

May 24, 2017

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
Subcommittee on Crime and
Terrorism
United States Senate
Washington, District of Columbia 20510

The Honorable Sheldon Whitehouse
Ranking Member
Committee on the Judiciary
Subcommittee on Crime and
Terrorism
United States Senate
Washington, District of Columbia 20510

Dear Chairman Graham and Ranking Member Whitehouse,

We strongly support your efforts to examine a critical policy issue for our members by holding the hearing “Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights.” 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 emerging 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 mid-sized tech firms like our members to compete and succeed in an environment driven by tech titans. However, smaller companies bear the brunt of the challenges created by the ambiguity within the existing Electronic Communications Privacy Act (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, as the witnesses in today’s hearing indicate, the law does not clearly state whether a warrant issued under ECPA may be served for communications data pertaining to foreign persons and stored overseas.

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 in 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 billion app ecosystem, without which the \$8 trillion IoT revolution would not be possible. 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 who operate offline.¹ 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 court's action may conflict with 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 that foreign jurisdiction's laws, or abiding by foreign law and refusing the U.S. warrant. In short, a company should never have to parse and decide with which legal framework to follow. 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 . . ."²

¹ WORLD ECONOMIC FORUM, GLOBAL INFORMATION TECHNOLOGY REPORT 2016 41 (2016), *available at* http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf.

² *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).

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”³ 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 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 then disadvantaged. Moreover, the current interpretation of ECPA 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 the U.S. 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 U.S. 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) is a Solid Approach

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, ICPA would not authorize an extraterritorial warrant for communications data pertaining to a person from a country with which the U.S. has a current MLAT. In that situation, U.S. law enforcement would

³ *Id.*

only be authorized to issue a warrant if that country does not object within 60 days.

ICPA would also make important updates to U.S. administration of MLAT requests and require a study on the execution of U.S. requests of foreign governments. These necessary steps would help improve and update the MLAT process. We urge this Subcommittee, as well as the full Judiciary Committee, to expeditiously take up legislation based on ICPA.

IV. Legislation Addressing This Issue Should Require a Warrant for Communications Content

For App Association members, clarifying lawful access to data overseas without updating ECPA's warrant for content requirement would be a missed opportunity. ECPA was enacted with a provision allowing law enforcement to obtain the content of electronic communications without a warrant as long as the content is stored in the cloud and is at least 180 days old. Communications older than six months—treated with lower due process protections ostensibly because the law considers them abandoned—could be obtained through less rigorous processes, such as subpoenas issued by prosecutors or FBI agents. Law enforcement officials need not show probable cause to a judge to obtain a subpoena.

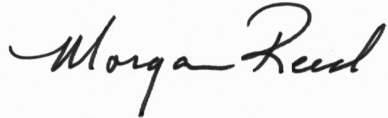
The glaring issue with this treatment of private e-mails is that most of our communications are now stored in the cloud. Tech firms, including our members, store private messages on remote servers all the time because such storage is inexpensive and highly efficient. In addition, service providers can store messages for much longer because cloud storage is much less costly. There is no longer any reason to believe e-mails from 180 days ago are any less private or sensitive than those sent today. In 1986, it might have made sense to treat e-mails stored in the cloud as abandoned after six months, but this argument no longer holds water in our current environment.

To remedy the incongruity in the law, ECPA reform legislation should subject stored communications to the warrant standard, regardless of how long the communications have been stored on a remote server. Private emails from September 2016 should receive the same protections as emails from last month. This would help align legal safeguards with our common expectation of privacy. Moreover, without this update to the ECPA law, it could defeat the purpose of the other changes ICPA seeks to make. If law enforcement can unilaterally serve an extraterritorial subpoena for content stored overseas for longer than 180 days, the limited authorization for extraterritorial warrants elsewhere in the bill for newer communications is less meaningful. We urge the members of the Subcommittee to take this consideration under serious review as they explore legislation to resolve this issue.

V. 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 Subcommittee consider these factors as they embark upon the legislative process to update ECPA in the 115th Congress.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is written in a cursive style with a large, prominent "M" and "R".

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

1401 K Street NW Suite 501
Washington, DC 20005

 202.331.2130

 @ACTonline

 ACTonline.org

 /actonline.org

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