Senator Orrin G. Hatch
The Law Enforcement Access to Data Stored Abroad Act
The Media Institute – Washington, D.C.
Wednesday, September 16, 2015

I appreciate the opportunity to be with you this afternoon. I particularly want to thank the Media Institute for inviting me to speak about the Law Enforcement Access to Data Stored Abroad Act—or LEADs Act—a bill aimed at safeguarding data from improper government access.

More than ever before, Americans rely on technology. They rely on their computers, cell phones, tablets, and other devices to access e-mail, texts, tweets, and phone calls. These data-driven technologies present great potential for improving our lives in areas related to health care, financial services, business, and consumer products.

With relative ease, people can transfer vast amounts of data to the cloud, which can be accessed anywhere and anytime. You in the media certainly appreciate the benefits of cloud computing.

Information that once would have been written on a reporter's notepad is now frequently kept in digital form. And it is not kept in the newsroom, but on a server run by a technology company.

The possibilities of data-driven technologies are endless and have already provided us with more efficient choices. But our digital world presents privacy and transparency challenges that merit everyone's attention.

In light of new forms of electronic communication and data storage, Congress must act to harmonize our nation's privacy laws with present realities to keep up with technological advances.

Most immediately, we need to update the Electronic Communications Privacy Act—or ECPA—to require a search warrant for <u>all</u> e-mail content within the United States.

Enacted in 1986, ECPA prohibits communications service providers from intercepting or disclosing e-mail, telephone conversations, or data stored electronically unless such disclosure is authorized.

As this morning's Senate Judiciary Committee hearing confirms, virtually everyone agrees that Americans should enjoy the same privacy protections in their online communications that they do in their offline communications. But Congress has not adequately updated the law since its enactment, and technological developments have resulted in disparate treatment between online and offline communications.

To make matters more complicated, ECPA is silent on the privacy standard U.S. officials must satisfy in order to access data stored abroad. And the federal government has taken advantage of this statutory silence to apply its own standard.

Currently, the U.S. government takes the position that it can compel a technology company to turn over data stored anywhere in the world, belonging to a citizen of any country, so long as the data can be accessed in the United States.

The issue of how far abroad, and under what circumstances, a U.S. search warrant may reach is being litigated before the Second Circuit, where Microsoft has challenged the use of an ECPA warrant to access e-email content stored on a server in Dublin, Ireland.

Last week, a three-judge panel of the U.S. Court of Appeals for the Second Circuit heard oral arguments in the case. Referencing Congress's failure to predict the global nature of the Internet in 1986 when ECPA was enacted, Judge Susan Carney observed that Congress did not seem to have anticipated the Internet in the statute.

The Court also recognized that it is dealing with an out-of-date statute, as Judge Gerard Lynch noted in his concluding remarks: "[T]he one thing that probably everyone agrees on is that, as so often, it would be helpful if Congress would engage in that kind of nuanced regulation, and we'll all be holding our breaths for when they do."

While we do not yet know the outcome of this case, the government's position regarding the reach of its warrant authority has significant implications for both the technology companies that store data abroad and the individuals and businesses whose data is stored.

The government's position presents unique challenges for a number of industries, which increasingly face a conflict between American law and the laws of other countries. For example, when technology companies receive demands from U.S. law enforcement to turn over data on behalf of foreign customers, they are forced to make a difficult decision: either comply with the demand and satisfy U.S. law or risk violating the privacy laws of the host country.

No one should be placed in this untenable situation.

Moreover, if federal officials can obtain e-mails stored anywhere in the world simply by serving a warrant on a provider subject to U.S. process, nothing stops governments in other countries—including China and Russia—from seeking e-mails of Americans stored in the U.S. from providers subject to Chinese and Russian process.

Lest you think there are no reciprocal or far-reaching consequences, imagine a scenario where China wants to access e-mails stored in the United States. Instead of going through established diplomatic channels or international treaties to obtain those e-mails, Chinese officials could go to a China-based company, like Ali Baba, and demand that it retrieve e-mails from its U.S. servers and turn them over.

This disturbing hypothetical could well become a reality because of our government's position on the extraterritorial reach of U.S. warrants. In fact, the lawyer who is litigating the Microsoft case on behalf of the government acknowledged last week that the ability for a foreign government to require disclosures of a U.S. provider "should be of some concern."

As media organizations, you are particularly sensitive to these issues. Here in the United States we respect free speech and media independence. Your newsrooms are free from government search or censure. Yet, because of this Administration's position on the extraterritorial reach of warrants, your rights could be circumvented by foreign law enforcement agencies seeking to access your confidential information—even if it is stored in the United States.

Recognizing the dangerous precedent our government's position could set, a group of media organizations filed an amicus brief in the Second Circuit case.

Let me read an excerpt from their brief: "[F]or those countries that are already taking extra-legal measures to try to penetrate and monitor journalists' e-mails, the government's position offers a far easier approach: simply raid the local office of a service provider and demand that a local employee retrieve the desired information remotely from U.S.-based accounts. This scenario would cause certain outrage in the United States—and rightly so."

Without an appropriate legal framework, the current state of affairs regarding extraterritorial use of warrants puts the privacy of American citizens at risk.

That is why I introduced the LEADS Act: to promote international comity and law enforcement cooperation. To date, the bill has received broad bipartisan support in both the Senate and the House of Representatives and from trade associations and the business community.

The proposed legislation would clarify ECPA by stating that the U.S. government cannot compel the disclosure of data from U.S. providers stored abroad if (1) accessing that data would violate the laws of the country where it is stored or (2) the data is not associated with a U.S. person—that is, a citizen or lawful permanent resident of the United States, or a company incorporated in the United States.

In instances where the laws of the U.S. and the laws of a foreign country conflict, law enforcement would be required to work with their foreign counterparts to access the data. The U.S. already does this through the Mutual Legal Assistance Treaty (or MLAT) process, which facilitates formal agreements for sharing evidence between the United States and foreign countries.

The LEADS Act also improves the MLAT process by making it more transparent and streamlined. The current process is slow and unreliable, sometimes taking several months to access data held by foreign jurisdictions. Not only does the Department of Justice need additional funds to hire more people to handle MLAT requests, but reforms to the underlying program are also needed to improve transparency and efficiency.

Finally, the Act recognizes via a Sense of Congress that data providers should not be subject to data localization requirements. Such requirements are incompatible with the borderless nature of the Internet, are an impediment to online innovation, and are unnecessary to meet the needs of law enforcement.

Of course, the LEADS Act as currently written is just one approach to resolving this complex area of the law. I am open to other ideas as well and want to ensure that the ultimate approach we take accounts for all situations and business models. For example, instead of focusing on where

the data is stored, we could focus on the nationality and location of the user. My office is currently engaged with a variety of stakeholders to strike the right balance.

In the end, we must strengthen privacy and promote trust in U.S. technologies worldwide while still enabling law enforcement to fulfill its important public safety mission.

Thank you, again, for having me this afternoon.

As you can see, there is a lot we must do to establish a functional legal regime to safeguard electronic communications stored at home and abroad. And I intend to do everything in my power to update our privacy laws.

###