WHEN OTHER GOVERNMENTS WANT YOUR STUFF: RULES OF THE ROAD FOR CROSS-BORDER LAW ENFORCEMENT DEMANDS

Greg Nojeim*

CITE AS: 1 GEO. L. TECH. REV. 130 (2016)
https://perma.cc/UU63-YN59

This year marks the twenty-fifth anniversary of the public gaining access to the World Wide Web.[1] To say communications have come a long way since then would be quite the understatement. Today, billions of people around the world can be reached in seconds—a far cry from the time when email was only common among academics, government workers, and military personnel. Global connectivity can advance freedom, prosperity, and innovation, but it has also presented extraordinary challenges and opportunities for law enforcement. A prime example is digital evidence located overseas.

Before the internet, law enforcement officials investigating a crime rarely had to go through the trouble of obtaining evidence in a foreign territory. Now, the global popularity of U.S.-based companies such as Google and Dropbox has changed everything. In the Digital Age, German law enforcement officials investigating a crime that took place entirely in Berlin, with a German victim and a German alleged perpetrator, may often need access to communications content stored on servers on American soil. Under the current system, German officials would generally be able to compel the assistance of the American service providers only by filing a request under a Mutual Legal Assistance Treaty ("MLAT") or similar process, and then working with the Department of Justice's ("DOJ") Office of International Affairs ("OIA") to amass the information necessary for DOJ to make a probable cause showing in an American court.

There is a privacy benefit to requiring a warrant based on probable cause before a user's communications content is turned over to a country with a lower threshold for authorizing surveillance. However, the current process is

---

* Senior Counsel and the Director of the Freedom, Security, and Technology Project at the Center for Democracy & Technology (CDT). For CDT's more detailed analysis of the MLAT reform issue, *see Cross-Border Law Enforcement Demands: An Analysis of the Department of Justice's Proposed Bill*, CDT.ORG (Aug. 17, 2016), https://cdt.org/insight/cross-border-law-enforcement-demands-analysis-of-the-us-department-of-justices-proposed-bill-2/.

[1] Michelle Starr, *Happy 25th birthday to the World Wide Web*, CNET (Aug. 23, 2016), http://www.cnet.com/news/happy-25th-birthday-to-the-world-wide-web/#ftag=CAD590a51e.

sometimes painstakingly cumbersome[2] and is not keeping up with the deluge of requests for electronic content the DOJ now receives.[3] Moreover, the current system fails to protect the privacy of internet users' sensitive traffic data (such as email logs), which can be even more revealing than communications content.[4] Under current law, U.S. providers may *voluntarily* disclose their users' traffic data to foreign governments,[5] despite the fact that the U.S. government can only obtain such information with a warrant or a court order issued under 18 U.S.C. section 2703(d). Reforming the MLAT process should thus cover both content and traffic data. If it does, MLAT reform could be a unique opportunity to make domestic and international legal processes better suited to both legitimate law enforcement needs as well as privacy.

In July 2016, the DOJ proposed legislation that would be a step forward for law enforcement, but a leap backwards for privacy.[6] Under its proposal, select foreign governments would be able to make surveillance demands directly to U.S. providers under their own domestic procedures and standards. The DOJ, with the concurrence of the U.S. State Department, would decide which countries may enter into a bilateral agreement permitting these direct demands, based on a series of "factors" that are supposed to indicate whether a country provides adequate substantive and procedural privacy and civil liberties protections.

---

[2] The MLAT process takes an average of ten months. *See* THE PRESIDENT'S REV. GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD, 227 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[3] The number of requests from foreign authorities for computer records handled by the OIA increased ten-fold within the last decade. The overall number of requests for assistance from foreign authorities increased by nearly sixty percent during that time. *See U.S. Department of Justice FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform + $24.1 Million in Total Funding*, DEP'T OF JUST. (July 13, 2014), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[4] Greg Nojeim, *When Metadata Becomes Megadata: What the Government Can Learn*, CDT.ORG (June 17, 2013), https://cdt.org/blog/when-metadata-becomes-megadata-what-the-government-can-learn/.

[5] Although ECPA bars U.S. service providers from voluntarily disclosing metadata to "governmental entities" (18 U.S.C. § 2702(c)(6) (2012)), the Act defines "governmental entity" to include only U.S. federal, state, and local government agencies (18 U.S.C. § 2711(4) (2012)). This definition does not include foreign governments, which means U.S. communication service providers are free to voluntarily disclose user metadata—be it of a U.S. or non-U.S. person—to other governments.

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

Bilateral agreements could be a viable mechanism for partially addressing the problem of cross-border law enforcement demands (or "C-BLED's") for digital content. Such arrangements should help decrease the wait time for law enforcement who need quick access to digital evidence stored overseas. They may also, in theory, encourage foreign governments to improve their privacy protections in order to qualify for such "express lane" agreements. However, substantial changes must be made to the DOJ's proposal to bring it more in line with human rights requirements. Here are some big-picture recommendations:

First, Warrants for Content. U.S. law must finally be updated to require a judicially approved warrant based on probable cause in order to access stored communications content in the United States. The U.S. already requires a warrant when a foreign government uses an MLAT request to seek content in the United States. The E-mail Privacy Act, which passed by a 419-0 vote in the House of Representatives, would require the U.S. government to obtain a warrant, as well, by updating the 1986 Electronic Communications Privacy Act (which currently permits the use of a mere subpoena to obtain certain types of emails).[7] The United States should get its own surveillance house in order before telling foreign governments what they should be doing with their surveillance practices.

Wiretapping. The provision of the DOJ bill that would allow foreign governments to conduct wiretapping on U.S. soil should be deleted.[8] Otherwise, the DOJ bill would go well beyond fixing the MLAT system—expanding surveillance to convey an authority to foreign governments not contemplated by the current system, and without many of the restrictions placed on such highly invasive conduct in the U.S. by the Wiretap Act.[9]

Establishing a Credible Designation Process. Whether a foreign government's laws and practices provide sufficient substantive and procedural human rights protections should be based on whether a series of *requirements* are met, not on mere "factors" to consider. Moreover, although the DOJ and the State Department should play an important role in the decision making process, they should not be the only deciders because their decisions may be influenced by political and other factors. Instead, the DOJ's decision 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] This would enable human

[7] Email Privacy Act, H.R. 699, 114th Cong. (2016).
[8] *See* DOJ Proposal, *supra* note 6, at § 3(a).
[9] 18 U.S.C. §§ 2516-2518 (2012).
[10] 5 U.S.C. § 553 (2012).

rights and other experts to share their knowledge and opinions about that particular country. The DOJ should be obligated to respond to public comments and, before moving forward, should obtain the Senate's advice and consent (as is currently required for the approval of Mutual Legal Assistance Treaties.

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. Traffic data can reveal one's interests, medical conditions, associations, and location over time. It is thus absurd to have no standard for foreign governments while requiring a court order based on specific and articulable facts for U.S. government access—the privacy invasion is severe, regardless of who obtains the metadata.

Encryption and the Scope of Provider Assistance. The DOJ's proposed legislation should bar foreign surveillance demands with provider assistance mandates that go beyond the level assistance providers must afford under current U.S. law. This would prevent the scope of such requests from reaching into the dangerous and politically dicey territory of mandated encryption backdoors—mandates that technology policy experts have warned would undermine the security mechanisms that internet users rely on to protect them from criminal hackers and rights-abusing governments.[11]

Reciprocity Provisions. The bill contemplates C-BLED agreements that are reciprocal (meaning the United States would obtain the same ability to make surveillance demands on the foreign providers in partner countries). However, there are no provisions in the bill that would operationalize these demands by the U.S. government. Clear, privacy-protective rules of the road for U.S. surveillance demands on foreign providers will be critical to avoiding abuse and gaining international acceptance of such bilateral agreements.

In addition to these big-picture recommendations, certain specific changes to the text of the legislation are essential:

Judicial Authorization. The DOJ legislation should require judicial or other independent authorization prior to any surveillance conducted pursuant to an agreement. It currently contemplates "orders" issued by foreign *governments*, not foreign courts. Moreover, those orders would be subject to oversight by independent authority only after-the-fact.

Evidentiary Standard. Judicial orders for surveillance under a C-BLED agreement should 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

[11] *See, e.g.*, Harold Abelson, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, CSAIL TECHNICAL REPORTS (July 6, 2016), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

for the belief that information relevant to the crime would be obtained by the surveillance. The current standard in the proposed legislation is too weak and too vague.

"Serious" Crime Definition. Cross-border law enforcement demands under a C-BLED agreement should be limited to crimes for which the maximum 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. The DOJ legislation limits such demands to "serious" crimes, but leaves "serious" undefined.

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 addition, legislation should give countries an incentive to abandon data localization mandates and extraterritorial warrants, which threaten to fragment the global internet and leave vulnerable citizens at the mercy of oppressive regimes.

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. In addition, if a U.S. prosecution is based in part on C-BLED-gathered evidence volunteered to the U.S. government, that fact should be disclosed to the defendant. A judge should be able to suppress that evidence if it was collected in a way that abused a C-BLED agreement in order to circumvent U.S. privacy protections.

Notice. The DOJ proposal should, but currently does not, require that the target of the foreign government's surveillance receive notice. Such notice could be delayed in limited circumstances to protect the investigation or prevent risk of flight or serious bodily harm.[12]

Bilateral agreements may be part of the solution to the problem of cross-border law enforcement demands. However, the DOJ proposal lacks adequate protections. If Congress considers C-BLED legislation, it should take an approach more respective of human rights and civil liberties of people in the United States and abroad. Such an approach will be crucial to carrying the global internet through the next twenty-five years and beyond.

---

[12] 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. § 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. § 2703(b)(1)(B) (2012).