Written Statement by

Richard Littlehale
Assistant Special Agent in Charge
Tennessee Bureau of Investigation

Before the United States Senate Committee on the Judiciary

Hearing on
"Reforming the Electronic Communications Privacy Act"

September 16, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to speak to you today. I am the Assistant Special Agent in Charge of the Technical Services Unit of the Tennessee Bureau of Investigation. We are the high-tech investigative unit of Tennessee's statewide criminal investigation agency. One of my unit's most important responsibilities is to help law enforcement agencies at all levels of government throughout Tennessee use communications records in support of their criminal investigations. I have used these techniques for twenty years 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 challenges that law enforcement faces when gathering digital evidence. The evidence regulated by ECPA can be invaluable in the most critical of law enforcement investigations, and improvements in the law can help my colleagues and I work faster and more efficiently to bring the guilty to justice and exonerate the innocent. My fellow practitioners and I especially appreciate the signal sent by your invitation to today's hearing, because state and local law enforcement conducts the vast majority of criminal investigations in this country. Since the laws before the Committee today govern our access to much of the digital crime scene, any change in the law will impact us greatly. Our community appreciates your recognition that our expert perspective should be a central consideration of any update to ECPA.

I offer testimony here today 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.

Access to Evidence in the Digital Crime Scene

The crime scene of the 21st century is often replete with digital evidence. This digital crime scene, including electronic communications records in the possession of private companies, often holds the key to solving the case. It also holds the key to ruling out suspects and exonerating the in-

nocent. Investigators' ability to access that evidence quickly and reliably under the law is fundamental to our ability to carry out our sworn duties to protect the public and ensure justice for victims of crime.

To date, the lion's share of the scholarly, media, and advocacy attention given to the question of lawful access to stored content has focused on the level of proof required to obtain digital evidence. This narrow focus neglects a set of critical issues that impact law enforcement's ability to gather digital evidence from private companies every day across the country. I am referring to the quality and character of service provider responsiveness to law enforcement legal demands, as well as well-intentioned but overly burdensome accountability considerations like customer notification and reporting requirements. From the perspective of an investigator working the digital crime scene, these concerns impact our ability to gather the digital evidence we need as much or more than any other, and they have been noticeably absent from the ECPA reform debate.

The simple truth is that legal and technological barriers are not the only ones that keep communications records out of law enforcement hands. In many instances, we are unable to utilize evidence that would be of enormous value in protecting the public because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain. That may be because of technological problems, but just as frequently it is because of **non-technical barriers to access**. The companies that retain these records are often unable or unwilling to respond to law enforcement's lawful demands in a timely manner, and there are few consequences for an incomplete or inaccurate response. The primary emergency disclosure provision in the section of ECPA that we use to obtain stored content is **voluntary** for the providers, not mandatory, and even where emergency access is granted to law enforcement, in some instances, there is insufficient service provider compliance staff to process legitimate emergency requests quickly.

As Congress considers simplifying the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to obtain those records, the full range of non-technical barriers to access must have a place in the discussion. I would urge Congress ensure that regardless of the level of process it ultimately decides is appropriate, that steps are taken to guarantee that law enforcement will be able to access the digital evidence that we need to do our jobs reliably and quickly once that process is obtained.

In an effort to better inform the committee, I solicited feedback on these non-technical barriers to access from a wide range of law enforcement agencies, specialties, and investigative focuses. More often than not, the responses were along the lines of "oh, you mean beyond the usual?" Beyond routine turnaround times measured in months, the inability to speak to a human being about your case in a timely manner, uneven access to records in emergencies? Beyond service providers who routinely pre-litigate the legal process instead of leaving that to the courts, who return legal demands without complying because the demand failed to use the magic language of the moment that the provider prefers, regardless of whether or not it is statutorily or constitutionally compelled? These are the day-to-day realities of professionals working the digital crime scene, not isolated and unfortunate bumps in the road.

Consider a case a few years ago regarding the stranger abduction of a 4-day-old infant in Nashville where my unit was tasked to work the digital crime scene. Over the course of an intensive

four-day investigation, my unit processed and explored leads on hundreds of telephone numbers, social media accounts, computers and mobile devices. At a time when every second counts, my fellow agents and I spent a significant amount of time simply trying to make contact with various providers to declare an emergency, calling and recalling to make sure that our process was received and expedited as necessary. In one instance, a voice mail that contained potentially critical evidence for the prosecution of the kidnapper was lost because a cellular provider mishandled a preservation request. In another, we had to spend precious time trying to get a service provider on the phone to figure out the time stamps of phone records, because it was unclear on the face of the records when the critical calls were made. All while processing hundreds of electronic leads, any one of which could be the one that holds the key to rescuing the victim. These issues are obviously problematic, but this is a routine part of a criminal investigator's day working the digital crime scene.

Another example that highlights a need for reform of current law started with a threat of a mass casualty attack on a high school in a large Texas city. An unknown party threatened a high school and responding police in March of 2015 on a popular social media platform, and backed it up with a picture of an assault rifle; this caused the school to go into lockdown. Law enforcement issued a subpoena and a judicial non-disclosure order (to keep the provider from notifying the user) to attempt to identify the user who posted the threat. Even though the threats were posted on the social media provider for everyone to see, the provider still would not turn over records under the emergency exception and required law enforcement to get a search warrant before they would release content. Fortunately, the attack did not materialize that day, and investigation continued. By late April, investigators had determined that the sender used a free virtual private network (VPN) service to mask their Internet Protocol address while posting the threats, and issued a court order to the VPN provider. Two and a half weeks later, they received a response stating that the provider found no responsive records, and indicated that "unfortunately due to limited resources our logs are purged at the latest every 48 hours." Was the threat real, or a hoax? Was the sender serious about the attack but deterred by the lockdown, or simply wasting resources and scaring children for their own amusement? Texas authorities may never know.

The Leahy-Lee ECPA Amendments Act, as introduced, could have the effect of providing more protection for digital evidence than evidence in the physical world, and does nothing to address the range of concerns that the above examples illustrate. That is a major concern, and if the intent is to bring the law into balance for the 21st Century, we strongly believe legislation should not create higher protections for a particular piece of evidence that is stored electronically rather than in a filing cabinet, nor should it elevate burdens on law enforcement without providing assistance with long-standing problems like the ones outlined below.

Non-Technical Barriers to Access

As we consider non-technical barriers to access in more detail, we should be mindful of a simple fact that is often overlooked in the public discourse on this topic: we are talking about law enforcement's ability to gather **evidence**. Not "information" or "content" or "communications records," but **evidence**. All hammers are tools; a hammer only becomes evidence if it is relevant to a criminal investigation. Similarly, law enforcement has no interest in communications records unless they advance a criminal investigation, whether to prove guilt or exonerate the innocent.

Timeliness and quality of service provider response. The importance of the timeliness and quality of service provider responses to lawful demands from criminal investigators for digital evidence cannot be overstated. Of all the issues that we are concerned about in this ECPA reform discussion that could increase the safety of the American citizens we serve without negatively impacting their privacy, this is the most significant. When we get the legal process that we need, let's make sure we get the records quickly, and make sure that they are complete and responsive. Let's minimize administrative latency in the compliance process. That is what would help us solve crimes more effectively.

There is no requirement in current law – including the service and execution of search warrants based upon probable cause – for providers to respond in a timely fashion to lawful process requests by governmental entities. Voluntary compliance has not worked as effectively as we need, because a truly efficient compliance operation might put a provider at a competitive disadvantage, because their competitors aren't required to spend the same resources. Any contemplated change in the law that would result in a lengthening of the investigative timeline – including moving some evidence to a probable cause standard that can currently be obtained on a lesser showing – should be accompanied by provisions that ensure accountability and prompt response by service providers to legitimate law enforcement requests.

It is worth considering the traditional legal framework surrounding search warrants as we consider these questions. We should keep in mind that in a traditional context, when law enforcement demonstrates probable cause to a neutral magistrate and the magistrate issues a warrant, it then becomes the law enforcement officer's decision about when to execute the warrant, how hard to search, and so on, based on the facts and circumstances of the case. In the digital space, it is the providers who actually conduct the search. Law enforcement typically has no visibility into the process of conducting the search or how thorough the search is. This results in sometimes haphazard diligence with respect to compliance, incomplete responses, and turnaround times measured in weeks and months.

Further, service providers often "pre-litigate" search warrants, returning them without being executed because of some perceived defect in language in the warrant. That is unheard of in other contexts; law enforcement gathers the evidence that they feel is responsive to the warrant, and then the defendant has an opportunity to challenge that collection later. The only option to really explore this would be to ask the prosecutor to seek a show cause hearing, and it is difficult to find the time for that when you are looking for a missing child or dangerous fugitive. As a result, this practice on the part of service providers goes largely unchallenged. This would be unheard of outside the digital space: when law enforcement demonstrates probable cause to a neutral magistrate and obtains a search warrant, we decide what evidence to gather and when we gather it, and any aggrieved party has the ability to object later through the courts. By creating a statutory requirement for responsiveness that looks more like response to legal demands in the physical world, this Committee would give law enforcement and industry a benchmark to ensure fairness across the industry, transparency for citizens, and adequate safeguards for public safety.

I have heard some service providers cite the high volume of law enforcement requests as a reason for response times that stretch into months, threatening the underlying investigation. We

have heard they do not have the staff necessary to process the volume of requests quickly. While staffing levels are obviously the prerogative of the company, we understand the difficulty of assigning new resources to an activity that is not a profit center. But the consequences of these decisions in world of criminal investigations is significant. Further, many of these providers are in the business of finding technological solutions to just this kinds of problem - automating processes to enhance efficiency and accountability and share information effectively. They are well acquainted with monitoring customer service centers and determining adequate staffing levels. The people on the other end of the line when we call providers are often very knowledgeable and helpful, and they often demonstrate significant interest and investment in our cases. It is not a matter of their willingness, but rather the resource allocation decisions made at different levels.

Since providers have little economic incentive to innovate or increase staffing levels in their compliance shops, a reasonable legal requirement for responsiveness may be part of the solution to these problems. Such a solution need not be overly costly or burdensome. Congress can protect citizens' privacy and at the same time ensure that victims of crime see justice done thanks to the persistent work of investigators who have timely and reliable access to evidence. Any reform of ECPA should take this issue into consideration.

Notification provisions may put a significantly greater and more costly administrative burden on law enforcement. Several ECPA reform proposals have borrowed language from wiretap law requiring notification of customers of legal demands, or securing a series of separate court orders delaying notification. These provisions risk diverting critical law enforcement resources from investigations simply to comply with burdensome notification provisions or delay orders. We would urge the committee to carefully balance the need for notification and reporting against the resources it will drain away from a range of investigative priorities. In addition, due to the nature of investigations today and the way people create accounts, there is no way to clearly understand - within the timeframes specified in pending ECPA reform legislation - who exactly is to be notified. How much time must investigators spend chasing down parties to notify, rather than working their investigations?

Concerns about the volume of law enforcement legal demands. As I address the issue of volume of legal process and its effect on timeliness of service provider response, I must also address a common talking point about those who would further restrict law enforcement access to stored content: namely, that the number of law enforcement requests for this information is growing. Our response is simple: of course it is. That is because in the digital age, a growing percentage of the available evidence in any criminal case is going to exist in the digital crime scene. Communications records have taken their place alongside physical evidence, biological evidence, testimonial evidence, and the other traditional categories. Laws and policy should reflect this reality and ensure law enforcement access to evidence that by its nature can't make a mistaken identification in a lineup or testify untruthfully, and should further ensure that law enforcement does not face greater obstacles to gathering digital evidence that we do to the other types.

A casual review of transparency data supplied by major service providers will disclose that law enforcement legal demands affect only a tiny percentage of accounts. I encourage the committee to keep these numbers in mind when some parties claim that law enforcement is "snooping" without regard to privacy. When we request these records, it is for a reason – we believe that the

records constitute evidence that will help us identify sexual predators, recover kidnapping victims, successfully prosecute murderers. Any consideration of changes to ECPA that will make obtaining communications records more time-consuming and laborious should reflect an understanding of how those changes will impact our ability to do our job, and whether or not the public would truly be upset about the balance as it is currently struck.

Current emergency provisions within ECPA are not adequate to allow law enforcement to respond effectively in all cases. Few dispute that law enforcement should have rapid access to communications records in a life-threatening emergency, but few outside of our community truly understand how flawed the current emergency options are. The "emergency" provision in current law (18 USC 2702(b)(8)) puts the decision to release records before legal process is obtained, and about whether a situation is an "emergency," in the hands of the provider, rather that the law enforcement experts who are the boots on the ground. This has led to situations where responses to legitimate law enforcement requests have been delayed. In some cases, providers make a decision never to provide records in the absence of legal process, no matter the circumstances, as baffling as that may sound in the light of day.

Another Tennessee case comes to mind; once again, my unit was handling the communications component of an AMBER Alert investigation. One of the many leads that we received about someone who might have knowledge of the missing child's location appeared in a post on the site of a social media provider. Keep in mind that when we contacted them, this was only one of a flood of leads, any one of which could be critical to rescuing the victim. We can't know which one until we receive the evidence we need. That social media provider told us that while they agreed that the situation was an emergency, they were aware that the emergency provision in ECPA was permissive rather than mandatory, and it was their policy never to provide records on an exigent basis; they always wanted legal process (in this case, a search warrant) first. Could we have found the victim sooner, and spared them additional time in the hands of their abductor? We'll never know.

We would further point out that 18 USC 2258, which has been erroneously cited as an emergency option for law enforcement in child exploitation cases, is in fact a requirement that service providers send information about online child exploitation to the National Center for Missing and Exploited Children. Law enforcement cannot use it as a means to obtain records directly. The service providers still require legal process or an emergency declaration under 2702 before they will provide the evidence that generated the referral to law enforcement.

Any effort to reform ECPA should address the creation and logging of certain types of records. Certain types of widely used electronic communications are not retained by some providers, which can hinder law enforcement investigations. In particular, law enforcement faces challenges with respect to "IP logs," records of which computer or other device is linked to a particular communication. Without a statutory requirement for logging and retention of those records, it is possible to make online threats or victimize children with impunity, secure in the knowledge that law enforcement cannot identify the point where the communications were made. I am well aware that retention means a cost for service providers; it is for precisely that reason that voluntary compliance is not likely to work, and a statutory requirement should be considered. I would urge Congress to find a balance that is not overly burdensome to service providers, but that ensures that law enforcement has access to critical evidence for at least some period of time.

Preservation provisions under current law should be revisited to ensure that law enforcement can prevent service providers from notifying customers of the existence of the request. One provision of the bill the committee is considering would cause prior notification to law enforcement before a provider notifies a customer or subscriber about the existence of a warrant, order, or subpoena, and we believe that provision is important. However, a similar provision relating to preservation orders under 2703(f) should be considered. There are service providers who have stated a policy of notifying customers of any government inquiry unless they are in receipt of process ordering them not to do so. The threat to investigations is clear if these situations are not handled appropriately, and there should be no room for interpretation by service providers in this matter.

Conclusion

Any effort to modify the standard of proof for access to stored content that does not address the concerns outlined above will lengthen law enforcement's investigative timeline, and therefore reduce our effectiveness. A robust debate about balancing personal privacy and security is beneficial to all Americans, but the people and their representatives must be able to make an educated judgment about what they are giving up and what they are getting. There is no question that a growing number of personal details about all Americans move in the digital world, and some of those details make their way into digital crime scenes. Just as there is no question that the people living those lives have an interest in preserving the privacy of that information, there can be no question that some of those devices hold the keys to finding an abducted child, apprehending a dangerous fugitive, or preventing a terrorist attack.

Our society benefits from an open exchange of ideas on topics critical to the public interest, and we believe that the ECPA reform debate remains largely one-sided. Redrafting the laws governing law enforcement access to communications records raises significant implications for law enforcement's ability to protect the public. I urge the members of this committee to ensure that members of the state and local law enforcement community who are in the trenches doing this work every day - and whose jobs will be significantly impacted by any changes in the law - are given the opportunity to continue to share their perspective on the potential human implications of any proposed reform of the Electronic Communications Privacy Act. Competing factors must be balanced appropriately, yet to date the conversation around the issues I have described has been mostly absent. We must be mindful that any restriction of law enforcement's lawful access to electronic evidence, whether by redefining legal barriers, heightening protections for evidence in the digital world compared to the physical world, or allowing service providers to erect new technological barriers, may well come at a price, and some of that price could be paid by our most vulnerable citizens. We should be sure we are willing to require them to pay it. We can enhance citizens' privacy, and we can also ensure criminal investigators get evidence they need quickly and reliably when lawfully authorized to do so.