University of Kentucky
College of Law
Andrew Keane Woods
Assistant Professor

Statement of

Andrew Keane Woods
Assistant Professor
University of Kentucky
College of Law

Before the

Committee on the Judiciary
United States House of Representatives

For a Hearing Entitled

"Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era"

June 15, 2017

Statement of
Andrew Keane Woods
Assistant Professor
University of Kentucky
College of Law

Before the
Committee on the Judiciary
United States House of Representatives

For a Hearing Entitled
"Data Stored Abroad: Ensuring Lawful Access
and Privacy Protection in the Digital Era"

June 15, 2017

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for inviting me to testify today about the challenges of creating a sensible regime for guiding law enforcement access to data across borders.

The Electronic Communications Privacy Act (ECPA) is the greatest source of conflicts of laws in the technology sector today and it desperately needs reform. There are two distinct but related problems: (1) U.S. law enforcement agents with a warrant cannot access foreign-held data and (2) foreign law enforcement agents engaged in lawful investigations cannot access U.S.-company-held data. In my testimony, I will address each issue in turn.

Before I do, let me emphasize that this problem is neither as novel nor as complicated as it first seems. At its core, the challenge we are here to discuss is an old one: determining the scope of one government's authority over a globally distributed good. People and things have been moving around the world at fast speeds for a long time. The principle that has long guided these matters is territorial sovereignty, and that should be the Committee's lodestar in crafting new legislation. As my comments will make clear, I am not arguing for privileging sovereignty or law enforcement interests over privacy. Rather, in my view the best way to ensure privacy and security on the global Internet is to craft a regime that respects rather than frustrates legitimate state interests.

I. Widespread Agreement on the Need for Reform

Before discussing possible reforms, it is worth noting the strength of the consensus—from a broad array of companies, governments, and civil society groups—both about the scale of the problem and the need for reform. A word about both is in order.

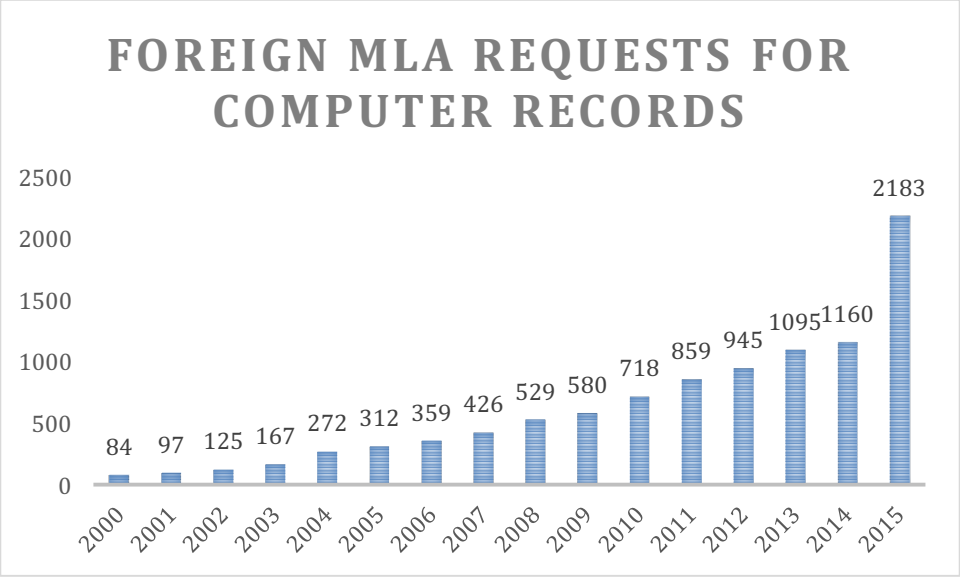
a. The Scale of the Problem

Law enforcement officers increasingly struggle to get crucial evidence in criminal cases. Why? Because criminal evidence today is often digital, often stored in the cloud, and often held by a provider in another jurisdiction.[1] This problem is not limited to electronic crimes—though those are affected

[1] For a summary of this problem, see Andrew Keane Woods, *Against Data Exceptionalism,* 68 STAN. L. REV. 729, 739–

as well—but rather it applies to bread-and-butter law enforcement investigations into crimes like murder, kidnapping, and theft. The problem is particularly acute for foreign law enforcement agents, since so many of the world's citizens use American Internet services. Because of ECPA's blocking features, foreign law enforcement officers often cannot compel American firms to comply with their laws. When foreign governments cannot get access to data they seek in criminal cases by using domestic legal process, they typically must ask the U.S. government for mutual legal assistance (MLA), a notoriously slow procedure.

ECPA, in other words, creates a problem for law enforcement *around the world*. Not only is the scale of this problem enormous, but it is growing. I started looking into this issue approximately five years ago, and in that short time conditions have become considerably worse. In 2000, for example, the U.S. government received 84 MLA requests for computer records; in 2015, that number was 2183, and poised to increase dramatically as the chart below indicates.[2]



The Department of Justice has testified to what a strain these requests place on the Office of International Affairs and on the U.S.'s diplomatic relations.[3] Many of these requests take nearly a year to complete.[4] Worse, these numbers do not represent the true scale of the demand because many foreign law enforcement agents never make a request at all, knowing that the petition will languish for months or years.[5]

---

51 (2016).

[2] FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform, U.S. Dep't of Justice, http://www.justice.gov/sites/default/ les/jmd/legacy/2014/07/13/mut-legal -assist.pdf.

[3] Brad Wiegmann, Statement Before the Senate Judiciary Committee, May 24, 2017.

[4] The White House concluded that these requests typically take an average of ten months. See PRESIDENTS REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS 227 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[5] ANDREW K. WOODS, GLOBAL NETWORK INITIATIVE REPORT, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE (2015), https://globalnetworkinitiative.org/sites/default/les/GNI%20MLAT%20Report.pdf.

The consequences of this broken system go far beyond the stakes of any given criminal investigation. When foreign governments cannot get access to the data they seek in criminal cases because of ECPA's provisions, they are increasingly opting to take matters into their own hands—by demanding that data be stored locally, or that providers not use encrypted services, making them easier to intercept. As I noted recently:

> If domestic law enforcement cannot conveniently access criminal evidence held by American Internet companies, it might 1) demand that data be held on local servers, where it can more easily be accessed (and surveilled); 2) deploy covert surveillance efforts to access the data (and perhaps demand a way around the service provider's encryption); and/or 3) assert extraterritorial jurisdiction over the foreign-held data, throwing Internet companies into an unfortunate conflict of laws. Each of these problematic policies has resulted from states' frustrations with the existing regulatory and technological framework.[6]

These extreme measures pose considerable threats to privacy on the global Internet. Indeed, one sure way to threaten the global success of the American technology sector is to encourage foreign countries to devise rules for regulating the Internet that dramatically increase the costs of running a global Internet business or worse—make it impossible to operate in two countries at the same time, worsening the problem of a splintered and decidedly less-worldwide web.

The stakes are also sky-high for law enforcement agents in the United States, who have been unable to solve important criminal cases as a result of their inability to compel service providers to hand over data stored abroad. The desire for access to critical digital evidence has led government to push quite hard to gain access to evidence however possible, including through the explosively controversial calls to legislate law enforcement access to encrypted technologies. Rather than grant the government a master key to every iPhone in the world, Congress should act to remove jurisdictional barriers that prevent law enforcement from accessing data that they have probable cause to seek.

b. Universal Desire for Reform

There is overwhelming agreement that as it is currently drafted, ECPA—which is silent about its territorial reach—is not a sensible way to regulate law enforcement access to data across borders. American law should not get in the way of legitimate criminal investigations, here and abroad, and we should not incentivize foreign governments to find other means of accessing the data they cannot get because of ECPA's blocking features. There is also widespread agreement that the U.S. government should be sensitive to the fact that whatever rules are developed will have a significant impact on the privacy of non-U.S.-citizens.

So how do we satisfy this widespread desire for reform?

It turns out that achieving these goals is quite simple: revise ECPA to allow states to gain access to data when they have a legitimate interest in doing so—that is, when one of their laws has been broken. Specifically, ECPA must be reformed along two axes: (1) ECPA should allow U.S. law enforcement

[6] Andrew Keane Woods, *Mutual Legal Assistance in the Digital Age,* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (Stephen Henderson & David Gray eds., forthcoming).

to serve production orders within the U.S. that compel providers to produce data wherever it happens to be stored, and (2) ECPA should leave U.S. firms free to comply with the laws of the countries where they operate, including responding to production orders served on American firms outside the U.S. Let us examine these reforms in a bit more detail.

II. U.S. Law Enforcement Requests

a. The Problem: The Second Circuit's Recent Decision

As you know, Microsoft and the Justice Department have been engaged in a years-long conflict over access to an email account apparently stored on Microsoft's servers in Ireland. The Second Circuit concluded that a warrant issued under ECPA cannot compel Microsoft to produce the foreign-held data because (1) ECPA does not apply extraterritorially, and (2) the storage location of the requested data is the key factor in determining ECPA's territorial limits.[7] The Department of Justice asked the court to rehear the case *en banc*, but that request was denied.[8] In the meantime, a number of other courts have concluded nearly the opposite—that orders issued pursuant to ECPA compel providers to produce responsive evidence wherever it is stored.[9] The split among courts means that uncertainty reins among both providers and law enforcement, and it greatly increases the likelihood that the case may end up before the Supreme Court.

b. The Solution: Clarify That ECPA Operates on Firms in the U.S. Regardless of Data Location

There are two sensible and straightforward solutions to this problem, both of which would give the U.S. government the authority to compel a firm operating in the U.S. to produce data regardless of where it happens to be stored. One approach would be to clarify that Congress intends ECPA's production orders to be deemed to operate wherever the data is searched and/or seized *by U.S. law enforcement*. So if Microsoft received a warrant for emails, the warrant would compel production in whatever American jurisdiction Microsoft received the warrant—but it would be agnostic as to the location that Microsoft has chosen to store the data. This is perhaps the cleanest resolution to this issue because it does not change the scope of ECPA's territorial reach, only the test courts should use for determining when an order operates domestically or extraterritorially. Another approach would be to conclude that ECPA is designed to have extraterritorial reach, but only as to production orders—that is, a U.S. judge can issue an order under ECPA that will require firms in the U.S. to produce responsive data wherever it happens to be stored and wherever a court determines the relevant search or seizure to occur.

Both of these approaches are consistent with longstanding doctrine in other sorts of cross-border cases, where courts regularly compel banks and other intermediaries to provide records held abroad—even where doing so would potentially place the intermediary in jeopardy of violating another

[7] In re Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

[8] In re Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d 53 (2d Cir. 2017).

[9] See, e.g., 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).

country's laws.[10] This is helpful to keep in mind because one objection to the above proposals is that they will create conflicts of laws—that these proposals allow the U.S. government to compel a provider to deliver data held in another jurisdiction thereby putting the intermediary in jeopardy of violating that jurisdiction's laws. In fact, production orders that call for the retrieval of data held in foreign servers rarely produce a direct conflict of laws. Consider the dispute that gave rise to the Second Circuit's decision regarding Microsoft's Irish-held data. Although Ireland filed a brief asserting a vague interest in the case, in fact there was no conflict between Irish laws and the U.S. production order—Microsoft could have complied with the order without violating any Irish laws.[11]

In those rare instances where conflicts do arise from allowing the U.S. law enforcement to compel firms in the U.S. to hand over foreign-held data, courts will sort them out—just as they do in any number of cross-border cases today.[12] Under today's banking laws, for example, prosecutors regularly assert the power to regulate activity that has extraterritorial effects, and the world manages to carry on. When there is a conflict with another country's laws, courts have equitable tools at their disposal—doctrines like comity—that allow them to weigh the competing equities in a given case.[13] If a service provider receives a request for data that directly conflicts with another country's laws, the provider can use the time-tested method for managing conflicts of laws—it can challenge the order in court. In those cases where the conflict is severe enough to warrant a legal challenge, a court can evaluate the conflict and use any number of doctrines to resolve it.

Ultimately, fears about reforming ECPA in ways that create conflicts of laws are misplaced. It would be ironic indeed if Congress were so worried about creating conflicts of laws that it failed to fix the single biggest conflict today—which is ECPA itself. In the instance where a federal judge has decided to issue a warrant based on probable cause, it would be odd to deliberately create a regime that frustrates that warrant. The only reason to limit the warrant's reach would be if it interfered with another state's laws. If and when this happens, it can easily be managed by a court using longstanding conflicts of laws principles.

III. Foreign Law Enforcement Requests

a. The Problem: ECPA Makes It Hard for U.S. Providers to Comply with Foreign Law Enforcement

The leading cause of today's conflicts of laws in this space is ECPA. The world's most popular web services are American, and many U.S. providers interpret ECPA to prohibit them from producing

---

[10] See, e.g., United States v. First Nat'l City Bank, 396 F.2d 897, 900 (2d Cir. 1968) ("The basic legal question confronting us is not a total stranger to this Court. With the growing interdependence of world trade and the increased mobility of persons and companies, the need arises not infrequently, whether related to civil or criminal proceedings, for the production of evidence located in foreign jurisdictions."); United States v. Bank of N.S., 740 F.2d 817, 826-28 (11th Cir. 1984) (finding that bank records located abroad could be compelled in the United States, even where doing so would violate foreign law).

[11] Brief of Amicus Curiae Ireland at 1-3, *Microsoft Corp.*, No. 14-2985-cv (2d Cir. Dec. 23, 2014).

[12] See RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (Am. Law Inst. 1987).

[13] I understand that some legislators are considering mandating that a comity analysis be conducted *ex ante*. This strikes me as an odd requirement, since it will slow investigations down and is unlikely to lead to a meaningful change from today's practices.

digital content in response to anything but a U.S. government order.[14] When the U.K. government approaches Google with an order to produce emails, for example, Google points out that the order directly conflicts with ECPA's provisions. This understandably frustrates foreign governments, and it encourages them to take drastic measures like demand data localization and deploy covert surveillance techniques for otherwise lawful criminal investigations. Fortunately, the solution to this problem is straightforward.

b. The Solution: Reform ECPA to Remove the Conflict of Laws

The simplest solution to this problem is to clarify that ECPA has little to say about foreign governments' criminal laws or how U.S. firms choose to comply with them. Congress can do this by clarifying that ECPA's requirements do not apply to foreign government requests for data (even if they do apply to U.S. government and nongovernment requests). When a government makes a request of an American firm that is lawful under that country's laws, U.S. law should not create a barrier; in such a scenario, the U.S. government has little equity at stake, unless the data being requested belongs to a U.S. citizen.

Such a regime respects other countries' decisions about the scope of their criminal laws. The alternative to such a regime is much messier and, I fear, much less protective of privacy over the long run. That alternative would be to spell out the conditions under which U.S. Internet firms can comply with foreign law enforcement requests.

I know from speaking with foreign government representatives that they resent having to request assistance from the U.S. *and* to meet U.S. legal standards in order to enforce their own laws. What is the justification for this requirement? If the British police are investigating a crime that occurred in London, and they procure a lawful order to investigate the suspect's possessions and communications, U.S. law does not prohibit Bank of America from complying with a request for records. But U.S. law *does* prevent Google from complying. This is oddly inconsistent and foreign governments resent it; many now are poised to retaliate.

Some countries may manage to negotiate an agreement with the U.S. to grant them special passage into a club where their criminal laws would operate against Google and Facebook just as they do now against other American firms, like Chevron and Citibank. (As you know, the U.S. and the U.K. have been negotiating an agreement that would allow British law enforcement to make lawful requests directly of U.S. providers for data relating to British investigations when the data does not belong to an American.) Other countries—those not in the club—would not enjoy the same ability to enforce their laws on their own soil against American Internet firms, absent some dramatic action on their part. So Brazil and India, for example, might simply pass a law requiring any company operating on their soil to store local records locally—where they can more easily be searched and seized. Such forced data localization rules are costly and a significant threat to privacy on the Internet, but they are the natural response by a country struggling to enforce its own laws.

The creation of a club not only encourages those left out to take drastic legal measures—measures such as data localization and anti-encryption mandates—but it also encourages the creation of anti-

[14] This is in part because of the way these firms have structured their networks, in part the way that they interpret ECPA's territorial scope, and in part their reading of ECPA's definition of government entities, in Section 2711(4), which explicitly limits itself to U.S. government agencies.

clubs. One could imagine Brazil and India, for example, joining forces to create separate rules for regulating the Internet. With Internet governance already highly politicized—and viewed as American dominated—this seems like an outcome worth trying to avoid.

Another possibility is that countries left out of the club will be more inclined to adopt blocking statutes and other unfriendly legal rules to regulate the conduct of their Internet companies abroad. This may not matter to the U.S. government at the moment, when so many Americans are using American Internet services. But American dominance of Internet services will not last forever, even here in the U.S. It is not hard to envision a time in the very near future when many Americans regularly use an app that comes from one of the countries not in the club. If non-club countries pass retaliatory blocking statutes making it hard for their firms to comply with U.S. law enforcement, our law enforcement agents will find themselves in the situation that their foreign counterparts are in today.

Congress should remove ECPA's blocking features and resist the temptation to replace it with an overly complicated set of requirements for countries to enforce their own laws on their own soil. This is not only the simplest solution to the conflicts of laws created by ECPA, but it is the path least likely to incentivize foreign allies to adopt privacy-eroding policies. I understand, of course, the temptation to outline the privacy protections that Americans think ought to apply in criminal investigations around the world, but I worry they will backfire.

IV. Conclusion

Congress is faced with a momentous task: to devise a set of rules for law enforcement access to criminal evidence stored in the global cloud. One option would be to craft a set of bespoke principles to guide U.S. and foreign law enforcement access to that data. That seems like a heavy lift, one that risks producing a club of countries operating by American-mandated principles (and perhaps an anti-club, operating by another set of principles). A better option may be to treat this issue as we have treated so many other cross-border issues: by allowing American firms to cooperate with law enforcement at home and abroad.