the State Department has assessed to have committed serious human rights violations.

Fails to ensure notice to targets and others. The bill fails to require notice -- even after the fact -- to the target of a data request, or others whose communications will inevitably be "incidentally" collected. Yet notice is a key human rights protection that gives targets and others an opportunity to ask a court to vindicate their rights and seek redress where abuses occur. The bill does not even require notice to the U.S. government when a foreign government demands data stored in the United States from a U.S. company, to allow the U.S. government to recognize any patterns of abuse.

For these reasons, without significant amendments to the bill, we urge you to oppose this legislation. We would welcome the opportunity to meet with you to discuss how to address the government's concerns in a rights protective manner.

Sincerely,

Access Now
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
Amnesty International
Center for Democracy and Technology
Center for Media and Democracy
Constitutional Alliance
Council on American-Islamic Relations
Defending Rights & Dissent
Demand Progress
Electronic Frontier Foundation
Fight for the Future
Government Accountability Project
Government Information Watch
Human Rights Watch
National Association of Criminal Defense Lawyers
National Security Counselors
New America's Open Technology Institute
Project On Government Oversight
Restore The Fourth