Written Statement by

Richard Littlehale
Special Agent in Charge
Tennessee Bureau of Investigation

Before the United States House of Representatives Committee on the Judiciary

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 speak to you today. I am the Special Agent in Charge of the Technical Services Unit of the Tennessee Bureau of Investigation, the high-tech investigative unit of Tennessee's statewide criminal investigation agency. I offer testimony as a representative of the Association of State Criminal Investigative Agencies (ASCIA). The Director of the Tennessee Bureau of Investigation, Mark Gwyn, is the current president of ASCIA, and I serve as Chair of ASCIA's Technology and Digital Evidence Committee.

For more than 20 years, I have helped law enforcement agencies at all levels of government throughout Tennessee obtain and use communications records in support of their criminal investigations, and I now supervise a unit of specialists who are carrying that mission forward into the digital age. We gather much of this digital evidence through the service of legal demands on a range of private companies, both for use in our own Internet Crimes Against Children (ICAC) and cyber investigations, and in support of cases ranging from searches for violent fugitives to efforts to recover abducted children and victims of minor sex trafficking.

I am grateful to the Committee for the opportunity to share a criminal investigator's perspective on the latest barrier impeding law enforcement's lawful access to the evidence we need to work the digital crime scenes of the 21st century. The recent "*Microsoft Ireland"* decision and its broad application by tech companies has created an unprecedented blind spot in state and local law enforcement's ability to access digital evidence of U.S. crimes stored across global networks.

The current pattern of refusal to respond to U.S. legal demands about evidence created in the U.S. that is needed for U.S. investigations seeking justice for U.S. victims defies common sense. We urge quick action on the problem of law enforcement access to US data stored abroad, and we ask you to continue to consider that we need your help in other areas as well. The evidence regulated by the Stored Communications Act can be invaluable in the most critical of law enforcement investigations, and improvements in the law can help my colleagues and me work faster and more efficiently to bring the guilty to justice and exonerate the innocent. For investigators like me, there is a sense

of frustration when we encounter unnecessary barriers to evidence in an investigation. But our frustration pales in comparison to the feelings of victims and their families if we have to tell them that evidence may exist to help solve the crime, but a court ruling or corporate decision prevents us from getting it, even if we have a warrant signed by a judge.

Barriers to Lawful Access

The digital world holds a tremendous amount of data stored across a range of devices, networks, and systems. Much of that evidence is extremely valuable in a wide range of criminal investigations. That makes it all the more troubling that law enforcement is too often being denied access to that evidence. Law enforcement has a need, but even more, an obligation to seek any evidence relevant to an investigation, and without some measure of access to that evidence, bad outcomes become more likely. We don't need everything, but we find it very problematic that technological or business constraints increasingly have more impact than public safety considerations or the expectations of victims or their families. So while some like to say we are in a "golden age of surveillance," those of us in the trenches protecting the public see things differently.

The barrier to law enforcement access to digital evidence that brings us together today grew out of the 2nd Circuit Decision in Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), sometimes called *"Microsoft Ireland"*. In that case, Microsoft successfully argued that the Stored Communications Act could not be used to compel production of evidence that was created in the U.S. but stored abroad, even though Microsoft could access the data in the United States. Despite a trend in trial courts in other circuits to reject the *Microsoft Ireland* reasoning, Microsoft and other companies continue to apply the standard across the board and reject legal demands across the country.

Federal, state, and local law enforcement across the country rely on the SCA and the legal demands that it authorizes to obtain critical evidence from service providers. In the absence of SCA authority, investigators are told that they must turn to the Mutual Legal Assistance Treaty (MLAT) process. MLATS provide a mechanism for the compelled production of evidence from other signatures through treaty obligations. They are widely regarded in the law enforcement community as a wholly ineffective alternative to obtaining evidence. Delays run from many months to years, and that time frame and the administrative burden that surrounds it simply do not allow investigators to obtain the evidence that they need in a time frame that is useful in most criminal cases. I am aware of a number of cases where the denial letters did not even provide the investigator with any information about what country to direct the MLAT to, if the investigator was willing to weather a 9-month or greater delay.

Further, as significant a barrier to our operations as the data stored abroad denials are, I understand that they are an even greater one for our closest foreign allies, as U.S. companies following the choices noted above command a large share of the market in many countries. My unit has been involved in several cases where the assistance of law enforcement authorities in allied democracies,

coordinated through our federal partners, was instrumental in our success, and it troubles us that the ineffective MLAT process is the only one available to them.

In Judge Lynch's concurrence to the *Microsoft Ireland* panel decision, he writes that he does so "without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy." Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 233 (2d Cir. 2016). We couldn't agree more that the outcome is irrational from a policy standpoint, and that a search warrant from a neutral magistrate settles the privacy equities consistent with our constitutional traditions. This fits into a larger pattern where the technical and legal complexities of running modern multinational networks increasingly impact police officers - mostly at the state and local levels - trying to gather the evidence we need to do our jobs. The human consequences of this state of affairs are significant and growing. We urge Congress to legislate a solution to this problem that puts common sense public safety needs alongside privacy concerns and the business interests of the providers and their customers. Public safety should not be an afterthought or side issue in the advance of technology.

Examples of the Consequences of the Broad Application of *Microsoft Ireland*

Two recent examples highlight the cost of the *Microsoft Ireland* decision and its broad application. The first case is one of many that have been discussed in the Internet Crimes Against Children investigations community, where the effect of this barrier to lawful access is felt very strongly. The second, cited by my colleague Chris Kelly from the Massachusetts Attorney General's Office at the recent Senate Judiciary Committee hearing on this topic, is also alarming.

The first case began when a service provider advised the National Center for Missing and Exploited Children that an unknown party has uploaded known child exploitation images to a cloud email account in November of 2016. The tip was forwarded to a Mississippi ICAC investigator in early January, and the investigator obtained a search warrant for the contents of the account. While waiting for the search warrant proceeds, the investigator continued to work the case, and was able to identify and confront a suspect. The suspect, who was found to be in possession of child exploitation images, confessed that it was his practice to meet people online, establish a relationship, and exchange child pornography in order to receive child pornography in return. When asked whether he ever received pictures that made him think the people sending them were actively molesting children, he stated that he didn't know, but that he was talking with "some very bad, bad people." In early February, the investigator received a "foreign evidence" denial as to some of the requested account contents, despite the fact that everything points to the subject accessing the account from within Mississippi. The investigator sent two responses over the next month requesting any information on how he might obtain the content that could lead to the possible undiscovered minor victims referenced by the subject. As of today's hearing, the investigator has yet to receive a response.

In his testimony before the Senate Judiciary Committee Subcommittee on Crime and Terrorism in May 2017, Chris Kelly mentions a case where California investigators are investigating the disappearance and suspected murder of a young girl. The investigators developed information that the contents of an account maintained with a cloud service provider could help them determine what happened to the girl and where to look for additional evidence. A court agreed and issued a search warrant. The provider objected to production of any content stored outside the U.S., which according to the investigators included all categories of records most likely to be useful in that particular investigation.

Significantly, neither of the legal demands in the examples I just mentioned originated within the 2nd Circuit. The denial letters that I have seen in my work and shared by others all cite the *Microsoft Ireland* decision as the basis for the refusal to provide the evidence, without mentioning whether it is controlling authority in the jurisdiction at issue in the case at hand.

Conclusion

For the reasons discussed above, I urge you to move quickly to address these concerns. As you consider legislation, you will have to consider the question of when to mandate compliance with process. It has been suggested by some that the country of the user should govern, but that ignores the very real challenge in some cases of identifying the country of the user before the account contents are produced. I understand the difficult issues Congress has to wrestle with on this particular question, but an approach that looks to the issuing court's authority over the matter being investigated appears to be the most promising.

The state and local law enforcement community agrees that laws intended to guarantee meaningful law enforcement access to digital evidence like ECPA and CALEA need to be updated to make sense in the digital world of the 21st century, but those updates must be balanced to address the needs of the law enforcement community as well as the privacy concerns of the public and the border-spanning challenges facing global technology companies. We must consider reform of the law surrounding access to digital evidence in the context of the very real and very problematic impact that global pressures have on our ability to keep the public we serve safe from harm, and quickly investigate crimes when they occur.

Thank you for inviting me today. ASCIA is eager to be a constructive partner with the committee and all of the other stakeholders on this issue.