Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google Inc.
House Judiciary Committee
Hearing on "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 the opportunity to appear before you this morning to discuss our views about potential solutions to the challenges that a broad array of stakeholders are confronting in the area of cross-border law enforcement requests.

My name is Richard Salgado. As the Director for Law Enforcement and Information Security at Google, I oversee the company's response to government requests for user information under various authorities from around the world. This includes requests from authorities in the U.S. under the Electronic Communications Privacy Act (ECPA) and pursuant to diplomatic mechanisms such as mutual legal assistance treaties (MLATs) and agreements, and letters rogatory. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the U.S. Department of Justice, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and most recently at Stanford Law School.

At the outset, I want to express my gratitude to this Committee for its steadfast efforts to advance the Email Privacy Act. For many years, we have called upon the U.S. Congress to update the Electronic Communications Privacy Act (ECPA) to codify the requirement that U.S. governmental entities obtain a search warrant in order to compel service providers to disclose the content of users' communications. As we have noted in previous testimony before this Committee, a warrant-for-content standard is effectively the law of the land today. This standard is observed by governmental entities and providers alike and has been embraced by courts as necessary to satisfy federal constitutional standards. As a result of this Committee's hard work, the House of Representatives unanimously passed the Email Privacy Act in 2016 and by voice vote in 2017. We hope to see this standard enacted into law in conjunction with other changes to ECPA that are necessary to accommodate appropriate cross-border law enforcement requests.

An ECPA for the 21st Century

In the realm of cross-border law enforcement requests, there are two distinct, but related, challenges that confront law enforcement agencies and service providers alike. These challenges arise from the fact that ECPA, a statute that has been vital for decades, has become antiquated in some key respects.

First, as the Committee well knows, a unanimous panel of the United States Court of Appeals for the Second Circuit ruled last year that a search warrant issued under ECPA only permits U.S. government entities to compel a provider like Google to search for, seize, and produce records that are stored in the United States. The Second Circuit recently denied the government's petition for rehearing *en banc*. No other appellate court has addressed the issue, leaving the Second Circuit opinion as that of the highest court to address the issue. In litigation as well as testimony to the Senate, the Department of Justice has argued that there are good policy reasons to adopt a different legal rule than is provided for in ECPA, as that statute is interpreted by the Second Circuit.

Second, ECPA includes a broad, so-called "blocking" provision that restricts the circumstances under which U.S. service providers may disclose the content of users' communications to foreign governments. There are legitimate reasons that a country may wish to control to whom a provider discloses data (e.g., preventing the disclosure of the content of communications to governments with poor human rights records). A broad blocking statute that is divorced from such policy concerns and lacking nuance, however, can leave countries with a legitimate need for information looking for alternative means, some of which can be unsavory and aggressive. Indeed, the blocking provision in ECPA is a source of enormous frustration for democratic countries that respect the rule of law and maintain robust substantive and procedural protection of civil liberties, and who need to investigate local crimes involving local users of U.S. services.

These countries are often unable to obtain timely access to digital evidence solely because it is retained by a U.S. service provider subject to ECPA, even for crimes that are wholly domestic in nature. The inability to obtain this data creates incentives for these countries to seek other techniques to get the information, including enforcement of their laws extraterritorially, even in the face of conflicting U.S. law. It also creates incentives for enactment of data localization laws and aggressive investigative efforts that can undermine security in general and redound to the detriment of users' privacy.

In both of these cases, it is quite clear that the status quo is unsustainable. As technological innovation has flourished and U.S. Internet companies have established footholds in markets outside the U.S., the assumptions underlying ECPA – a 1986 statute – are crumbling. Congress should holistically modernize and update ECPA to address the panoply of challenges that have emerged in recent years. This includes, but is not limited to, statutory changes that would:

- Require U.S. government entities to obtain a warrant to compel the production of communications content from providers.

- Provide clear mechanisms for the U.S. government to obtain user data from service providers wherever the data may be stored, but with protections built in for certain cases when the U.S. government endeavors to obtain from U.S. companies content data of users who are nationals of other countries or located abroad.

- Permit U.S. providers to disclose data to certain foreign governments in response to appropriate legal process in serious cases when the domestic laws of these foreign countries provide baseline privacy, due process, and human rights guarantees.

ECPA Warrants and the U.S. Government

As the statute is written, and as the Second Circuit held, U.S. government entities cannot use an ECPA warrant to compel a provider to search for, seize or produce data held outside the US. This of course has presented challenges to law enforcement. Google agrees with the Department of Justice that ECPA should be amended to address this challenge. Rather than imposing limits on the reach of legal process under ECPA based on the location of data at the moment the records are sought, a criterion applicable to traditional warrants, legal process under ECPA should be modified to consider the underlying user's nationality and location.

This is not to criticize the Second Circuit's decision, which is based on well-established and long-held principles of statutory construction. Rather, it is to underscore the importance of Congressional intervention. The cases pending around the country have judges working to understand what Congress intended in this statute enacted in 1986, well before providers like Google, Microsoft and Facebook existed. The Second Circuit's reasoned, thorough decision shows yet again that ECPA is overdue for an update. Addressing this issue is a task that ultimately should not and cannot be left to the courts. Service providers appreciate the important law enforcement equities at stake in this debate, and we are confident that Congress can fashion a legal framework that reflects these and other important equities.

In its current form, ECPA is ill-suited to address modern-day technological realities and cross-border law enforcement investigations. Modern Internet networks increasingly store data intelligently, often moving and replicating data seamlessly between data centers and across borders in order to protect the integrity of the data and maximize efficiency and security for users. This technological reality underscores the importance of legislative solutions that eschew data location as a relevant consideration in determining whether a particular country can exercise jurisdiction over a service provider.

Notably, all of the judges who issued pertinent rulings in the Second Circuit case (including both the original 2016 panel opinion and a 2017 ruling denying rehearing before the entire Second Circuit) urged Congress to consider appropriate changes to ECPA that would definitively resolve the policy questions at the heart of the case. Judge Lynch's concurrence in the 2016 case is notable in this regard:

> Although I believe that we have reached the correct result as a matter of interpreting the statute before us, *I believe even more strongly that the statute should be revised*, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 233 (2d Cir. 2016) (Lynch, J., concurring).

Inaction means that important policy decisions about electronic privacy and government access fall by default to the courts. Indeed, since the Second Circuit's ruling in 2016, magistrate judges in other circuits have continued to grapple with the issue. As did the Magistrate Judge and District Judge in the Second Circuit, they have ruled that ECPA warrants can be used to compel U.S. providers to search for, seize and disclose electronic communications content stored abroad. All of these courts are being asked to resolve individual disputes in ways that are divorced from sound policy solutions, without the robust opportunity for debate among a variety of stakeholders, and indeed potentially entirely in closed courtrooms. This is hardly the path for appropriately addressing the equities of users, law enforcement agencies, service providers, and foreign sovereigns.

Congress has an opportunity to update ECPA for the Internet age, and to consider how the application of domestic U.S. surveillance laws affects the equities of foreign countries and the privacy rights of non-US persons. We are confident that Congress can find mutually agreeable solutions. Last month, in testimony before the Senate Judiciary Committee, the Department of

Justice outlined six principles that should govern any legislative framework that Congress develops to address the Second Circuit's decision and the broader issue of cross-border law enforcement requests. We agree with these principles, and we have worked with some of the world's largest internet companies on how we might embody them in a legislative framework.

A legislative framework that addresses the equities of relevant stakeholders is far preferable to a protracted litigation battle that is missing critical voices and perspectives. This is a job for Congress, not the courts. In the last Congress, Representatives Marino and DelBene, and Senators Hatch, Coons, and Heller, introduced the International Communications Privacy Act (ICPA). With some further refinements, ICPA can provide the right framework for cross-border law enforcement demands for user data. These refinements can and should address both the six principles DOJ underscored in previous testimony and principles that concern those who use the services:

- **Data Location.** Subject to the following additional principles, the location of data held by a U.S. provider should not in and of itself determine whether lawfully issued legal process issued under the stored communications chapter of ECPA can reach that data.

- **Notice:** When a government agency in one country endeavors to obtain, through lawful process to a provider in its jurisdiction, the electronic data of a user who is national of or located in a different country, that agency should provide notice to the other country. There will be understandable exceptions and limitations to this notice requirement, but a country that has established diplomatic mechanisms (e.g., a Mutual Legal Assistance Treaty (MLAT)) with another country for the production of data in cross-border investigations, and that observes shared, baseline principles of privacy, due process, and human rights, should honor this notice principle. This affords the other country an opportunity to raise concerns, through diplomatic channels for example, about the request in light of the legitimate privacy interests of its citizens and the comity interests and values of that country.

- **Redress and Comity Factors:** A jurisdiction that receives the notice contemplated above should have the opportunity for redress in the requesting country's jurisdiction. This may include the opportunity to initiate a legal challenge. Courts that hear such challenges should conduct a comity analysis to help weigh the equities of the countries. Factors to be considered under that analysis could include: (i) the location and nationality of the customer or subscriber; (ii) the location of the crime; (iii) the seriousness of the crime; (iv) the importance of the data to the investigation; and (v) the possibility of accessing the data via other means.

- **Reciprocity**: Countries that extend the aforementioned rights (i.e., notice and redress) to other countries under their domestic laws should expect reciprocity. Countries should not be required to provide notice or redress mechanisms to other countries that are not obliged to reciprocate. And no country, of course, should be required to extend the aforementioned rights to countries that fail to adhere to baseline privacy, due process, and human rights standards.

We believe that the four principles outlined above are complementary to those underscored by the Department of Justice in its testimony before the Senate Judiciary Committee last month. The basis for a legislative framework that addresses the various equities at stake exists, and we are eager to work with this Committee and the Congress writ large to update ECPA in this manner.

ECPA Prohibitions and Foreign Governments

Just as the U.S. government has increasingly sought information from U.S. providers, so too have foreign governments. In fact, since 2009 Google has received more requests from foreign authorities than it has from criminal law enforcement agencies in the U.S. That is not surprising, given that many of the users of U.S. providers are outside the U.S., and the providers may have evidence needed in foreign investigations. Congress could not, of course, have envisioned this in 1986 when it passed ECPA.

ECPA generally prohibits U.S. companies from disclosing communications content to foreign law enforcement agencies. As a result of ECPA's "blocking" provision, law enforcement agencies in these countries often need to go through diplomatic channels with the U.S. government to secure the information. This can take many different forms, including letters rogatory and, where there is a treaty or executive agreement, through mutual legal assistance. These diplomatic channels are critical tools and need to work efficiently. The volume of incoming MLAT requests to the U.S. government has put tremendous pressure on this critical system. President Obama's Review Group on Intelligence and Communications Technologies reported in 2013 (p.229) that, on average, MLAT requests "appear to average approximately 10 months to fulfill, with some requests taking considerably longer." These delays can frustrate the investigation and prosecution of serious crimes.

As concerns about crime and terrorism grow, countries looking for solutions that are faster than diplomatic mechanisms like MLAT are considering more aggressive and potentially dangerous unilateral approaches, such as extraterritorial application of greatly expanded surveillance authorities. Many of the proposals under consideration threaten to create a chaotic environment of conflicting laws, and threaten to undermine the security of the services we all depend on. This

is bad for the governments battling to have their laws prevail, the companies that are put in an untenable position, and most importantly the users of the services.

This reaction is also preventable. Amending ECPA to lower the blocking provision for cases involving serious crime being investigated by countries that commit to baseline principles of privacy, human rights, and due process can go a long way to addressing the need for such unilateral and unsavory reactions. Indeed, amending ECPA in this way would have the salutary effect of incentivizing foreign countries to update and raise their privacy and due process standards in order to avail themselves of this approach, which would be faster and more efficient than the traditional MLAT process. This doesn't eliminate the need for governments to otherwise improve diplomatic mechanisms like MLAT of course, but does help make the MLAT process work better as the volume decreases.

In July 2016, the U.S. Department of Justice unveiled legislation that would amend ECPA to authorize, but not require, U.S. providers to disclose communications content to foreign governments that adhere to baseline due process, human rights, and privacy standards. Under the proposed legislation, the U.S. government would be authorized to enter into executive agreements with foreign governments that meet minimum requirements of substantive and procedural protection of rights. Under such an agreement, a qualifying foreign government could make legal requests to U.S. service providers in certain types of criminal investigations without going through diplomatic channels. DOJ and the Department of State would be required to determine and certify that such a country adheres to baseline privacy, due process, and human rights principles before U.S. companies could disclose the content to the country under the new provision. Notably, foreign governments would be required to afford reciprocal rights to the U.S. government in obtaining access to electronic data that a foreign country may prohibit service providers from disclosing. The U.S. and U.K. governments are in the process of negotiating this type of agreement. The U.K. for its part has enacted legislation to implement what I understand are key components of this agreement.

Google supports this approach. A framework of this sort can help set expectations about the types of changes that foreign governments will need to make in order to satisfy threshold privacy, due process, and human rights standards. Providing a pathway for these countries to obtain electronic evidence directly from service providers in other jurisdictions, where such jurisdictions have no appreciable equity to block disclosure, will remove incentives for the unilateral, extraterritorial assertion of a country's laws, data localization proposals, aggressive expansion of surveillance authorities, and dangerous investigative techniques, which are ultimately bad for us all.

There is no panacea for the range of challenges presented by aging legal regimes that are ill-equipped to address technological innovation, modern law enforcement needs, and strong privacy, due

process, and human rights standards. MLAT improvements remain critical to instill confidence in the ability of the U.S. to provide responsive data to foreign law enforcement agencies in a timely manner. The vast majority of countries are going to rely on MLATs and comparable diplomatic mechanisms for the foreseeable future, which underscores the importance of moving quickly to fully fund and implement the necessary reforms to the MLAT process. ICPA furthers that objective by codifying important reforms that can begin the process of modernizing the MLAT process. It is also clear that democratic regimes that recognize due process should have other mechanisms, in addition to the MLAT process, to obtain communications content of their nationals and others living within their border. These mechanisms need to include robust protections against abuse, and should be limited to serious cases.

****

Congress must address the underlying challenges concerning cross-border law enforcement requests. We are confident Congress can do so in a way that respects the equities of all countries that may be affected, improves the privacy rights of users worldwide, avoids creating conflicts of law for U.S. Internet companies, and provides the tools governments need to conduct legitimate investigations.

Thank you for your time and consideration.