

August 9, 2016

The Honorable Charles Grassley  
Chairman, Senate Judiciary Committee  
U.S. Senate  
Washington, D.C. 20510

The Honorable Bob Goodlatte  
Chairman, House Judiciary Committee  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Patrick Leahy  
Ranking Member, Senate Judiciary Committee  
U.S. Senate  
Washington, D.C. 20510

The Honorable John Conyers, Jr.  
Ranking Member, House Judiciary Committee  
U.S. House of Representatives  
Washington, DC 20515

**RE: Department of Justice Proposal on Cross Border Data Sharing, Amending the Electronic Communications Privacy Act and the Wiretap Act.**

Dear Chairman Grassley, Chairman Goodlatte, Ranking Member Leahy, and Ranking Member Conyers:

The ACLU, Amnesty International USA, and Human Rights Watch strongly urge you to oppose legislation proposed by the Department of Justice (DOJ), transmitted to Congress on July 15, 2016, which would weaken privacy protections contained in the Electronic Communications Privacy Act (ECPA) and Wiretap Act.<sup>1</sup> We would oppose such legislation as a stand-alone bill. In addition, we would oppose H.R. 699<sup>2</sup>, the Email Privacy Act (passed by the House 419-0), if it is amended, as the DOJ suggests, to include such a proposal.

The proposed legislation would largely supplant the existing process for cross-border data requests and, in doing so, jettison the existing privacy protections they offer both for Americans and foreigners. Currently, for example, when the UK government is investigating a domestic crime and wants the content information such as an email, it generally follows a process laid out in an agreement between the United States and United Kingdom, called a “mutual legal assistance treaty” (MLAT). Under the MLAT, the UK government may submit its request to the U.S. DOJ, which, after reviewing the request and ensuring it complies with the MLAT’s requirements, would then seek an order from a U.S. court for the content.<sup>3</sup> The United States has similar arrangements with other foreign governments.

---

<sup>1</sup> Letter from Peter J. Kadzik, Assistant Attn’y Gen., U.S. Dpt. Of Justice, to the Hon. Joseph R. Biden, President, U.S. Senate (July 15, 2016), *available at* <https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4>. [hereinafter “DOJ Proposal”].

<sup>2</sup> The ACLU supported H.R. 699, though preferred prior versions of the legislation.

<sup>3</sup> Mutual Legal Assistance, U.S.-U.K, Jan 6, 1994, T.I.A.S 96-1202, *available at* <https://fas.org/irp/world/uk/us-uk-mla.pdf>. For more information on MLATs, see also, *Mutual Legal Assistance Treaties*, <https://mlat.info/> (last visited July 27, 2016).

Under the proposed legislation,<sup>4</sup> however, ECPA and the Wiretap Act would be amended to grant the Executive Branch broad discretion to enter into agreements with foreign countries that would allow those countries to request stored data and real-time communications directly from U.S. providers in cases involving undefined “serious” crimes. Under such agreements, foreign governments would be permitted to obtain communications without satisfying a probable cause standard, obtaining prior authorization from a judge or other independent and impartial tribunal, or, in the case of real-time interception, satisfying the requirements of the Wiretap Act. While the legislation prohibits the targeting of U.S. persons,<sup>5</sup> it permits foreign governments to collect communications involving U.S. persons or other third country nationals. The U.S. government is already negotiating one such agreement with the United Kingdom,<sup>6</sup> which is expected to serve as a template for similar agreements with other countries.

The ACLU, Amnesty International USA, and Human Rights Watch urge you to oppose the DOJ proposal for the following reasons, including:

**The proposed legislation permits foreign governments to acquire the content of stored communications of Americans and foreigners without a warrant.**

Under the current MLAT process, a judge in the U.S. must issue a warrant based on probable cause in order for a U.S. company to turn over content to a foreign government. This ensures that Americans’ communications with foreign targets are not handed over to foreign governments without meeting the same protections afforded by the U.S. Constitution. In addition, the requirement protects individuals abroad—who may live in countries with weak privacy and human rights protections—by requiring foreign governments to meet certain standards when seeking information held by U.S. companies.

The agreements permitted by the proposed legislation would remove the essential safeguard provided by the existing U.S. requirement for a judicial warrant. In addition, they would not require sufficiently robust safeguards in the requesting state, a flaw which further exacerbates the problems posed by the removal of the fundamental function played by the U.S. judge. Indeed, among other deficiencies, the legislation does not require that requests from foreign governments are based on a prior judicial authorization. For example, in the UK, a Secretary of State—a senior government minister who is not independent from requesting agencies—can approve an order to request content. While the proposed legislation requires foreign governments to conduct independent oversight of its data requests, an after-the-fact “review” is no substitute for *prior* authorization by an independent judicial body. Ex post facto scrutiny cannot entirely cure a rights violation that has already been committed.

Also, the legislation does not require that requests from foreign governments meet a probable cause standard. Instead, it only requires that orders be based on “articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.” Such a standard is ambiguous at best, given that it is not tied to an existing body of case law and would likely be interpreted differently based on a country’s specific domestic precedent. More likely, in certain cases, it would be weaker than the

---

<sup>4</sup> DOJ Proposal, *supra* note 1.

<sup>5</sup> *Id.* at §4.

<sup>6</sup> Ellen Nakashima & Andrea Peterson, *The British Want to Come to America—With Wiretap Orders and Search Warrants*, WASH. POST, Feb. 14, 2016, [https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9\\_story.html](https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html).

probable cause standard under the Fourth Amendment, which requires a reasonable basis to believe that the *specific information sought* is contraband or evidence of a crime. Thus, the DOJ is asking Congress to pass legislation to allow foreign governments to obtain content under a standard that would be unconstitutional and unlawful if adopted by the U.S. government itself.

**The proposed legislation would allow foreign governments to request that U.S. companies assist in real-time surveillance for the first time and without meeting the standards in the Wiretap Act.**

ECPA does not permit any government—including the United States—to compel providers to disclose communications in real time. Instead, when the U.S. government wants to conduct real-time surveillance, it must comply with the Wiretap Act, which imposes heightened privacy protections. Under the Wiretap Act, the government must demonstrate to a judge that there is probable cause to believe that its target has committed a serious crime and other investigative procedures have been exhausted.<sup>7</sup> In addition, the government must minimize the interception of irrelevant communications, and, within 90 days of concluding the surveillance, provide notification to the target and, if a court deems it to be in the interest of justice, any other party surveilled.<sup>8</sup> The Wiretap Act also permits individuals to seek remedies and damages in cases where they have been surveilled in violation of the statute.<sup>9</sup>

The proposed legislation would, for the first time, allow foreign governments to request assistance from U.S. providers to intercept communications in real-time—and it would do so without requiring compliance with Wiretap Act standards. For example, the proposal does not require that foreign governments obtain an order from a judge authorizing real-time interception, demonstrate probable cause to believe that an individual has committed or is about to commit certain serious offenses, give notice to the target of surveillance (or Americans and foreigners who are parties to such communications), provide damages when an individual is unlawfully surveilled, or provide an avenue to prevent use of unlawfully obtained information in criminal proceedings. Thus, the agreement would allow foreign governments to request the types of real-time interception on U.S. soil that the U.S. government itself is prohibited from engaging in.

**The proposed legislation's information sharing provisions provide an end-run around the protections of the Fourth Amendment and Wiretap Act.**

The DOJ proposal prohibits foreign governments from requesting information on behalf of, or for the purpose of providing information to the U.S. government. However, once foreign governments have collected information, the proposal permits them to voluntarily funnel that information back to the U.S. government or other third parties. Such information may then be used as evidence in criminal or other legal proceedings, circumventing the requirements of the Fourth Amendment and Wiretap Act. Indeed, it stretches credulity to think that such disclosures would not be made, given that the U.S. has a series of reciprocal information sharing agreements with the UK and numerous other foreign partners. Moreover, the proposal permits the country receiving the information from the U.S. to then disclose it to other countries, posing a host of additional security and human rights concerns for both Americans and foreigners.

---

<sup>7</sup> 18 U.S.C. 2518

<sup>8</sup> 18 U.S.C. 2518

<sup>9</sup> 18 U.S.C. 2520

**The proposed legislation grants the executive branch broad discretion, without adequate oversight, to enter into bilateral agreements that weaken privacy protections for Americans and foreigners.**

The proposal would give the Executive Branch the discretion to enter into a bilateral agreement with any country whom the Attorney General, with the concurrence of the Secretary of State, certifies as providing “robust substantive and procedural protections for privacy and civil liberties.” However, the proposal fails to set out a list of criteria for such a determination, instead merely offering a list of potential “factors to be considered.”<sup>10</sup> For example, under the DOJ proposal, whether a country “demonstrates respect for the rule of law and principles of non-discrimination” is simply a “factor” rather than a requirement.<sup>11</sup> Thus, it permits the government to enter into agreement with governments that the State Department has found to have a mixed record on human rights issues.

Moreover, the DOJ proposal fails to ensure that such designations are not arbitrary or the result of political influence. For example, the proposal explicitly states that such certification is not subject to judicial or administrative review, and the proposal does not require congressional approval. As a result, under the proposed legislation, there would be little recourse in cases where the Executive Branch’s determination differs from that of human rights experts, members of Congress, or international bodies. Indeed, past country designations by the Executive Branch have been strongly criticized for failing to accurately reflect actual country practices, being subject to political influence, and lacking appropriate transparency. For example, the U.S. government has provided millions of dollars in military assistance to foreign governments such as Mexico and Colombia following human rights vetting of security forces despite evidence of continued human rights violations.<sup>12</sup> Likewise, the Executive Branch has authorized arms sales to foreign governments such as Saudi Arabia despite evidence of dozens of unlawful airstrikes in Yemen that have killed hundreds of civilians, and a 2014 Presidential Policy Directive requiring human rights abuses be assessed in arms sales.<sup>13</sup>

**The proposed legislation weakens existing privacy protections by eliminating individualized review of information requests.**

Under the DOJ proposal, the Executive Branch would consider whether a foreign country meets certain baseline standards related to the rule of law and human rights. However, such a country-wide assessment will inevitably be inadequate. It is not enough that a country, as a whole, is deemed to be generally in

---

<sup>10</sup> DOJ Proposal, *supra* note 1 at §4.

<sup>11</sup> *Id.* at §4(a).

<sup>12</sup> See, Press Release, Amnesty International USA, Human Rights Groups Call on U.S. to Withhold Aid to Mexican Military, (July 21, 2016), *available at* <http://www.amnestyusa.org/news/press-releases/human-rights-groups-call-on-us-to-withhold-aid-to-mexican-military>; Amnesty International, *2015/16 Annual Report (Colombia)*, <https://www.amnesty.org/en/countries/americas/colombia/report-colombia/>, (last visited July 27, 2016). See also, U.S. DEPT. OF STATE, MEXICO 2015 HUMAN RIGHTS REPORT (2015), *available at* <http://www.state.gov/documents/organization/253239.pdf>; U.S. DEPT. OF STATE, COLOMBIA 2015 HUMAN RIGHTS REPORT (2015), *available at* <http://www.state.gov/documents/organization/253213.pdf>.

<sup>13</sup> See Press Release, Human Rights Watch, Suspend Saudi Arabia from the UN Human Rights Council, (June 29, 2016), *available at* <https://www.hrw.org/news/2016/06/29/suspend-saudi-arabia-un-human-rights-council>; Press Release, Amnesty International USA, President Obama Must Cancel 1.29b Arms Deal with Saudi Arabia, (Dec. 10, 2015), *available at* <https://www.amnestyusa.org/news/press-releases/president-obama-must-cancel-129b-arms-deal-with-saudi-arabia>; See also U.S. DEPT. OF STATE, SAUDI ARABIA 2015 HUMAN RIGHTS REPORT (2015), *available at* <http://www.state.gov/documents/organization/253157.pdf>; U.S. State Dept., *Conventional Arms Transfer (CAT) Policy*, <https://www.state.gov/t/pm/rsat/c14023.htm> (last visited, July 27, 2016).

compliance with human-rights standards. The Attorney General and Secretary of State might conclude that India, for example, satisfies human-rights standards in some broad and nebulous sense; yet an investigation conducted while a suspect is held in “preventive detention” might violate, for instance, the suspect’s fair-trial rights, or an order subject to the agreement may be based on information obtained by torture.<sup>14</sup> Before the U.S. government permits tech companies to hand over sensitive and private data to foreign countries, it must ensure that *each request* is lawful and consistent with human rights protections. It is inappropriate and inadequate to delegate this task to private companies, which, in addition, may not have the incentive or expertise to conduct robust individual reviews since they will have broad liability protection if they have acted in good faith reliance on a foreign order.<sup>15</sup>

**The proposed legislation contains inadequate oversight to ensure that technology companies are only turning over information that is consistent with the terms of a particular agreement.**

Technology companies vary widely in the expertise and resources they have to devote to processing government requests for information. Yet, the DOJ proposal provides virtually no oversight to ensure that technology companies are only turning over information permitted in a specific agreement. For example, under the proposed legislation, a bilateral agreement may permit disclosure of information only in response to orders that do not infringe on freedom of speech. However, the legislation does not require that individual companies have appropriate processes to weed out requests that may infringe on speech rights; nor are there periodic audits to ensure that companies are properly responding to foreign government information requests.

In addition, while the proposed legislation indicates that foreign governments must agree to “periodic review of its compliance with the terms of its agreement by the United States government,” it does not provide details of what such reviews must include or who will conduct them. Congress should be skeptical of DOJ promises to ensure compliance given its history of failing to conduct appropriate audits and assessments required by law. For example, despite testifying to Congress that the FBI’s facial recognition database would be subject to strict audits, the GAO found that the Department has yet to conduct even one audit and failed to conduct timely privacy assessments required by law.<sup>16</sup>

**The proposed legislation would permit information disclosures that do not meet human rights standards.**

Under international human rights law, governments can conduct surveillance only when: based on individualized and sufficient suspicion; authorized by an independent and impartial decision-maker; necessary and proportionate to achieve a legitimate aim, including by being the least intrusive means possible.<sup>17</sup> In addition, individuals must receive notice of surveillance as soon as doing so would no

---

<sup>14</sup> HUMAN RIGHTS WATCH, *BROKEN SYSTEM: DYSFUNCTION, ABUSE, AND IMPUNITY IN THE INDIAN POLICE* (2009), available at <https://www.hrw.org/report/2009/08/04/broken-system/dysfunction-abuse-and-impunity-indian-police> (reporting systematic and widespread use of torture by Indian police, despite procedures mandated by Indian Supreme Court, Indian law and India’s human rights treaty obligations).

<sup>15</sup> DOJ Proposal, *supra* note 1 at §3.

<sup>16</sup> GOV’T ACCOUNTABILITY OFF., *FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY* (2016), available at <http://www.gao.gov/assets/680/677098.pdf>.

<sup>17</sup> Article 17 of the International Covenant on Civil and Political Rights, which was ratified by the United States in 1992, has been interpreted to incorporate these protections. *See e.g.* International Covenant on Civil and Political Rights, art. 17, Dec. 19, 1966, U.N.T.S 999.

longer jeopardize the lawful investigation, and have access to meaningful and effective remedies to seek and obtain redress for rights violations. The DOJ proposal fails to require that orders issued by foreign governments comply with these and other human rights standards or make compliance with these standards a pre-requisite for entering into an agreement with the United States.

\* \* \*

We urge Congress to reject efforts to move the proposed legislation as a stand-alone bill or, as the DOJ has proposed, as an amendment to the ECPA reform bill. In addition, should Congress explore avenues to address concerns with the existing MLAT process, we urge you to include standards governing the disclosure of metadata by providers as part of any such proposal. Currently, such disclosure lacks clear requirements, sufficient oversight, and appropriate transparency.

If you have any questions, please feel free to contact Legislative Counsel Neema Singh Guliani at 202-675-2322 or [nguliani@aclu.org](mailto:nguliani@aclu.org).

Sincerely,



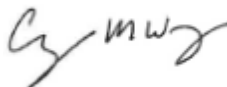
**Karin Johanson**  
Director, Washington Legislative  
Office  
American Civil Liberties Union



**Naureen Shah**  
Director, Security with Human Rights  
Amnesty International USA



**Neema Singh Guliani**  
Legislative Counsel  
American Civil Liberties Union



**Cynthia M. Wong**  
Senior Internet Researcher  
Human Rights Watch