CENTER FOR DEMOCRACY & TECHNOLOGY

Cross-Border Law Enforcement Demands:
Analysis of the US Department of Justice's Proposed Bill

August 17, 2016

I. Summary

On July 15, the U.S. Department of Justice proposed legislation[1] that would permit foreign governments hand-picked by DOJ to conduct wiretapping in the U.S. for the first time, and to do so without a court order based on probable cause of crime. Billed as legislation that would fix the current Mutual Legal Assistance Treaty (MLAT) process for cross-border disclosure of stored communications content, the legislation goes significantly beyond MLATs to authorize real-time surveillance, as well. If enacted in its current form, the legislation would herald a worldwide diminution of communications privacy rights as strong U.S. protections of probable cause and a judicial warrant or court order for disclosure of communications content are effectively swapped out for less privacy protective laws of countries with which the DOJ strikes a deal. The legislation would implement a bi-lateral agreement the DOJ has already negotiated with the United Kingdom, the current text of which has not been publicly released.

That said, the existing U.S. system for cross-border law enforcement demands for users' internet content is not meeting the legitimate law enforcement needs of foreign countries. It moves too slowly to keep up with crime conducted over the internet. As a result, it subjects people worldwide to crimes that could be solved or prevented with a more efficient system. Governments around the world will not tolerate the protracted delays in the current system, and are increasingly resorting to extra-territorial warrants and data localization mandates that can effectively eliminate protections that foreign nationals now enjoy under U.S. law. Bilateral cross-border law enforcement demands (C-BLED) agreements such as those contemplated in the legislation the DOJ has proposed could be part of the solution if limited to stored content and metadata, and if based on strong human rights standards. However, legislation to clear the way for such agreements must be preceded by enactment of Electronic Communications Privacy Act (ECPA) reform legislation such as the Email Privacy Act (H.R. 699 in the 114th Congress) and must also close a gap in current U.S. law that permits U.S. providers to voluntarily disclose their users' traffic data to foreign governments.

While we oppose the DOJ proposal, we believe that bilateral agreements could be a viable mechanism for partially addressing the problem of cross-border law enforcement demands.

---

[1] Letter, Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the United States Senate, July 15, 2015 (conveying proposed legislation and a section-by-section analysis). http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

II. The Current Problems and Protections

When considering the issue of cross-border data flows, there are really two separate processes that help illustrate both the protections and problems at issue. The first process covers the disclosure of *content.* It is strict and requires a foreign government to enlist the assistance of DOJ to gain for it the issuance of a U.S. warrant by a U.S. judge. This is true even though criminal conduct may have no tie to the United States other than that the communications content needed to solve the crime is located in the United States or held by a U.S. provider. The second type of process is for the disclosure of *metadata*. There is no standard for disclosure of metadata to foreign governments under U.S. law. As such, U.S. providers can volunteer it to any foreign government that asks for it, even if the metadata pertains to the communications of a U.S. citizen or lawful permanent resident (U.S. person).

Disclosure of Communications Content

When an official outside the United States is investigating a crime over which he or she purports to have jurisdiction, internet communications relevant to that crime are often stored by U.S. providers, such as Google and Facebook, in the United States. Sometimes the communications are stored in third countries, sometimes they are stored in both the United States and in third countries, and sometimes they are stored in many countries at the same time. U.S. law, ECPA, as interpreted by the courts, by U.S. providers, and by the U.S. Department of Justice, permits the provider to disclose communications content only in certain circumstances, including when a U.S. governmental entity obtains a judicial warrant under U.S. law, based on a finding of probable cause of crime, compelling the provider to make the disclosure.

For a foreign government to secure such disclosure—even in a wholly domestic case, where the crime, victim, and perpetrator are all in the same country—that country must file a request for mutual legal assistance under an MLAT treaty or other process. The Department of Justice's Office of International Affairs works with the foreign government to amass the information necessary to make the probable cause showing in court. This process takes an average of 10 months.[2]

A primary reason why the MLAT process moves so slowly is that foreign governments' MLAT requests often fail to include sufficient facts to establish probable cause. Sometimes this happens because such facts do not exist. Sometimes this happens because foreign governments that can access communications at a lower standard under their own laws do not include such facts in their requests, though they possess the necessary information. The U.S. probable cause requirement thus provides a level of privacy protection that is not available under the law of the requesting country. This protection applies regardless of the nationality or location of the person whose data are sought. That is, non-U.S. persons outside the United States benefit from this privacy protection even if their only tie to the United States is that they have chosen to use a U.S. communications service provider. While requirements for demonstrating probable cause vary among U.S. courts, the probable cause standard is widely regarded in the United States as an exacting requirement. It provides a high level of privacy

[2] President's Review Group, "Liberty and Security In a Changing World," (December 12, 2013), p. 227. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

protection both because of the level of proof required to meet the standard and because a neutral and detached magistrate decides whether the proof meets the standard.

In other words, a significant cause of the frustration to the investigator or prosecutor in the requesting country seeking communications content is the operation of this strong human rights and civil liberties protection in the United States.

Disclosure of Communications Metadata

There is a second problem as well - foreign law enforcement demands for disclosure of metadata are treated differently from demands for content disclosure under ECPA. While ECPA generally bars communications service providers from disclosing communications *content* to *anyone* unless a U.S. judge issues a warrant based on probable cause, it permits providers to voluntarily disclose *metadata* to any foreign government that asks for it.[3]

Consequently, foreign governments who seek metadata disclosure from U.S. providers often do not have to file requests for mutual legal assistance. Because federal law permits voluntary disclosure, the U.S. government may never even learn that a metadata demand was made; U.S. law permits the provider to volunteer it. In fact, under ECPA, foreign governments enjoy easier access to metadata of both Americans and of non-U.S. persons than does the U.S. government itself.[4]

III. Overview of the DOJ's Proposed Solution

The Department of Justice has proposed legislation that would ignore the problem of disclosure of metadata to foreign governments without standards, remove the requirement of a U.S. judicial warrant based on a finding of probable cause for the disclosure of certain communications content to certain countries, and permit those countries to, for the first time, engage in wiretapping in the United States. Foreign governments who benefit from such an agreement would be barred from targeting people known to be U.S. persons or persons located in the United States. However, there is no mechanism in the bill to enforce this prohibition by preventing this surveillance up front. The United States government would not even know that this was occurring unless tipped off by a U.S. provider, but this is not a reliable protection. Providers of electronic communications service seldom know their users' country of citizenship and often have imperfect information about their location.

Under the DOJ proposal, the foreign government would make its surveillance demands directly to U.S. providers, and would make those demands under its own domestic procedures and standards. The

[3] Although ECPA bars U.S. service providers from voluntarily disclosing metadata to "governmental entities" (18 U.S.C. Section 2702(c)(6)), the Act defines governmental entity to include only U.S. federal, state and local government agencies (18 U.S.C. Section 2711(4)). This definition does not include foreign governments. Therefore, U.S. communication service providers are permitted to voluntarily disclose user metadata—be it of a U.S. or non-U.S. person—to other governments.

[4] U.S. providers can voluntarily disclose metadata to foreign governments upon request. However, they are permitted to disclose traffic data (such as email logs) to the U.S. government only when it has a warrant, or a court order issued under 18 U.S.C. Section 2703(d). For subscriber information, such as a person's email address, the minimum required legal authority is a subpoena.

DOJ, with the concurrence of the U.S. State Department, would decide the countries with which the DOJ would enter into a bilateral agreement permitting these direct demands. The U.S. Senate, which under current law must approve any MLAT treaty by a two-thirds vote, would have no role in deciding whether such an agreement should be entered into.[5] Though the House and Senate judiciary and foreign relations committees would receive 60 days' notice of the DOJ's intention to enter into a particular agreement, they would have no role in approving it. The DOJ's determination would be based on information that it does not publish and its determination would not be subject to judicial or other review.

The DOJ proposal goes well beyond the current issues with the disclosure of stored communications content under the MLAT system. It would permit foreign governments to issue orders for real-time interception as well – wiretapping of both phone calls[6] and IP-based communications of non-U.S. persons outside the U.S. – without the knowledge or participation of the U.S. government, and without many of the protections that apply when U.S. governmental entities engage in wiretapping. While wiretapping orders issued by the foreign government must be for a "fixed, limited duration," and "must last no longer than is reasonably necessary to accomplish the approved purposes of the order," no upper limit on duration is established. (Under U.S. law, a wiretap order can last no longer than 30 days, and is renewable only in 30-day increments. In practice, the average wiretap in the U.S. lasted 43 days in 2015 and 34 days in 2014.)[7] There would be no requirement to show probable cause or to obtain an order from a U.S. judge.

The DOJ proposal could also operate as an end run around the probable cause requirement that protects people in the United States and U.S. persons. Under the proposal, foreign governments can share with the U.S. government the product of the surveillance they conduct in the United States even though that surveillance was conducted without meeting the probable cause requirement. That surveillance product could be shared if it is merely "relevant" to prevention, detection, investigation, or prosecution of a serious crime. Foreign governments with which the United States enters into an agreement would not be permitted to serve orders on U.S. providers that intentionally "target" U.S.

---

[5] According to the U.S. Department of State, the United States has MLAT agreements with 63 countries. http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/253357.htm. Each is subject to a requirement of the advice and consent of the U.S. Senate and none can enter into force except with a two-thirds vote of the U.S. Senate. The United States also has mutual legal assistance executive agreements with five countries: Singapore, Taiwan, Hong Kong, Russia and China. Based on their surveillance laws and human rights records, none of these five countries is a likely candidate for a cross-border law enforcement demands agreement. This suggests that if this legislation is enacted, the Senate's advice and consent role would be diminished with respect to permitting disclosure of communications content to foreign governments.

[6] The scope of telephonic wiretapping that could be conducted under the DOJ proposal is unclear. The foreign government would not be allowed to target a person in the United States. It appears, therefore, that the foreign government would not be able to serve an order on a U.S. wireless provider to compel the disclosure in real time of one of its customer's cell phone calls made or received in the United States. Ninety-six per cent of the wiretapping now conducted in the United States targets cell phone conversations, text messages and mobile apps. In 2015, there were only 32 wiretaps for electronic communications. Administrative Office of the United States Courts, *Wiretap Report*, 2015. http://www.uscourts.gov/statistics-reports/wiretap-report-2015. (*Wiretap Report, 2015*).

[7] *Wiretap Report, 2015.*

persons (to "target" is undefined) or a person located in the U.S. However, if that targeted person talks to or about a U.S. person or a person located in the U.S. in a manner that incriminates, the conversation can be shared.

IV. Key Features of the DOJ Proposal

Which Countries Could Benefit from a C-BLED Agreement?

The DOJ's proposed legislation would permit C-BLED agreements only with countries that "afford[] robust substantive and procedural protections for privacy and civil liberties. . . ." as shown by:

- Demonstrated respect for the rule of law and principles of non-discrimination;
- Adherence to international human rights obligations, including protection from arbitrary and unlawful interference with privacy, fair trial rights, freedom of expression, association and peaceful assembly, prohibitions on arbitrary arrest and detention, and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment;
- Clear legal procedures governing the entities authorized to seek data;
- Mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and
- Demonstrated commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the internet.

Unfortunately, these are only "factors" DOJ would consider; they are not requirements. As a result, DOJ could, for example, determine that because a country scored well on other "factors," that it was appropriate for the United States to enter into a C-BLED agreement with a country that engages in torture. This would be permissible even if DOJ could reasonably anticipate that the product of surveillance conducted in the United States would be used in connection with torture.

Each of these "factors" should be sharpened and clarified, and be made into "requirements" to preclude such results.

As requirements, they would be important protections if supplemented with a proper mechanism for ensuring that each requirement was met. Unfortunately, the bill includes no such mechanism. The DOJ, with the concurrence of the Department of State, determines whether each is met, does so based on information that is not available to the public, does so without the advice and consent of the U.S. Senate, and their decision cannot be reviewed in any judicial or administrative proceeding. It seems likely that the pressures of other U.S. foreign policy interests would unjustly weigh in this decision.

Requirements of Foreign Government's Orders

In addition to the factors DOJ and the State Department must consider in their assessment of the foreign government's laws and practices, the bill also imposes important requirements on the orders that would be issued by the foreign government to the U.S. provider pursuant to the bilateral treaty. In effect, this part of the bill establishes standards for C-BLED agreements. The orders:

- May be issued only for criminal purposes – intelligence surveillance orders are not permitted;

- May be issued only for investigation of "serious" crimes, but "serious" is left undefined;
- Must identify as the object of the order "a specific person, account, address, or personal device, or any other specific identifier" – no bulk collection orders are permitted;
- "[M]ay not be used to infringe on freedom of speech" – an important concept, but a concept interpreted differently by different countries. The U.S. tends to have stronger free speech protections than do other countries, many of which criminalize blasphemy, hate speech and "glorification of terrorism." The bill leaves unclear which standard would apply.

Moreover, the DOJ proposal contemplates service on U.S. providers of surveillance "orders" issued by foreign governments, not by foreign courts. As discussed later, authorization by a court or other independent tribunal should be a pre-requisite of any order issued under one of these agreements. That court order would then be served on the U.S. provider by a central authority in the foreign government.

V. Big Picture Changes Required

In the next section, we recommend a number of particularized changes to the DOJ proposal to bring it more in line with human rights requirements. In this section we recommend "big picture" changes to the DOJ proposal that would make it more acceptable as a starting place for addressing cross-border law enforcement demands.

Warrants for Content

Ironically, U.S. law would fail the test that the bill would establish for the laws of a foreign country seeking a bilateral agreement with the U.S. for the disclosure of communications content. The bill would require that content disclosure orders issued by the foreign government be subject to review or oversight by a judge or another independent authority. ECPA does not impose such a requirement. Instead, it permits law enforcement to use a subpoena to compel disclosure of communications content that is more than 180 days old held by an electronic communications service provider, such as an ISP. It permits use of a subpoena to compel disclosure of communications content no matter its age if it is held by a remote computing service – such as the content of one's documents, diaries, and photos stored on-line. No legislation should move forward without addressing this obsolete portion of U.S. law. Specifically, stored communications content should be accessible to a governmental entity in the U.S. only when it obtains a warrant. The E-mail Privacy Act (H.R. 699 in the 114th Congress), passed by a 419-0 vote in the House of Representatives, would establish this rule.

Wiretapping

Foreign governments should not be authorized to conduct wiretapping in the U.S. Real-time surveillance has traditionally been regarded as much more invasive than compelled disclosure of stored communications. That is why the Wiretap Act requires a "super warrant" for real time surveillance. Such surveillance can be authorized only in increments of 30 days, can be authorized only for specified crimes (not for all felonies or other "serious" crime) and can be authorized only when other investigative techniques have been tried and have failed, or reasonably appear to be unlikely to

succeed.[8] None of these protections appear in the DOJ proposal. Moreover, giving wiretapping authority in the U.S. to foreign governments goes well beyond fixing the MLAT system; it amounts to an expansion of surveillance. Finally, proponents of this power will argue that it is needed to respond to terrorist attacks as they unfold. And yet, wiretapping is already authorized in the U.S., including for crimes of terrorism, and is used overwhelmingly for drug crimes, not for terrorism.[9] Section 3(a) of the bill should be deleted.

Establishing a Credible Designation Process

Whether a foreign government's laws and practices afford sufficient substantive and procedural protections under the DOJ proposal should be based on whether a series of requirements are met, not on mere "factors" to consider. DOJ, with State Department concurrence, cannot be the sole deciders; their decisions would be driven by political and other factors, not by an objective application of the requirements in the legislation. DOJ and the State Department should, though, play an important role in the decision-making process.

First, DOJ's determination (with the concurrence of the State Department) to certify a country for a C-BLED agreement should be made subject to the notice and comment procedures of the Administrative Procedures Act.[10] The DOJ should be required to give public notice in the Federal Register of its intention to enter into an agreement that would permit a particular foreign government to serve demands for stored communications content directly on U.S. providers. It should be required to prepare a public report that states the factual basis for the proposed determination that the foreign country meets each of the requirements for such agreements set forth in the legislation. The Federal Register notice would request comment from the public as to whether the criteria have been met. Human rights experts both in and outside the U.S. would have a chance to participate by providing information about the country's human rights practices and surveillance activities that DOJ may lack and that may cast doubt on whether those practices meet the requirements in the bill. DOJ would then be obligated to respond to those comments in a final notice that would indicate whether it would move forward with an agreement, and if so, the features of the agreement that the United States would demand in order to accommodate the human rights concerns raised in the comments it received. Court review under the deferential "*Chevron*"[11] standard would be available to ensure that DOJ's determination to move forward with an agreement was lawful and not "arbitrary and capricious."

Second, the Senate's advice and consent should be required, just as it is required of Mutual Legal Assistance Treaties. This may also serve as a check against misuse of this new authority. It would subject the C-BLED to public review by another branch of government. While the Senate is influenced by political considerations (and properly so), those considerations are perhaps different than those at play at the DOJ and in the executive branch of government.

---

[8] 18 U.S.C. Sections 2516-2518.

[9] In 2015, 79% of wiretaps in state and federal investigations were installed in drug investigations. In 2014, 89% of those wiretaps were installed in drug investigations. *Wiretap Report, 2015.*

[10] 5 U.S.C. Section 553.

[11] *Chevron v. Natural Resources Defense Council, Inc.,* 467 U.S. 837 (1984).

Metadata Standards

ECPA should be amended to establish standards for disclosure of the most sensitive metadata – traffic data, such as email logs – to foreign governments. Right now, that data can be disclosed voluntarily to any foreign government that asks for it, posing an enormous risk to user privacy. Traffic data can reveal one's interests, medical conditions, associations, and location over time. It is absurd to have no standard for foreign governments while requiring a court order based on specific and articulable facts for U.S. government access. Ideally, an amendment to ECPA would apply this court order requirement to all such disclosures to foreign governments. The legislation would then carve out an exception for governments with which the United States enters into a C-BLEDs agreement. In those cases, the disclosure would be made under the agreement pursuant to the laws of the country seeking the data, with similar (but not necessarily identical) requirements for the disclosure of content. This would incent more countries to seek such agreements and raise their own standards.

Alternatively, if this is viewed as too disruptive (because it would add to the number of requests subject to the MLAT process), a more limited approach would be for Congress to impose a standard for traffic data disclosure for countries with which the U.S. enters into an agreement, permitting such disclosures under the laws of the country seeking the disclosure, provided those laws meet the standard. Congress could also call on providers to establish "best practices" through a multistakeholder process for their disclosure of traffic data to foreign governments with which there were no C-BLED agreements.

Encryption and the Scope of Provider Assistance

Like the United States, many governments require communications service providers to assist with governmental surveillance. This is appropriate because many kinds of surveillance could not be conducted without such assistance and surveillance can be conducted with assistance much more efficiently, and without physical coercion. On the other hand, the scope of compelled provider assistance varies from country to country. The scope of permissible provider assistance orders should be set forth in the legislation to ensure that the U.S. does not enter into agreements with foreign governments that would impose overly broad provider assistance mandates.

Decryption mandates are one illustration of this problem. There is a robust debate in the United Kingdom right now about whether pending legislation, the Investigatory Powers Bill, would authorize orders ("Technical Capability Notices") that require providers to decrypt communications carried over their services. They would have to provide this form of assistance when it is "reasonably practicable" for them to do so. With respect to services encrypted end-to-end (only the sender and recipient have the keys), when it is "reasonably practicable" will vary according to the circumstances, said Lord Howe, speaking for the government as the legislation moved through the House of Lords.[12] New services might be particularly vulnerable; it may be more "reasonably practicable" to require that a new service permit only communications that the provider can decrypt, in lieu of offering a service encrypted end-

[12] *See,* Natasha Lomas, *UK Surveillance Bill Includes Powers To Limit End-To-End Encryption,* TechCrunch, July 15, 2016, https://techcrunch.com/2016/07/15/uk-surveillance-bill-includes-powers-to-limit-end-to-end-encryption/.

to-end. Communications encrypted end-to-end are much less susceptible to subversion by criminal hackers and rights-abusing foreign governments than are other communications.

The legislation should be amended to ensure that bilateral agreements that are entered into bar surveillance demands with provider assistance mandates that go beyond the level of assistance providers must afford under current U.S. law. This will help ensure that the outcome of the debate about encryption backdoors for law enforcement access now raging in the U.S. is not prejudiced by accommodations demanded of U.S. providers under a bilateral agreement.

Reciprocity Provisions

The bill contemplates C-BLED agreements that are reciprocal, meaning the U.S. would obtain the same authority to make surveillance demands on foreign providers that the foreign government could make on U.S. providers. However, the bill includes no provisions to operationalize these reciprocal demands by the U.S. government. Without them, it would not appear that U.S. law imposes any standards at all on the surveillance demands the U.S. would make of foreign providers, and it does not appear that there would be a specific statutory authority to make any such demands in the first place. Our understanding had been that such demands by the U.S. government for content held by foreign providers would be conditioned on law enforcement entities obtaining a warrant under U.S. law. However, there is no provision in U.S. law – or in the proposed bill – that would permit a U.S. court to issue such a warrant with extraterritorial effect, and the Second Circuit's 2016 Microsoft-Ireland decision[13] indicates that such warrants, if issued, would have no extraterritorial effect.

Reciprocity with clear rules will be extremely important to international acceptance of such agreements. Not only should U.S. law require that the United States will seek content held by foreign providers only pursuant to a warrant, but it should also make it clear that the warrant requirement will not be circumvented by intelligence surveillance conducted under much weaker standards. Surveillance conducted using a warrant will collect the identifiers of foreign communicants with a foreign criminal surveillance target. Under the DOJ proposal, the government could then use those identifiers to conduct warrantless intelligence surveillance. It could, for example, use the email addresses it collects using a warrant as "selectors" for intelligence surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA). [14] That surveillance requires no judicial authorization and no finding of probable cause. The reciprocity rules governing criminal surveillance pursuant to a C-BLED agreement should prevent this result.

[13] *Microsoft v. U.S.,* (2d Cir. 2016), http://www.ca2.uscourts.gov/decisions/isysquery/04aa4a95-3a3d-4ea4-b7c5-83fd9cc1367c/1/doc/14-2985_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/04aa4a95-3a3d-4ea4-b7c5-83fd9cc1367c/1/hilite/. *See also,* Jadzia Butler, *The Microsoft Ireland Case: A Clear Answer, an Uncertain Future,* Center for Democracy & Technology, July 18, 2016. https://cdt.org/blog/the-microsoft-ireland-case-a-clear-answer-an-uncertain-future/.

[14] 50 U.S.C. Section 1881a. https://www.law.cornell.edu/uscode/text/50/1881a.

VI. The Specifics of What Must Be Changed

In addition to the big picture changes mentioned above, certain changes to the text of the legislation are essential:

Judicial Authorization

Any legislation to clear the way for C-BLED agreements should require that a judicial or other independent tribunal authorize surveillance conducted pursuant to the agreement. The DOJ proposal does not require this. It contemplates "orders" issued by foreign governments, not by foreign courts. The orders would have to be subject to oversight by an independent authority. This after-the-fact possibility of independent review is entirely inadequate and would mark a dramatic elimination of a key civil liberties protection in U.S. law that is afforded people outside the United States. It appears to be an effort to accommodate current British law, which permits a government official – the Home Secretary – to issue "interception warrants" to obtain both stored and real time communications, and allows for a deferential review by the Investigatory Powers Tribunal. Moreover, the kind of very limited oversight that the U.S. FISA Court has over surveillance conducted under FISA Section 702 would meet the test in the DOJ proposal: intelligence officials often claim that the FISA Court "oversees" this surveillance[15] even though it does not authorize surveillance of particular targets. It merely approves guidelines.

Evidentiary Standard

The DOJ's proposed bill would substitute a weak, vague standard for the strong probable cause standard that must now be met in the MLAT process for cross-border law enforcement demands. Instead of probable cause, foreign law would have to require "a reasonable justification based on articulable and credible facts, particularity, legality and severity regarding the conduct under investigation." DOJ could interpret that standard quite flexibly, and reach findings that even weak evidentiary standards suffice. This too would mark a dramatic elimination of a key civil liberties protection in U.S. law. Any legislation to clear the way for C-BLED agreements should require that judicial orders for surveillance be based on a strong factual basis for the belief that a serious crime has been, is being, or will be committed, and a strong factual basis for the belief that information relevant to the crime would be obtained by the surveillance.

"Serious" Crime Definition

Legislation clearing the way for C-BLED agreements should define the crimes for which disclosure of content may be sought. The DOJ proposal requires that surveillance be conducted only for "serious" crimes, leaving "serious" undefined. This leaves to the vagaries of foreign law the types of crimes for which surveillance orders could be served on U.S. providers.[16] Under U.K. law, a "serious crime" is one

---

[15] *See, e.g.,* Letter, Robert S. Litt, General Counsel, Office of the Director of National Intelligence, to Justin S. Antonipillai, Counselor, U.S. Department of Commerce and Mr. Ted Dean, Deputy Assistant Secretary to the U.S. International Trade Administration, February 22, 2016 (attached as Annex VI to the E.U.-U.S. Privacy Shield Agreement). http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

[16] U.S. law has a number of definitions of "serious" crime. Under the immigration code, it includes reckless driving that results in personal injury. 8 USC 1101(h).

for which the period of incarceration may be at least three years for an adult with no previous convictions, a crime involving violence or that results in substantial financial gain, or a crime conducted by a large number of people acting with a common purpose.[17] ECPA permits the disclosure of communications content for the investigation of any felony, defined to include any crime punishable by a sentence of one year or more. The Wiretap Act includes a list of crimes (some serious, some not so serious) for which a wiretap order can be sought. We suggest that cross-border law enforcement demands under a C-BLED agreement be limited to crimes for which the minimum period of imprisonment is three years or more, or that involve violence, risk of serious bodily harm or death, sexual assault, human trafficking, or crimes against children, including child pornography.

Requirements of Foreign Law

As indicated above, each of the "factors" that would be considered in determining whether to enter into a C-BLED agreement with another country should be sharpened and should become a "requirement." In particular, a finding should be required that the country with which an agreement would be struck does not engage in torture or cruel, inhuman, or degrading treatment or punishment, prohibits arbitrary arrest and detention, provides fair trial rights, freedom of expression, association and peaceful assembly, and protects against the arbitrary and unlawful interference with privacy. Rather than merely "demonstrate respect for the rule of law and principles of non-discrimination" as suggested in the DOJ legislation, any legislation to authorize C-BLED agreements should prohibit agreements with countries that show a pattern of discrimination or of conduct inconsistent with the rule of law.

In addition, the legislation should give countries an incentive to abandon data localization mandates and extraterritorial warrants – the very real threats that DOJ cites as reasons to address the cross-border law enforcement demands problem. It should include an exclusivity clause making it clear that any warrants seeking data from U.S. providers outside the territory of the issuing country will be issued only pursuant to the agreement. It should bar agreements with countries whose laws indicate that providers must localize data within the country.

Freedom of Speech and Dual Criminality

As indicated earlier, the DOJ bill would require that orders issued under a C-BLED agreement "may not be used to infringe on freedom of speech," but does not indicate under which country's law "infringement" will be tested. Rather than try to resolve this issue directly, a better approach would be for C-BLED agreements to adopt the dual criminality requirement that pertains in U.S. law today. Under that requirement, a crime for which a warrant would be sought in the U.S. under an MLAT must involve conduct that, if committed in the U.S., would be a felony under federal or state law.[18]

[17] The Regulation of Investigatory Powers Act (RIPA) 2000, Section 81(3). http://www.legislation.gov.uk/ukpga/2000/23/contents.

[18] 18 U.S.C. Section 3512(e).

Surveillance Involving Americans

The DOJ's proposed legislation does not authorize U.S. providers to disclose communications content pursuant to orders that target U.S. persons or persons located in the United States. The legislation should define what "targeting" means. The legislation also leaves entirely to the foreign government the discretion to adopt procedures designed to meet this requirement. More importantly, even when an American is not the target of surveillance, the foreign government will collect the American's communications with targets. Those communications can then be volunteered to the U.S. government even though the U.S. warrant requirement was never met. This creates the possibility of an end run around the warrant requirement even when the U.S. is not asking the foreign government to conduct surveillance of a U.S. person or a person located in the U.S. To prevent this circumvention, any U.S. prosecution based on this type of evidence must disclose that fact to the defendant. A judge should be authorized to suppress that evidence if there is a basis to believe it was collected as part of an effort to circumvent U.S. privacy protections.

Notice

The DOJ proposal does not require that the target of the foreign government's surveillance receive notice, even if provided after the fact. This should change to require notice, which could be delayed in limited circumstances to protect the investigation or prevent risk of flight or serious bodily harm.[19]

VII. Bilateral Agreements Are Superior to Other Proposals

While the DOJ proposal has significant problems as is discussed above, it proposes an approach for cross-border law enforcement demands for users' communications that is superior to many of the alternatives. It is superior to the use of extraterritorial warrants, through which one country asserts the authority to compel disclosure of communications content in another country without that country's consent. Extraterritorial warrants could be a privacy nightmare because they compel disclosure under authorization statutes that provide only weak privacy protection. Moreover, they put providers in an untenable situation where they violate one country's law if they make a disclosure mandated by another country's law and legal process.

C-BLED agreements are superior to the approach taken in the International Communications Privacy Act (ICPA, S. 2986 and H.R. 5323 in the 114th Congress). ICPA authorizes U.S. courts to issue extraterritorial warrants to compel disclosure of communications content stored outside the United States without the consent of the country in which the content is stored when the content is stored in an account of: (i) a U.S. person, (ii) a person located in the United States, (iii) a person of undetermined nationality; (iv) a person of undetermined location, (v) a person who is a national of a country with which the United States has no MLAT or other Law Enforcement Cooperation Agreement;

[19] U.S. law requires notice to the target of a wiretap, to other parties to the wiretap "in the interests of justice," and to persons whose stored communications content is disclosed pursuant to a wiretap or a court order issued under 18 U.S.C. Section 2703(d). U.S. law does not require notice to a person whose stored communications content is disclosed pursuant to a warrant. 18 U.S.C. Section 2703(b)(1).

and (vi) a person who is located in a country with which the U.S. has no MLAT or other Law Enforcement Cooperation Agreement. If the approach taken in ICPA was adopted worldwide, any country could issue legal process with extraterritorial effect under that country's standards (whatever they may be) to compel disclosure of information stored in the United States when in the account of one of its nationals (even that of a dissident national of a repressive regime taking refuge in the U.S.) and in other circumstances.

C-BLED agreements are superior to forced data localization, through which a country compels providers to locate data servers within its territory so the data are subject to compelled disclosure under local law. Data localization mandates can fragment the global internet. They stymie the development of start-up entities because they lack the resources to localize data in many jurisdictions in which they might have users, and they can prevent potential users in a country with a localization mandate from gaining access to new and useful information services.

A multilateral treaty might be preferable to bilateral C-BLED agreements because it would allow for the setting of strong, internationally acceptable standards. However, negotiating such a treaty would take many years and might be impossible. The problem of cross-border law enforcement demands will need to be addressed before such an agreement could be reached.

Reforms to the MLAT process, such as those in Section 4 of ICPA, could be put in place. They would, for example, require DOJ to develop a standardized, online form for submitting MLAT requests and require DOJ to establish a docketing system for such requests. However, they amount to a Band-Aid on a gaping wound that needs a major intervention: even with MLAT reform, there will continue to be a strong need for timely reform of C-BLED processes. The MLAT system won't scale to meet the demands that will be put on it.

VIII. Conclusion

Bilateral agreements may be part of the solution to the problem of cross-border law enforcement demands. However, the DOJ proposal should be rejected because it lacks adequate protections. Congress could consider C-BLED legislation that takes an approach more respective of human rights and civil liberties of people in the U.S. and abroad.

[For more information, contact Greg Nojeim (gnojeim@cdt.org), Director, Freedom, Security and Technology Project at the Center for Democracy & Technology]