

June 14, 2017

The Honorable Bob Goodlatte  
Chairman  
Committee on the Judiciary  
United States House of Representatives  
Washington, District of Columbia 20515

The Honorable John Conyers  
Ranking Member  
Committee on the Judiciary  
United States House of Representatives  
Washington, District of Columbia 20515

Dear Chairman Goodlatte and Ranking Member Conyers,

We strongly support your efforts to continue this Committee's examination of potential updates to the Electronic Communications Privacy Act (ECPA) by holding the hearing "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era." ACT | The App Association represents more than 5,000 app makers and connected device companies throughout the mobile economy. Our members are industry leaders and innovators whose products improve productivity, accelerate learning, deliver entertainment, and promote healthier lifestyles.

Our members depend on cloud computing to deliver their services to domestic and international customers and expand their businesses around the globe. In fact, cloud computing provides a platform that allows small- and medium-sized tech firms like our members to compete and succeed in an environment driven by large companies. We therefore appreciate this Committee's work to secure the passage of the Email Privacy Act (H.R. 387) through the full House of Representatives this year. If enacted, this legislation would ensure that a warrant is required to obtain communications content, even when it is stored in the cloud for more than 180 days.


However, the ECPA framework for law enforcement requests abroad remains outdated, and we are gratified that this hearing draws on a variety of stakeholders to begin addressing this issue. Smaller companies bear the brunt of the challenges created by the ambiguity under ECPA. Enacted in 1986, ECPA was intended to govern when and how U.S. law enforcement agencies may access data stored digitally by U.S. companies. However, a recent decision by the U.S. Court of Appeals for the Second Circuit held that under ECPA U.S. law enforcement agencies may not use a warrant to obtain digital communications content stored abroad. This determination, along with conflicting decisions by judges in other circuits, has injected new urgency into the need for congressional action in this area.

#### **I. Ambiguity in Current Law Disadvantages American Small- and Medium-Sized Firms**

Every day, 2.5 quintillion bytes of data are created on the internet, and our members provide apps or platforms that require the transmission, storage, or processing of that data across international borders. Without clarity under ECPA as to when and how U.S. law enforcement may access data stored overseas, our members, and businesses of all sizes, face uncertainty and serious threats to their operations and success.

Our members design and maintain the software components of everything from the internet of things (IoT) to back-office inventory management. They contribute to a rapidly growing, \$143

1401 K Street NW Suite 501  
Washington, DC 20005

 202.331.2130

 @ACTonline

 ACTonline.org

 /actonline.org

billion app ecosystem, without which the \$8 trillion IoT revolution would not be possible.<sup>1</sup> Moreover, sharing and storing data in all corners of the globe is an integral part of their business model. Small- and medium-sized enterprises that use the internet for global trade have a survival rate of 54 percent, which is 30 percent higher than companies that operate offline.<sup>2</sup> The expansion, and even the survival, of these companies is at stake when the law governing international data storage is unclear.

Our members support law enforcement officials and will comply with reasonable warrant requirements to help officers perform their job effectively. However, ECPA’s ambiguity creates a legally and financially untenable environment for owners of small businesses, who struggle to discern which law governs, especially in the context of extraterritorial warrants. For example, when a U.S. court issues an extraterritorial warrant to obtain the communications data of a foreign person that is stored outside of the United States, the U.S. court’s action may conflict with the laws of the foreign country where the data is stored. This puts our members in the conundrum of either complying with the U.S. warrant and disobeying the foreign jurisdiction’s laws; or abiding by foreign law and refusing the U.S. warrant. In short, a company should never have to decide which legal framework to follow, and which to violate. Congress must act to provide clarity and eliminate the challenges this ambiguity creates.

Although various parties are litigating this issue in federal court, Congress is better equipped to resolve the complex issues at stake in this debate. Courts can only decide the cases and controversies before them, and they are therefore limited to piecemeal remedial measures, which can take decades to resolve. The direct conflicts between extraterritorial warrants issued by U.S. investigators and foreign laws, coupled with the need to update mutual legal assistance treaties (MLATs), pushes the matter beyond the scope of the controversies before the courts. Moreover, it is the responsibility of Congress to ensure the agreed upon framework remains appropriate for anticipated future developments. This is why we agree with U.S. Court of Appeals Circuit Judge Carney’s statement that ECPA is “overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs . . .”<sup>3</sup>

Beyond the immediate concerns addressed above, our members continue to lose business due to the perceived lack of restraint on U.S. law enforcement under existing statute. For example, European firms have repeatedly declined to partner with U.S. software service providers because their status as American companies might avail U.S. agencies of the ability to obtain communications data from them, even if the data pertains to Europeans. This apprehension to partner and invest hurts our economy generally, and it undercuts opportunities for the app developer community specifically. While cloud computing should provide smaller companies with the ability to expand overseas at unprecedentedly low cost, our laws are pulling back on that progress.

## **II. Ambiguity in Current Law Ultimately Disadvantages U.S. Law Enforcement**

The fact that ECPA has been “left behind by technology”<sup>4</sup> surely disadvantages tech firms, but U.S. law enforcement agencies stand to lose as well. If the United States continues to proceed as though ECPA authorizes extraterritorial warrants without regard to conflicts with foreign

<sup>1</sup> See [http://actonline.org/wp-content/uploads/App\\_Economy\\_Report\\_2017\\_Digital.pdf](http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf)

<sup>2</sup> WORLD ECONOMIC FORUM, GLOBAL INFORMATION TECHNOLOGY REPORT 2016 41 (2016), available at [http://www3.weforum.org/docs/GITR2016/WEF\\_GITR\\_Chapter1.2\\_2016.pdf](http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf).

<sup>3</sup> See *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 14-2985, Dkt. 328 (2d Cir. Jan. 24, 2017) (Carney, J., concurring in denial of rehearing en banc).

<sup>4</sup> *Id.*

jurisdictions, other countries could begin to follow suit. As a result, foreign governments may stop coordinating their efforts with U.S. agencies, especially when their investigations involve data stored in the United States, or when data pertains to U.S. persons. Cooperation between governments suffers, and U.S. law enforcement is disadvantaged as a result. Moreover, issuing warrants under ECPA that conflict with foreign legal regimes encourages other governments to require the localization of data otherwise accessible to U.S. law enforcement. Data localization policies impede U.S. investigations because data that would otherwise be sent back to the United States to be processed would be required to remain in other jurisdictions. This “balkanization” of the internet would force investigators to make requests through the MLAT process for data that is now available to them in the United States. Pushing foreign governments to adopt localization regimes could result in an “arms race” of countries using technical barriers to prevent access to their citizens’ data.

### **III. The International Communications Privacy Act (ICPA) Provides a Solid Foundation to Begin Legislative Work**

It has been suggested that legislation should simply repeal the Second Circuit decision. However, such a proposal would authorize extraterritorial warrants for any data a U.S. company stores overseas. This would be an incomplete solution, causing more conflicts with foreign laws—not less—and leading to negative consequences for U.S. businesses and consumers. Instead, we urge Congress to address this matter fully, as the legislative branch is the proper venue to deliberate the international and forward-facing issues at stake.

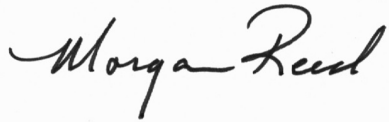
Introduced last Congress, ICPA would authorize U.S. law enforcement agencies to issue extraterritorial warrants under certain circumstances. When requesting communications data pertaining to a U.S. person, regardless of where the data might be stored, ICPA would amend ECPA to clearly authorize law enforcement to issue an extraterritorial warrant. However, if the data pertains to a person who is a national of or located in a country with which the United States has an MLAT, ICPA would only authorize U.S. law enforcement to obtain a warrant if that country does not object after receiving notice. ICPA would also make important updates to U.S. administration of MLAT requests and require a study on foreign governments’ execution of U.S. requests. These necessary steps would help improve and update the MLAT process.

Some commenters have raised objections related to the process in ICPA for foreign countries to object to data requests from U.S. law enforcement agencies. We believe the investigative necessity of obtaining communications content stored abroad can be addressed while also preventing unnecessary conflicts of law. We would support reasonable amendments to ICPA, consistent with the interests of comity, strong privacy protections, and the protection of due process rights. We urge this Committee to expeditiously take up legislation based on ICPA and welcome a robust legislative process.

### **IV. Conclusion**

If we allow conflicts between U.S. and foreign data access laws to continue, we risk quietly killing our most productive businesses and stifling our fastest-growing, most innovative sectors. For these reasons, the App Association members support reform legislation that clarifies lawful access to data, patterned on ICPA. We hope the Members of this Committee consider these factors as they continue their legislative work in updating ECPA in the 115<sup>th</sup> Congress.

Sincerely,



Morgan Reed  
President  
ACT | The App Association

Dear Honorable Member of Congress,

As a coalition of small and medium-sized mobile application companies driving innovation across the country, we urge you to update the Electronic Communications Privacy Act (ECPA), a law that was written in 1986 and is incongruent with today's cloud computing reality.

Considering the 2.5 quintillion bytes of data created and shared on the internet daily, ECPA is an outdated statute that does not account for the transitory nature of data today. The law's failure to address when and how U.S. law enforcement may access data stored abroad not only creates uncertainty, but it also presents a real threat to our businesses. While a major concern for big companies, the legal conflicts created through ambiguous ECPA legislation also pose dire consequences for small companies. When U.S. law enforcement seeks our data in a manner that conflicts with other sovereign laws, our small teams lack the robust legal departments or funds to address foreign governments in court. We are left with an untenable dilemma: either abide U.S. law enforcement and challenge sovereign governments, or cooperate with foreign governments and disobey domestic authorities. We don't have an easy answer. But you can help.

Last year, the International Communications Privacy Act (ICPA) was introduced to clarify the ambiguity under ECPA in a manner that avoids unnecessary conflict with international laws. Forthcoming legislation modeled after ICPA, with expected adjustments to ensure the Department of Justice can effectively conduct international investigations, would achieve these goals and help American app companies of all sizes continue to thrive in the global economy. We urge you to join your colleagues to modernize ECPA and clarify lawful access to data.

For more information or to join the effort, please contact **Senators Orrin Hatch or Chris Coons, or Representatives Tom Marino or Hakeem Jeffries.**

Sincerely,

Ann Adair  
Thinkamigo  
Tampa, FL

Christopher Adams  
Southern DNA  
Atlanta, GA

Bruce Backa  
NTP Software  
Nashua, NH

Joe Bonnell  
Alchemy Security, LLC  
Denver, CO

Luke Chung  
FMS, Inc.  
Vienna, VA

Libby Curran  
The Learning Train  
Wilmot, NH

Natalie Divney  
ND Consulting  
Ashburn, VA

Nicholas Emery  
Kosmik Koding  
Savage, MN

Jordan Epstein  
Stroll Health  
Berkeley, CA

Betsy Furler  
Communication Circles  
Houston, TX

Jeff Hadfield  
1564B  
Sandy, UT

Emily Hart  
MotionMobs  
Birmingham, AL

Greg Haygood  
Southern DNA  
Atlanta, GA

David Heenan  
Aces Health, INC  
Atlanta, GA

1401 K Street NW Suite 501  
Washington, DC 20005

 202.331.2130

 @ACTonline

 ACTonline.org

 /actonline.org

Marcus Hogue  
AppDynamics  
Bartlett, IL

Sebastian Holst  
Preemptive Solutions  
Chagrin Falls, OH

Maureen Homnick  
Homnick Systems  
Boca Raton, FL

Patrick Larsson  
Happi Papi LLC  
Sarasota, FL

Tyler Leonard  
Dogtown Media  
Venice, CA

Mark Liber  
StartUp Health  
New York, NY

Mike Meikle  
secureHIM  
Richmond, VA

Dave Noderer  
Computer Ways, Inc.  
Deerfield Beach, FL

Taylor Peake  
MotionMobs  
Birmingham, AL

Mike Sax  
Wellbeyond  
Ewugene, OR

Gomathy Shankaran  
Kidz Learn Applications  
Edison, NJ

David Shear  
SheerID  
Eugene, OR

Chris Sims  
Sigao Studios  
Millbrook, AL

Alice Thacker  
You42 Inc.  
Cumming, GA

Charlotte Tschider  
Cybersimple Security  
Minneapolis, MN

Scott Weiner  
NeuEon  
Mansfield, MA

Ray Wijangco  
Box  
Chicago, IL

Bill Wolff  
Agility Systems  
Dresher, PA