WRITTEN STATEMENT OF

CHRISTOPHER W. KELLY
DIGITAL EVIDENCE LABORATORY DIRECTOR
ASSISTANT ATTORNEY GENERAL
OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL

BEFORE THE UNITED STATES SENATE JUDICIARY COMMITTEE
SUBCOMMITTEE ON CRIME AND TERRORISM

HEARING ON
LAW ENFORCEMENT ACCESS TO DATA STORED ACROSS BORDERS: FACILITATING COOPERATION AND PROTECTING RIGHTS

MAY 10, 2017

Chairman Graham, Ranking Member Whitehouse, members of the Committee, thank you for the opportunity to testify before you today on this important issue. My name is Christopher Kelly and I serve as the Director of the Digital Evidence Laboratory, and an Assistant Attorney General, for the Massachusetts Attorney General. I am also a staff instructor and curriculum developer for the United States Secret Service's National Computer Forensics Institute. During the course of my more than 19-year career as an investigator and prosecutor I have focused almost exclusively on the investigation, prosecution, and forensic examination of digital evidence in criminal cases involving technology.

As the Committee knows, state and local law enforcement and prosecutorial agencies handle the vast majority of criminal cases in this country including murder, rape, robbery, child sexual exploitation, drug offenses, human trafficking, and property crimes. Because technology in our culture is ubiquitous, nearly all criminal activity has a cyber component. Consequently, law enforcement is faced with the continuing mandate, and challenge, to identify, preserve, and analyze digital evidence in the course of these investigations. This evidence can provide powerful, objective facts and information used to prosecute the guilty and exonerate the innocent.

I am here today to testify to the challenges faced by state and local law enforcement from a recent court decision, and the follow-up changes in practice that have impeded our agencies from accessing subscriber data during criminal investigations. It was Congress' intent, with the passage of the Stored Communications Act, that law enforcement personnel, upon service of a judicially authorized search warrant, receive responsive records and content held in storage by United States-based electronic communication and remote computing service providers (hereinafter collectively referred to as "providers"). Congress' intent has been thwarted by a recent judicial opinion restricting law enforcement access to data stored in data centers outside the United States. The Mutual Legal Assistance Treaty (hereinafter "MLAT") process is a proposed solution that is improper, and unworkable. It was developed prior to this advanced technical era and is not suitable as a remedy to this problem. State and local law enforcement need and applaud the Subcommittee for considering an update to existing statutes that will allow us to do our work to enhance public safety in communities across the country.

State and local law enforcement agencies investigating the aforementioned crimes frequently apply for search warrants for the content of communications and files stored by internet, social network, and cellular providers. Law enforcement personnel applying for these warrants seek evidence of criminality in the custody of these providers, using the process Congress specifically prescribed in the warrant provisions of the Stored Communications Act. The evidence sought is generated by or relates to United States residents. This evidence is within the constructive control and custody of companies in the United States. In fact, some companies ensure that only their own representatives *within the United States* can access the data for the purpose of compliance with legal process.

The warrants, applications, and affidavits are approved by judicial authorities in the United States with the Federal and respective state constitutional authority to uphold the law, scrutinize the documents, and prohibit improper searches and seizures. The providers collect, copy, and produce responsive data in the United States. And there are means of redress in the United States for those who can demonstrate some

violation of their rights. This was the legal process contemplated by Congress in the Stored Communications Act and it has been followed by state and local law enforcement officers for years. Though there are other flaws and challenges including the: untimely disclosure of records; potential for loss or deletion of data as a result of current notification standards; and emergency disclosure provisions in need of clarity, the process has worked.

However, the recent Second Circuit opinion in the matter now commonly referred to as "Microsoft Ireland" changed the landscape.[1] In the wake of the decision, many providers changed their process for responding to warrants, and do not fully comply with judicial orders issued in jurisdictions outside the Second Circuit. Significantly, since the Second Circuit denied re-hearing on January 24th of this year, three separate federal district courts have now rejected the Second Circuit's holding and ordered the production of records on similar facts.[2]

There is a significant negative impact on criminal investigations because of this new practice. Concrete case examples help provide context. First, police investigating a case now being prosecuted in Utah received information from a woman who was looking at her minor daughter's phone and opened an application that allowed access to the cloud storage files of the defendant. The woman observed a photograph of the defendant sexually abusing a minor. Police applied for and were issued a warrant to the provider to collect the content of the account. The provider did not comply with provisions of the warrant and police did not obtain copies of the evidence from the provider as a result. Second, law enforcement officers in several agencies investigating online child sexual exploitation offenses, including my own as

[1] *Microsoft Corporation v. United States of America*, 829 F.3d 197 (2nd Cir. 2016) *rehearing denied*, 2017 WL 362795 (2nd Cir. Jan. 24, 2017)

[2] *In the MATTER OF the SEARCH OF CONTENT THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE*, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *IN THE MATTER OF THE SEARCH OF CONTENT THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE*, 2017 WL 1398279 (N.D. Cal. Apr. 19, 2017); *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo and In re: Two email accounts stored at Google, Inc.*, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *IN RE SEARCH WARRANT NO. 16-960-M-01 TO GOOGLE and In re Search Warrant No. 16-1061-M to Google*, 2017 WL 471564 (E.D. Pa. Feb. 03, 2017).

well as other agencies in Massachusetts, Indiana, Vermont, Illinois, Mississippi, New Hampshire, and others have not received data responsive to properly issued search warrants in their jurisdictions. And last, investigators in California are currently investigating the disappearance, and suspected murder, of a young girl. Investigators are aware that there is a cloud account containing photos of the girl that could be instrumental in determining a timeline for her disappearance and possible location. A California court issued a warrant for the account. Here too, the provider did not comply with provisions of the warrant mandating disclosure of certain content.

The responses investigators receive to search warrants for content are problematic. Some providers respond that they do not know whether the data is stored domestically or abroad, and consequently refuse to comply with valid legal process. Others have confirmed that some or all data is stored abroad, and on that basis refuse to comply with valid legal process.

These responses and considerations leave law enforcement in a difficult position. First, the process of applying for search warrants for evidence held by third party providers can be time consuming and happen only after sufficient facts to develop probable cause are confirmed. In that time, data cannot only be moved to data centers outside the country, it can be lost or deleted if not secured. Second, if the MLAT process is the only legal means of obtaining evidence that the provider stores outside the country, but the country cannot be determined, the MLAT process is both the only proper mechanism to obtain it and at the same time rendered completely useless. It is a Catch-22 for law enforcement. Third, if the country can be determined, the MLAT process is slow, time consuming, and costly from a resource perspective. Fourth, if the provider only allows its' United States-based keepers of records to access subscriber account data, a MLA request served on another country would serve no purpose because the company representative within that respective country would never be able to access the data. Fifth, each provider has its own unique network, technical capacity, and constraints.

The end result here is that providers ultimately make the decision on whether or not data – including critical evidence in criminal investigations – is accessible to law enforcement regardless of judicial authorization. This is simply by virtue of how the respective providers' networks operate. That proposition is a significant concern. A clear, singular legal mandate for provider compliance to legal process is the only viable solution. That mandate should be the same regardless of how the providers' network operates. In short, the mandate should be technology neutral. And it should remedy the chaos and confusion caused to the providers in the wake of the Second Circuit's decision. The MLAT process shouldn't be necessary in the first place, and is not a viable solution to this problem.

On behalf of the Massachusetts Attorney General's Office and my colleagues in state and local law enforcement, we urge the Subcommittee to develop a legislative solution that will help us to perform our mission to prevent, investigate, and prosecute crime. The plain language of the Stored Communications Act demonstrates that Congress intended that providers comply with proper judicial orders and produce responsive records and content. That intent should be effectuated as soon as possible.