Before the

Committee on the Judiciary

Subcommittee on Crime, Terrorism, Homeland Security and Investigations

Rayburn House Office Building Room 2141

Washington, D.C. 20515

HEARING ON ECPA PART 1: LAWFUL ACCESS TO STORED CONTENT

March 19th, 2013

Written Testimony
of
Richard Littlehale
Assistant Special Agent in Charge
Technical Services Unit
Tennessee Bureau of Investigation

Chairman Sensenbrenner, Ranking Member Scott, and members of the subcommittee, my name is Richard Littlehale, and 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 the better part of eighteen years in support in cases ranging from searches for violent fugitives to efforts to recover abducted children.

I am grateful to the subcommittee for giving me the opportunity to share a law enforcement electronic surveillance practitioner's perspective on how access to stored communications evidence can be invaluable in the most critical of law enforcement investigations, and how 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 investigations in this country. Our community appreciates your recognition that our expert perspective should be a central consideration of any update to ECPA.

I offer testimony here today both on behalf of my agency, and as a representative of the Association of State Criminal Investigative Agencies (ASCIA), led by President Ron Sloan, the Director of the Colorado Bureau of Investigation. My agency's chief executive, TBI Director Mark Gwyn, is a member of ASCIA's Executive Board and a member of ASCIA's Technology Committee. He and the ASCIA Technology Committee chairman Steve Schierholt, Assistant Superintendent of the Ohio Bureau of Criminal Investigation, have asked me to serve as the ASCIA's subject matter expert on issues such as those before this subcommittee today.

Access to Evidence in the Digital Crime Scene

The crime scene of the 21st century is filled with electronic records and other digital evidence. The contents of this digital crime scene, including electronic communications records, often hold the key to solving the case. They also hold the key to ruling out suspects and exonerating the innocent. Law enforcement's ability to access those records 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, much of the scholarly and media attention given to the question of lawful access to stored content has focused almost entirely on the level of proof required for law enforcement to obtain it, and to a lesser extent on accountability considerations like customer notification and reporting requirements. From the law enforcement perspective, a set of concerns that is critical to our ability to use these records has been largely absent from the ECPA reform debate. If Congress desires to update ECPA, it must do so in a way that addresses these concerns.

The simple truth is that legal 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 even more frequently it is because of logistical hurdles. The companies that retain these records are many times unable or unwilling to respond to law enforcement's lawful demands in a timely manner. 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.

If you or a member of your family were a victim of a crime, and law enforcement needed timely access to electronic communications records to identify and apprehend the offender, would you be satisfied with this reality?

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, these other barriers to access must have a place in the discussion. **I urge Congress to ensure that regardless of the level of process it ultimately decides is appropriate, steps are taken to guarantee that law enforcement will be able to access the required communications transactional records reliably and quickly once that process is obtained.**

As we consider various law enforcement concerns, we must keep in mind a simple fact that is nevertheless 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. The complete lack of a demonstrated

pattern of misuse or abuse by law enforcement to access electronic communications records bears out this truth.

A Law Enforcement Perspective on Lawful Access to Stored Content

Timeliness and quality of service provider response. The timeliness and quality of service provider responses to lawful demands is of primary importance to the law enforcement community. We continue to encourage a thorough review of constructive measures to enhance service provider responsiveness to legitimate law enforcement process requests to ensure that investigative timelines are as short as possible. That is what we owe to the citizens we protect. There is no requirement in current law – including search warrant practice – for providers to respond in a timely fashion to lawful process requests by governmental entities. Some providers routinely respond in a timely way, but others do not. This has resulted in unnecessary investigative delays that adversely impact public safety.

Any contemplated change in the law that would result in a lengthening of the investigative timeline – including moving to a probable cause standard where it is not currently required – should be accompanied by provisions that ensure accountability and prompt response by service providers to legitimate law enforcement requests. These responsiveness issues are important to address even in the absence of an enhanced standard.

Service providers will often cite the high volume of law enforcement requests as a reason for response times that stretch on into months, threatening the underlying investigation. They say they do not have the staff necessary to process the volume of requests more quickly. We would urge the committee to consider that many of these companies are in the business of finding technological solutions to just this sort of problem. Further, they are well acquainted with monitoring customer service centers and determining adequate staffing levels. It is not a matter of capability, but rather a matter of will. Responding to law enforcement legal demands costs service providers money and does not generate revenue, however, and so there is little financial incentive to innovate or increase staffing levels. Therefore, a reasonable legal mandate for responsiveness may be the best solution to this problem. Such a solution need not be overly costly or burdensome to the providers. In a time when Congress is reluctant to impose new regulations on private industry, I would argue that this is one type of regulation that has a clear positive impact for the public. It protects citizens and allows victims of crime to see justice done. It should be addressed in any reform of ECPA, and we look forward to working with the providers and this subcommittee to consider the best way forward.

Notification provisions may put a greater burden on law enforcement than an increased proof requirement. 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 that do not offer any additional constitutional protections, and may actually threaten ongoing investigations. We 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.

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 used by 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.

Google has provided an excellent example of how law enforcement demands truly relate to the new digital reality. Google now regularly publishes statistics on the number of government requests for information that it receives, broken down by the rate that it complies, proof standard, and a number of other factors. Public reporting on these statistical releases has tended to focus on the perception that law enforcement agencies are seeking access to this information at an excessive rate.

I applaud Google for this transparency initiative, but I believe some context is appropriate for the subcommittee's understanding. In June of 2012, Google claimed 425 million individual account holders for its Gmail product alone. In 2012, it reported receiving over 40,000 government requests for communications records worldwide, affecting about 68,000 users or accounts globally. In the U.S., Google reported a total of just over 16,000 government requests affecting just over 31,000 accounts. That means just a tiny fraction of one percent of Google's accounts were affected by government demands.

Consider that in the context of more than 17,000 law enforcement agencies in the United States. This means that on average, there was less than one request for information per law enforcement agency per year for Google

records. Contrast that with crime reporting statistics, which reflect that in 2011, more that 14,000 Americans were murdered, more than 83,000 were forcibly raped, and there were over 350,000 robberies. It is hard to conclude from these numbers that law enforcement demands for records are excessive.

My fellow professionals and I deal with cases like that every day, and stored communications are a critical part of the constellation of evidence that allows us to identify the guilty and keep the public safe. 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 lead to identification of sexual predators, the recovery of kidnapping victims, or the successful prosecution of a murderer. 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 with their 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.

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.

Records retention is an issue that should be considered in any effort to update ECPA. Certain types of widely used electronic communications are not retained by some providers, which can hinder law enforcement investigations. In particular, most cellular service providers do not retain stored

text messages accessible to law enforcement for any time at all. Billions of texts are sent every day, and some surely contain key evidence about criminal activity. In some cases, this means that critical evidence is lost. Text messaging often plays a big role in investigations related to domestic violence, stalking, menacing, drug trafficking, and weapons trafficking. I am well aware that retention means a cost for service providers. I would urge Congress to find a balance that is not overly burdensome to service providers, but that ensures that law enforcement can obtain access to critical evidence with appropriate legal process for at least some period of time.

Preservation provisions under current law should be revisited to ensure that law enforcement could prevent service providers from notifying customers of the existence of the request. Some proposals for ECPA reform 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 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 principle behind their stance is laudable, but the real-world impact can be harmful to criminal investigations. Section 2705 offers a delay of notification scheme for court orders and subpoenas, but does not address preservation letters directly. If there is reason to believe that customer notification of the existence of a warrant, subpoena, or court order may result in:

1) endangering the life or physical security of an individual;
2) flight from prosecution;
3) destruction of or tampering with evidence;
4) intimidation of potential witnesses; or
5) otherwise seriously jeopardizes and investigation or unduly delays a trial,

then it seems that the ability to prevent early notification of the existence of a preservation letter issued in the early stages of an investigation with the intent to assemble a quantum of proof – such as probable cause – would be essential.

The definition of content must be clear and carefully considered. Definitions of “content” and “non-content” information need to be clear and comprehensive. Efforts to update ECPA should constrain the definition of content so that it does not expand over time to cover parts of an electronic communication that are ancillary to the actual purport, idea or intent of the writing, such as signaling, addressing, routing or URL information.

Any move to alter the standard of proof required to access stored content should be carefully considered in the broader context of the concerns identified above. If governing law is changed to require probable

cause for any type of location information, there will be a negative impact on the time required for law enforcement to conduct certain types of investigations. Some of this impact can be balanced by changes in the law with respect to records retention and quality of service in response to law enforcement legal demands. 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 and negatively impact our ability to bring criminals to justice.

Conclusion

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 are moving around the digital world, and some of those details make their way into digital crime scenes. Just as there is no question that people have an interest in preserving the privacy of that information, there can be no question that some of that information holds the keys to finding an abducted child, apprehending a dangerous fugitive, or preventing a terrorist attack. Whenever we move forward with the privacy/safety debate, we should be mindful that any restriction of law enforcement's access to that information, whether by redefining legal barriers 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.

The thousands of law enforcement officers across this country who utilize communications evidence in the course of their duties recognize that we are guardians of a free society, a society that embraces in its founding law the decision to elevate the rights of the individual above incremental increases in public safety. The truth is that no one has put forward any evidence of pervasive law enforcement abuse of ECPA provisions. Law enforcement professionals also recognize that times are changing, and as a profession we are moving forward to utilize all available evidence in a responsible and effective way.

Ours is also a society that requires an open exchange of ideas on topics critical to the public interest, however, and we believe that the ECPA reform debate has been largely one-sided to date. As I hope to have shown, 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 subcommittee to ensure that the law enforcement community is given the opportunity to continue to share its perspective on the

potential human implications of any proposed reform of the Electronic Communications Privacy Act, so that all the competing factors may be balanced appropriately.

I have always been proud of the Tennessee Bureau of Investigation motto, borrowed from the United States Supreme Court in Berger v. United States. It seems particularly appropriate in this context. The evidence in the digital crime scene, now more than ever, will help law enforcement to ensure "that guilt shall not escape, nor innocence suffer."

Thank you for the invitation to testify and I look forward to working with you on these important issues.