

February 22, 2018

The Honorable Chuck Grassley  
The Honorable Dianne Feinstein  
The Honorable Orrin Hatch  
The Honorable Lindsey Graham  
The Honorable Sheldon Whitehouse  
The Honorable Chris Coons  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

**RE: CLOUD Act and law enforcement access to digital evidence**

Dear Senators Grassley, Feinstein, Hatch, Graham, Whitehouse, and Coons:

We write in support of the CLOUD Act of 2018 as a stand-alone remedy for some of the digital evidence access challenges that U.S. law enforcement agencies encounter when data is stored on servers located in other countries. However, if Congress acts on the CLOUD Act, it should do so separate from consideration of a more far-reaching update of the Electronic Communications Privacy Act (ECPA), such as the pending Email Privacy Act.

It has been our long-held position that Congress should ensure any comprehensive ECPA update must address law enforcement concerns about access to digital evidence regardless of where it is stored. As it stands today, the Email Privacy Act fails to address those concerns.

The CLOUD Act is a welcome fix to one digital evidence access challenge, but it should be part of a larger effort to improve the current compliance environment and ensure that law enforcement can obtain the evidence that we need to accomplish our mission without unnecessary delays or obstacles. Refusals by service providers to comply with US legal demands based on a foreign evidence objection introduced a new problem into an already challenging environment. So, this fix will support our public safety mission if comity objections are not abused, if the bilateral agreements themselves support the whole range of state and local law enforcement needs for evidence, and if any additional ECPA reform efforts address the updates which we believe are essential for public safety in the 21st Century.

With those caveats, we are assured that appropriate stakeholders have come together in good faith to remedy an acute problem for everyone involved, and we support the CLOUD Act's passage.

All parties agree that the current situation is untenable: evidence that can help solve crimes committed in the United States by people in the United States against victims in the United States is unavailable even after a judge has signed a warrant. We also understand that as significant a barrier to our operations as these denials are, they create a critical evidence gap for our closest foreign allies, as U.S. companies following these practices command a large share of the global communications traffic. Crime increasingly ignores national borders, and we believe our colleagues fighting the same fight in allied democracies should have access to the evidence that they need as well. We welcome the solution that the CLOUD Act provides, as long as it is implemented and interpreted consistent with our understanding as noted above. We urge

Congress to consider it a model of collaboration among stakeholders, and to bring all parties to the table to seek a similar balanced solution to the problems with the broader ECPA regime.

It is critical that law enforcement investigators have a clear and efficient path to lawfully obtain digital evidence from the service providers who hold it. We have long pointed out that the careful balance between privacy and the needs of public safety struck decades ago has been eroded, because communications technology has evolved in the absence of compliance standards for response to our legal demands. A sampling of the most pressing problems we have repeatedly identified in the existing ECPA regime includes a lack of legal structure around retention of evidence and timeliness of response, a lack of clear communication about the types of evidence service providers are holding, and an existing emergency access provision that leaves determinations of exigency in the hands of industry rather than public safety professionals.

These issues should be addressed in a comprehensive way. As we have consistently stated, the state and local law enforcement community agrees that laws like ECPA that govern access to digital evidence should be updated. But any update should remove unnecessary barriers to accessing digital evidence, restore balance, and consider public safety equities on a par with the interests of industry and individual privacy.

Sincerely,

Association of State Criminal Investigative Agencies  
Federal Law Enforcement Officers Association  
Major Cities Chiefs Association  
Major County Sheriffs' Association  
National District Attorneys Association  
National Sheriffs' Association