Statement of Chris Calabrese
Vice President, Policy
Center for Democracy & Technology

Hearing before the U.S. House Committee on the Judiciary on Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era

June 15, 2017

CENTER FOR DEMOCRACY & TECHNOLOGY

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee:

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We applaud the Committee for holding a hearing on the important and timely issue of government access to data stored abroad. We urge the committee to find solutions to this problem that update key components of the Electronic Communications Privacy Act (ECPA) and respect the privacy of individuals around the world while also meeting the legitimate needs of law enforcement.

First, we laud the committee for tackling this difficult and complicated issue. Potential policies have numerous direct and indirect consequences. Sorting out the appropriate policy response for the cross-border flow of data is fraught, involving the interrelationship of complicated systems and legal doctrines. However, in this area, there are three main policy objectives Congress must achieve: protecting individual privacy, respecting the comity between nations and speeding lawful access by government to electronic communications.

While there is no perfect solution, CDT believes that significant progress toward all three objectives can made through a package of reforms focused on improvements in four areas:

- Enactment of a strong, privacy protective reciprocal framework for enacting bilateral agreements between nations,
- Improvement to the existing MLAT system,
- Passage of the Email Privacy Act, and
- Adoption of a version of the International Communications Privacy Act (ICPA).

Bilateral Agreements

Bilateral agreements such as those contemplated by proposed legislation crafted by the U.S. Department of Justice (DOJ)[1] can be a viable mechanism for partially addressing the problem of cross-border law enforcement demands because they are among the best mechanisms for addressing a core issue with cross-border data flows – comity between nations.[2] This principle, which U.S. courts have long recognized, requires them to give due regard — and, where appropriate, deference — to the laws and legal system of a foreign country. This is important not only because the U.S. would expect equal deference to its own laws but also because it safeguards transnational actors such as U.S. companies who maybe be otherwise caught in a conflict between national laws. Additionally, because

[1] Letter from 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), ***available at*** http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

[2] A multilateral treaty might be preferable to bilateral 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.

these agreements allow direct access from a foreign government to communications held by a service provider, they are much faster for law enforcement than the traditional MLAT process.[3]

However, these bilateral agreements can also represent real privacy risks as nations without the strong constitutional standards of the U.S. – which require a warrant based on probable cause and approved by a neutral magistrate – are allowed to access communications under a potentially lower standard. CDT believes this weakness can be overcome with carefully crafted enabling legislation that safeguards personal privacy. In fact, if done properly they can actually be a spur for other nations to improve their own evidentiary standards. There is some evidence that this dynamic was in play in recent updates to UK surveillance laws, with the UK parliament adopting a so-called "double-lock" system in order to better match U.S. requirements for judicial review.[4] While the likelihood of this should not be overstated, any effort the U.S. government can make to encourage upward pressure on criminal and surveillance laws globally should be encouraged.

Of course, these agreements represent only a partial solution because only a limited number of nations will meet the criteria to negotiate such arrangements. Nonetheless, given these benefits CDT applauds DOJ for beginning a discussion for a legislative framework for bilateral agreements. While CDT opposes that legislation for the reasons listed below, we believe if improved it could be a key building block for an ultimate solution to this problem.

The Standards for Crafting a Bilateral Agreement Must be Mandatory

The DOJ's proposed legislation would permit bilateral agreements only with countries that "provide robust protections of human rights, privacy and other fundamental freedoms" 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.

---

[3] These agreements are also superior to another idea – 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.

[4] Paddy McGuinness, United Kingdom Deputy National Security Adviser, Written Testimony Before the United States Senate Judiciary Sub-Committee on Crime and Terrorism (May 10, 2017), ***available at*** https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf.

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 bilateral 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. First, DOJ's determination (with the concurrence of the State Department) to certify a country for a bilateral agreement should be made subject to the notice and comment procedures of the Administrative Procedure Act.[5] This would include public notice in the Federal Register of its intention to enter into an agreement, a public report that states the factual basis for the proposed certification, a public comment period and a requirement that DOJ responds to those comments. Human rights experts both inside 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. Court review under the deferential "***Chevron***"[6] 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 (MLAT). This may also serve as a check against misuse of this new authority. It would subject the agreement 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.

Access to Metadata

Currently under ECPA, foreign law enforcement demands for disclosure of metadata are treated differently from demands for content disclosure. While ECPA generally bars communications service providers from disclosing communications ***content*** to ***anyone*** unless through a lawful process, it permits providers to voluntarily disclose ***metadata*** to any foreign government that asks for it.[7]

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

[5] 5 U.S.C. § 553.

[6] ***Chevron v. Natural Res. Def. Council, Inc.,*** 467 U.S. 837 (1984).

[7] Although ECPA bars U.S. service providers from voluntarily disclosing metadata to "governmental entities," the Act defines governmental entity to include only U.S. federal, state and local government agencies. 18 U.S.C. §§ 2702(c)(6), 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.

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.[8]

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 an absurd result 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 bilateral 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 bilateral agreements.

Wiretapping

The DOJ proposal would permit countries entering into bilateral agreements 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. Providers of electronic communications service seldom know their users' countries of citizenship and often have imperfect information about their location.

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 be authorized only when other

[8] 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. § 2703(d). For subscriber information, such as a person's email address, the minimum required legal authority is a subpoena.

investigative techniques have been tried and have failed, or reasonably appear to be unlikely to succeed.[9] 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.

Judicial Authorization and Evidentiary Standard

Any legislation to clear the way for a bilateral agreement 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 inadequate and would mark a dramatic elimination of a key civil liberties protection in U.S. law that is afforded to people outside the United States. 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[10] even though it does not authorize surveillance of particular targets. It merely approves guidelines.

The DOJ's proposed bill would also 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 a bilateral agreement 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 would be committed, and a strong factual basis for the belief that information relevant to the crime would be obtained by the surveillance.

Further Considerations

In addition to these four main concerns, CDT also urges Congress to clarify the following issues:

- ***Scope of Provider Assistance*** - Like the United States, many governments require communications service providers to assist with governmental surveillance. 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, including requirements to decrypt communications.

[9] 18 U.S.C. §§ 2516-2518.

[10] ***See, e.g.***, Letter from 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), ***available at*** http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

- ***"Serious" Crime Definition*** – 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.[11]
- ***Freedom of Speech and Dual Criminality*** – The DOJ bill would require that orders issued under a bilateral 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 to adopt the dual criminality requirement that pertains in U.S. law today.[12]
- ***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 and may not target persons located in the United States. This is a crucial protection for any agreement but the legislation should also define what "targeting" means. The legislation also leaves entirely to the foreign government the discretion to adopt procedures designed to meet this requirement. In addition, when information on Americans is incidentally collected, 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.[13]

Finally, the bill contemplates bilateral 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. This is a crucial requirement; 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 decision in

[11] 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 U.S.C. § 1101(h).

[12] 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 U.S.C. § 3512(e).

[13] 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).

Microsoft v. United States indicates that such warrants, if issued, would have no extraterritorial effect.[14]

MLAT Reform

While we hope that bilateral agreements will be a key element in allowing the privacy protective sharing of information, they will not be a complete solution. Some nations will not qualify under the standards delineated above. Those requests should be handled by the current Mutual Legal Assistance Treaty (MLAT) process. As the committee knows, this system has been the subject of considerable criticism, often characterized as under-resourced and slow. One frequently cited static describes the process as taking an average of 10 months.[15]

While no one reform can ameliorate all the problems with the system, the International Communications Privacy Act (ICPA) contains a number of sensible improvements to the U.S. MLAT process, improvements that the U.S. can hold up as a model for other countries to emulate. The reforms would require DOJ to create and post an MLAT request form that foreign governments could use; create an online docketing system that would allow foreign governments to track the status of their MLAT requests; and report on an annual basis the number of MLAT requests the U.S. receives from foreign governments and makes to those governments, and the average processing time for each. The bill would also require the Attorney General to notify the Department of State of each disclosure of content to a foreign government pursuant to an MLAT request (ideally this would give State a chance to track whether disclosed communications content is used to violate a person's human rights), and to notify providers when information sought with a warrant is being sought pursuant to an MLAT request from a foreign government.

These requirements would make MLAT processing more efficient and transparent to the foreign government seeking the disclosures. In addition, CDT supports additional funding requests to allow for speedier processing of requests.

Finally, a significant 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. Foreign governments have begun to recognize this problem and seek solutions. For example, the Commission of the European Union is dedicating

---

[14] ***Microsoft v. United States***, 829 F.3d 197 (2d Cir. 2016). ***See also,*** Jadzia Butler, ***The Microsoft Ireland Case: A Clear Answer, an Uncertain Future***, Center for Democracy & Technology (July 18, 2016), ***at*** https://cdt.org/blog/the-microsoft-ireland-case-a-clear-answer-an-uncertain-future/.

[15] President's Review Group, ***Liberty and Security in a Changing World*** 227 (2013), ***available at*** https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

€500,000 to fund the creation of training materials and courses for EU practitioners on relevant U.S. law and procedures, notably the probable cause standard.[16]

Passage of the Email Privacy Act

For the all the reasons stated above, authorization of bilateral agreements are an important part of improving the flow of data across national borders – however a key component of any solution is the passage of the Email Privacy Act. The committee is intimately familiar with this bill, which updates ECPA to require a warrant for the content of communications. The Chairman and Ranking Member, as well as many other members of the committee, were crucial in securing its passage not only out of committee, but through unanimous passage by the full House in two consecutive Congresses, most recently in February of this year.[17]

While the committee has focused extensively on the importance of this legislation for the privacy of those in the U.S., it is also crucial here. The high privacy standard embodied by the Fourth Amendment of the U.S. Constitution – a warrant based on probable cause – is the gold standard for privacy. Warrants provide longstanding and meaningful protections – ensuring that police have a good reason to search for evidence of a crime in a particular location and that that search will be limited to only that particular evidence. Perhaps surprisingly, the current system has been a bulwark for privacy rights, not just in the United States but around the world. Because many U.S. tech companies have rightly applied the protections of the Fourth Amendment to all their customers, the practical result has been that they all receive this high level of protection no matter where in the world they reside.

When the Department of Justice testified before the Senate Judiciary Committee last month on this very issue, they mentioned warrants 30 times.[18] Each of the seven different examples the Department cites where they were unable to obtain evidence was in a case where they had a search warrant. It is assumed as the default. Yet as the committee knows full well, that is not the case. Because ECPA was passed in 1986 and has not been substantially updated since, it does not include a warrant standard in all cases, but in many cases allows the use of a simple subpoena with notice. While service providers deserve full credit for insisting on a warrant pursuant to the Sixth Circuit decision in ***Warshak***[19] and DOJ

[16] European Commission, ***Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*** (2017), ***available at*** https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf.
[17] For more on the importance of the Email Privacy Act, please refer to Chris Calabrese, Statement before the United States House Judiciary Committee on H.R. 699, the "Email Privacy Act" (December 1, 2015), ***available at*** https://judiciary.house.gov/hearing/h-r-699-the-email-privacy-act/.
[18] Brad Wiegmann, Deputy Assistant Attorney General of the U.S. Department of Justice, Statement Before the United States Senate Judiciary Sub-Committee on Crime and Terrorism (May 24, 2017), ***available at*** https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.
[19] ***United States v. Warshak***, 631 F.3d 266 (2010).

has stated that seeking a warrant is their policy in criminal cases,[20] policies and appellate court decisions are not a substitute for federal statutory reform.

It is actually the Department that best articulates the importance of warrants in its description of what it views as the problems with the ***Microsoft*** decision:

> The decision also does not enhance privacy. It involved a warrant that met all of the constitutional and statutory protections built into U.S. law. Indeed, requiring foreign legal process to access the data—as the court's opinion suggests is required—would not enhance privacy protections for U.S. persons. Foreign legal standards are no more demanding—and often are less demanding—than U.S. standards.[21]

This is precisely why, absent a bilateral agreement with its own set of protections and limitations, a warrant is so important.

Ironically, U.S. law would fail the test that the DOJ legislative proposal would establish as a baseline for the laws of a foreign country seeking a bilateral agreement with the U.S. The DOJ proposal 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 online. No legislation should move forward without addressing this obsolete portion of U.S. law.

Access to Cross Border Communications by Domestic Law Enforcement

With the baseline understanding that international comity issues should be mitigated through bilateral agreements and that any legislation must set as a baseline a warrant for the content of communications, what should be the standard for DOJ access to communications content held overseas, content of a foreign national or content when the nationality of the citizen is unknown? The International Communications Privacy Act (ICPA) – while not perfect – represents an important step forward.

[20] Elana Tyrangiel, Principal Deputy Assistant Attorney General of the U.S. Department of Justice, Statement Before the United States Senate Committee on the Judiciary (September 16, 2015), available at: https://www.judiciary.senate.gov/imo/media/doc/09-16-15%20Tyrangiel%20Testimony.pdf.

[21] Wiegmann testimony at 2-3.

The Current State of the Law: Microsoft v. United States

Prior to the Second Circuit's decision in the ***Microsoft*** case, U.S.-based communications service providers would disclose content pursuant to a warrant no matter whether they stored the content in the U.S. or abroad. Microsoft successfully challenged a judicial warrant covering communications content it stored in Ireland. Though Microsoft employees could retrieve the data from their desks in the United States, a three-judge panel of the Second Circuit found that the search of the data occurred in Ireland, where it was effectively copied, that ECPA has no extraterritorial reach because Congress had not explicitly given it extra-territorial effect, and that the DOJ would have to trigger the MLAT between the U.S. and Ireland in order to gain access to the data stored in Ireland.

Microsoft and other communications service providers have applied the Second Circuit decision on a nationwide basis. However, other providers do not architect their networks in the same way that Microsoft does. For example, according to the government's petition for rehearing in the ***Microsoft*** case, Google moves data around to data centers in different countries.[22] It also shares data so that different parts of one communication might be in several different data centers. Those data centers could be in different countries. Yet, only the Google employees in Mountain View, California, are authorized to access all the data that might be responsive to a warrant served on Google. According to the government, Google often does not know in what country responsive data are stored. This, the government argued, has created an untenable situation in which a warrant issued by a U.S. judge on the largest email provider in the U.S. (and perhaps in the world) may not reach data because parts may be stored outside the United States, and use of an MLAT request for the data may not practical or even possible.

The Second Circuit sitting en banc voted 4-4 not to grant the government's request for a rehearing. DOJ has since obtained orders from at least four magistrates outside of the Second Circuit that purport to compel a provider to turn over data that may be stored abroad.[23]

CDT filed an amicus brief in support of Microsoft in this case because the location of the data was known to be in a particular country outside the United States.[24] In that circumstance, we took the position that neither U.S. warrants or subpoenas should reach data stored outside the United States. Our primary concern is that a contrary rule, in which U.S. warrants reached data stored abroad, would result in chaos if followed on a reciprocal basis world-wide. Other countries would insist that their legal

---

[22] Petition for Rehearing and Rehearing ***En Banc*** of Petitioner-Appellant, ***Microsoft v. U.S.***, 829 F.3d 197 (2d Cir. 2016), ***available at*** https://www.justsecurity.org/wp-content/uploads/2016/10/Microsoft_14-2985-United-States-Appellee-Petition.pdf.

[23] ***See In re Search of Content that is Stored at Premises Controlled by Google***, No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); ***In re Search Warrant No. 16-960-M-01 to Google***, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017); ***In re Information associated with one Yahoo Email Address that is stored at premises controlled by Yahoo***, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); ***In re Search of Premises Located at [Redacted]@yahoo.com***, 6:17-mj-1236 (M.D. Fla. Apr. 7, 2017).

[24] Brief of BSA, et al., as ***Amici Curiae*** Supporting Appellant, ***Microsoft v. U.S.***, 829 F.3d 197 (2d Cir. 2016), ***available at*** https://cdt.org/files/2015/09/MSFT-data-AmicusBrief.pdf.

process would reach data stored in the United States, putting providers in an impossible position between conflicting legal regimes, and causing substantial damage to privacy interests because rules in other countries that govern law enforcement access to communications content for criminal purposes are often much more permissive than the U.S. rules.

International Communications Privacy Act

The fallout from the ***Microsoft*** case suggests that a location-based rule for the scope of U.S. warrants may not be practical when location of data is distributed or is unknown. ICPA was introduced to account for that reality. It would largely reverse the ***Microsoft*** decision. Even when location of data is known and is static, it would establish a rule for the scope of U.S. warrants that ignores the location of the data being sought and turns on the nationality and location of the subscriber or customer whose data are sought. ICPA's six-part test essentially boils down to this: U.S. warrants could be used to compel disclosure by a provider over which the U.S. has jurisdiction, of communications content and metadata of any person anywhere in the world, except that of a person reasonably believed to be a non-U.S. person located in – or a national of – a country with an MLAT or similar executive agreement with the U.S., which country has objected to the warrant within 60 days. ICPA also includes the MLAT reform proposals I described above.

This test represents a valuable effort to accommodate the interests of other nations, though it does not benefit those with no MLAT or executive agreement with the U.S. In those cases, the U.S. government would be able to essentially reach into data centers and compel disclosure of data of foreign nationals and of U.S. persons, without the consent of the country in which the data was held. Other countries might well insist that their legal process also has extraterritorial reach in the same circumstances. That would mean, for example, that a country that is a human rights violator and has no MLAT or executive agreement with the U.S., could argue that its legal process (something less than a warrant) compels disclosure by communications providers in the U.S. over which it claims jurisdiction. When U.S. providers locate employees in such countries, it can give such countries leverage to enforce their jurisdictional claims. Additionally as the Department of Justice has pointed out, it could also mean that a country like Russia, which does have an MLAT agreement with the U.S., could argue that its warrants compel providers in the U.S. to disclose the communications of their Russian subscribers even if they are lawful permanent residents of the United States and are physically located in the U.S., where ECPA would otherwise bar such a disclosure.

A further complication is that in some cases data of a foreign national will be known to be physically located in the judicial district in which the warrant is issued. It is difficult to accept the proposition that the warrant sometimes cannot reach the data even though warrants for physical searches of property in the judicial district would be proper.

Given these factors it is clear that ICPA is not a perfect solution to the problem raised by cross border data flows. However, we are encouraged by the focus on the nationality and physical location of individuals rather than the location of data and we believe Professor Jennifer Daskal has raised several useful ideas, including a mandatory comity analysis by courts and reciprocal notice and control

provision to foreign nations when their nationals' data is collected.[25] These ideas may help in further refining ICPA.

Additionally, if ICPA is combined with a framework for crafting a privacy protective bilateral agreement, it helps to address the concerns with international comity and extraterritorial warrants. Nations that do not have MLATs or who wish to gain speedier access to electronic communications held by U.S. service providers will have an avenue to pursue that outcome – domestic legal reform and a bilateral treaty. Countries that cannot meet the standard for a bilateral agreement would have less standing to argue their process deserves extraterritorial reach.

Conclusion

The problem of cross-border data demands is growing as the need for electronic data in criminal investigations grows. While there is no perfect solution to this problem, CDT believes that a package consisting of a combination of privacy protective bilateral agreements, MLAT reform, passage of the Email Privacy Act, and enactment of a version of ICPA is the best path forward for addressing the real needs of law enforcement, concerns over international comity, and the privacy rights of citizens around the globe.

[25] Jennifer Daskal, Associate Professor, American University Washington College of Law, Statement before the United States Senate Subcommittee on Crime and Terrorism (May 24, 2017), available at: https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf.