Questions for the Record
United States Senate Committee on the Judiciary
Hearing on
"Reforming the Electronic Communications Privacy Act"

September 16, 2015

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

Questions of Chairman Chuck Grassley

Special Agent Littlehale, in your testimony you described the many different ways in which the current ECPA regime poses problems for state and local law enforcement. Do you have any additional, real-life examples that illustrate these problems?

Response: Let me offer two additional examples of real-world problems faced by investigators working today's digital crime scene. I have picked two that illustrate some of the issues discussed in other questions for the record set forth below. It is worthy of note, given much of the discussion in the hearing, that in both of these cases, law enforcement obtained a search warrant, and in both cases, they were frustrated by delayed and obstructionist responses from the service providers.

Case #1: The first example illustrates the problems that law enforcement has with service providers pre-litigating the warrant, and with delayed response:

> In December 2014, the police department in a large city obtained a search warrant for stored messages from a deceased victim's account with a smartphone application provider during a capital murder investigation. The warrant called for a response within 15 days of receipt. No response was immediately forthcoming, and after a second service of the search warrant, six months after service, the investigators received a response that stated in pertinent part:
>
> *"[service provider] has additional responsive data that we can produce in a supplemental production; this data includes the contents of messages that were on [service provider's] servers as of January 19, 2015 (the messages that are on [service provider's] servers are limited to the messages that were not successfully delivered to the intended recipient – in this case, the target facility identified in the Search Warrant). Some of this data is responsive to this warrant (data between November 22, 2014*

through December 26, 2014) but [service provider] is unable to date-limit this message content and accordingly are requesting a new or amended warrant that includes language reflecting the use of a "taint team", a group of law enforcement's technical experts who will review the messages and seal any content that exceeds the scope of the Warrant.

An example of this language is:
Law enforcement personnel will review the information stored in the accounts and files received from [service provider] employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant as specified. Law enforcement personnel will then seal the original duplicate of the accounts and files received from [service provider] employees and will not further review the original duplicate absent an order of the Court.

The law enforcement agency refused to seek a fresh warrant and asked the prosecutor to intervene by threatening legal action. Only at that point did law enforcement receive the proceeds the original warrant sought.

Here, after a delay of <u>six months</u>, the service provider acknowledges that they have additional evidence that is responsive to the warrant, but refuses to provide it unless law enforcement obtains a new warrant setting forth a complicated review procedure identified by the service provider, all so that the service provider doesn't have to take the time to separate evidence from non-responsive data themselves. The decision of whether or not to employ a taint team rests properly with law enforcement in consultation with the prosecution, not with a company that holds evidence. If law enforcement should have employed a taint team and did not, the defense will have ample opportunity to raise the issue if criminal charges are brought. This type of pre-litigation of warrants is precisely the sort of burden that lengthens investigative timelines and complicates the job of investigators unnecessarily.

Case #2: This is another example of non-compliance, pre-litigation of the warrant, combative responses, and in this case, an absurd demand that law enforcement supply precisely the information that law enforcement was seeking in order to narrow their request:

A law enforcement agency investigating a murder that occurred in December 2014 identified a pre-paid smartphone in May 2015 as being relevant to the case. Investigators needed to identify an unknown person who was associated with a telephone number that was associated with the phone. A judge issued a search warrant calling for the smartphone manufacturer/cloud service provider to provide subscriber information for a specific telephone number for a single month.

The service provider responded that the telephone number was associated with multiple customer accounts, and requested the relevant "account email address, or full name and telephone number, and/or full name and physical address of the

subject [account]." The investigators responded that they could not provide the requested information because that was precisely the information that they were seeking in order to identify their unknown user, and asked the provider to comply with the original warrant, stating:

"*If there is more than one subscriber, then provide information for all subscribers associated with phone number xxx-xxx-xxxx, from December 1, 2014, through December 31, 2014. This is not an unreasonable request and we expect [service provider] to comply with the search warrant – as is."*

The service provider responded:

We have reexamined this matter. However, we have not been in a position to provide you with account information due to the fact that there is not enough account identifying information provided in your warrant. In this regard we are not in the position to identify any account based solely on the telephone number due to the potential number of accounts pertaining. We need an individual's full name, physical address and/or email address in addition to the telephone number in order to identify any account which may be associated with the individual in question. Further, your warrant does not provide us with any information which will assist in identifying any account which may be associated with this individual. If you would be kind of to provide us with either a name, email address and/or physical address for the individual who is the subject of this warrant. We will conduct searches to establish if there is an account associated with these details, and if so provide the results to you. We trust this clarifies the position for you at this time and we look forward to receiving the further identifying details from you should you be kind enough to provide them.

Here, the service provider admits to having responsive information…in other words, the compliance personnel can see multiple accounts associated with the telephone number in question. Despite being in possession of this evidence, the provider has decided that it will not provide the range of subscribers that have used the number in question, because law enforcement's request is not specific enough to identify a particular subscriber. The provider renews their insistence that law enforcement provide precisely the information that law enforcement does not have in order to receive the evidence called for in the warrant.

Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses, and/or anything else you did not have a chance to respond to that was discussed at the hearing.

Response: One term that I heard repeated in the hearing was a familiar assertion of those who insist that law enforcement has all the access to evidence we need: that we

live in the "golden age of surveillance," when law enforcement has access to an endless buffet of data. I certainly agree that a steadily increasing amount of evidence relevant to any criminal investigation exists in the digital world, and that digital evidence can be of enormous value to investigations. It is also true, however, that we now have access to less and less of that evidence; we are allowed to look at the buffet, but even with a search warrant in hand, all too often, we go hungry.

Imagine a person who wishes to communicate with another person without the government having access, and wants to exchange pictures and other materials and keep those private as well. Fifty years ago, those communications would be subject to interception on any available means of communication available to the public, and any enciphering of the information would have had to be manual and subject to decryption by experts. A cache of pictures could be buried in the woods, locked up in a bank, or hidden behind a false wall, but would be subject to discovery by a diligent enough search. Now, that person can put all of those communications and materials on a mobile device that fits in a pocket, and if the person chooses the device carefully, they can give the device to the police for a week with the expectation that their secrets – or the evidence of their criminal conduct – cannot be accessed.

That sounds more like the Golden Age of Privacy to me. If we continue to allow technological advancement without any consideration of the importance of collecting digital evidence in criminal investigations, it will place law enforcement at an unprecedented disadvantage in gathering the evidence we need to do the job the public expects us to do.

Questions of Senator Mike Lee

1. **Mr. Littlehale, when you testified before the House Judiciary Committee in 2013 about the emergency issue, you said that some "providers make a decision never to provide records in the absence of legal process, no matter the circumstances." But Google, Facebook, Microsoft, and Yahoo! have all put out transparency reports that show that they do respond to emergency requests and provide responsive data the majority of the time.**
   - **Do you acknowledge that the largest service providers usually do voluntarily disclose content in response to an emergency request?**

Response: It has been my experience, and the experience of the state and local investigators with whom I am acquainted, that larger service providers will sometimes respond to emergency requests under the existing provision in ECPA. How often and how quickly they respond varies widely from case to case and provider to provider (and even from call-taker to call-taker). It is fair to say that in my experience, most large providers will usually provide records on an emergency basis for a child exploitation investigation, for example, or in response to a child abduction. The same is not

necessarily true for other situations which those of us in law enforcement would consider life-threatening emergencies.

I wouldn't use the word "usually" across the range of cases and providers, therefore, and even when the providers do provide an "emergency" response, what that means in terms of investigative latency also varies. Turnaround times of an hour or two for basic information on an emergency basis are normal for some large and small providers, but emergency responses in the four to eight-hour range are distressingly frequent, and even longer delays occur regularly with providers who do not adequately staff their compliance office.

Better data about the number of requests and the timeliness of service provider response in emergencies would be a welcome addition to this conversation; at present, law enforcement does not have a central mechanism to collect that data, and generally concentrates on the emergency itself rather than on data collection.

Most providers have a policy that is more restrictive than the statute; that is, they state a willingness to provide records in an emergency in a set of cases smaller than the range authorized by 18 United States Code Sec. 2072(b)(8), which permits voluntary disclosure "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." Some will provide emergency response in cases involving a danger to children, for example, or will only provide emergency access to non-content records.

It is worthy of note that the service providers who publish transparency reports often claim a certain number of emergency requests that they have rejected. It does not necessarily follow that those emergency requests were objectively flawed, but rather that the service provider chose not to respond to them. Without an independent examination of the facts, it is irresponsible to suggest that all of those cases were not true emergencies.

Service providers routinely require law enforcement to include language in legal process and other measures beyond what the Constitution and laws require. For example, when one Circuit issues a particular ruling raising the bar for access to a particular category of records, some service providers routinely extend that ruling to law enforcement in other parts of the country not bound by the decision.

- **Can you identify the service providers that have a policy of categorically rejecting emergency requests in the absence of compulsory legal process? If not, why not?**

Response: I have generally avoided naming specific service providers in my testimony because I do not want to publicly highlight forms of communication that are

particularly problematic for law enforcement, whether by virtue of policy, practice, or technology. It may be that the time will come when that practice is no longer practical in this area, as has become the case with developers of certain forms of encryption.

All of that said, I am personally aware of law enforcement officers who have attempted to obtain records on an emergency basis and been told by service providers that they agree that an emergency exists, but that the provider will not provide records in the absence of process. Some of those providers are among the "larger" companies in the market.

An example from a large provider's compliance manual might be helpful. The following quote was included with an example provided by a colleague; the compliance manual in effect at the time of the example stated "If we receive information that provides us with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, **we may provide** information necessary to prevent that harm, if we have it." Isn't the implication of "we may provide" that in some instances, when there is "an exigent emergency involving the danger of death or serious physical injury to a person," they might not provide it on an exigent basis? There is the justification for a mandatory disclosure provision in a nutshell.

2. **In your written testimony, you discuss the need for law enforcement to have immediate access to evidence when the officer determines that an emergency exists.**
   - **What limits would be placed on such an emergency exception? Would it be entirely up to the discretion of the officer making the request?**

Response: The statute should contain a statutory definition of emergency that an officer must identify as having been satisfied in a declaration to the service provider. This definition should be broad enough for an officer to require accelerated response when the circumstances lead that officer, in his or her informed professional opinion, to believe that a person is in danger. Once the guidelines were established, it would be up to the officer to require an expedited response through a declaration.

The definition must be clearer than it is now, and the officer is in the best position to evaluate the facts and whether or not they qualify. What about the case of someone missing under suspicious circumstances, for example? What about a murderer on the run…how many people does someone have to kill before they are judged an unreasonable danger to the public? How specific does law enforcement's evidence of a specific intent to harm others, rather than simply an intent to flee capture, have to be? Right now, those questions are entirely in the hands of call-takers without any public safety experience.

Any effort to reform this provision in ECPA should retain voluntary disclosure as an option for officers who are less familiar with this type of interaction with service providers, and who are willing to allow the service provider to retain responsibility for declaration of an emergency disclosure as a result.

- **Wouldn't this create powerful incentives for law enforcement to compel the disclosure of content in situations where a statutory emergency (i.e. risk of serious bodily harm or death) doesn't truly exist?**

Response: The incentive is only powerful if one is predisposed to think that law enforcement routinely circumvents limitations placed on their authority. Yes, law enforcement is often frustrated by the lack of timely responses by service providers in routine cases, and yes, when those delays prevent access to evidence, there are often have very real impacts on investigations and public safety. To the extent that there are missteps in this area, they are generally based on a misunderstanding of what constitutes an emergency, not on a deliberate attempt to avoid seeking legal process.

- **Do you think a suppression remedy would be appropriate to ensure content obtained in a falsely claimed emergency isn't used in a later investigation or prosecution?**

Response: No, a statutory suppression remedy would cause over-deterrence. Existing administrative sanctions are sufficient to deter unsupported exigent requests. One might also ask why the sanction would be exclusively on the law enforcement side. Shouldn't Congress create a civil cause of action against a service provider if their delay or negligence in responding to an emergency demand causes harm to someone? Or are the existing remedies that the common law provides sufficient to deter willful or negligent noncompliance by service providers?

3. **You have suggested that Congress ought to statutorily mandate time limits for service providers to respond to legal process, but judges routinely prescribe deadlines for compliance.**
   - **Are state judges ill-equipped to be serving this function? Do service providers routinely ignore judge-imposed deadlines?**

Response: Judges routinely impose deadlines in areas where they are given the discretion to do so by rule or statute, such as in discovery. The rules for most state judges in this area are less clear. In some instances, state statutes provide some guidance, and in others the judges are willing to place a deadline in a search warrant or other order.

In my experience, and the experience of my colleagues, yes, service providers large and small routinely disregard judge-imposed deadlines placed on routine legal demands unless they are being actively litigated. Such disregard, and the reasons it often goes unanswered, can be largely explained by the fact that state prosecutors and judges are already generally overburdened by their caseload. The only remedy for this problem is to set aside time for a show cause hearing, and that requires the judge and the

prosecutor to litigate an issue which is often moot by the time a hearing could be held, either because the provider has finally responded to the process, or because the investigation has progressed in a different direction.

Please do not mistake this for evidence in support of the conclusory and unsupported "law enforcement will always find another way" argument. In fact, even if law enforcement does find another way to work the case, it often imposes delays, takes additional resources, and impacts the overall quality of the prosecution. "Well, you were able to scratch and claw your way most of the way there, even though you didn't have access to the digital evidence," isn't a reasonable burden to place on law enforcement.

The difficulty in finding the time to pursue show cause orders – and the reason why they are not sought more often – is effectively illustrated by some simple figures from a large American urban court system: in one urban county, as of October 2015, there are 18,535 pending felony cases across 22 felony courts. These courts average 843 pending cases at a time, and each court has 3 prosecutors assigned. It shouldn't be a surprise that cancelling court to hold a show cause hearing is not the most attractive option to secure service provider compliance for those judges and prosecutors.

Questions of Senator Amy Klobuchar

The Justice Department, and in particular the Federal Bureau of Investigations (FBI), often works in concert with local law enforcement.

- **How can we enhance cooperation between law enforcement at the federal level?**

Response. There are already a number of mechanisms in place for information-sharing among law enforcement agencies at all levels of government. In the area of digital evidence collection from service providers through ECPA, state and local law enforcement's most pressing needs are for technical and legal assistance in securing the evidence that we need for our cases. We depend on the FBI, the Department of Justice, and other federal partners to provide us with advanced technical assistance and the support of compliance infrastructure through the federal system in cases where our local courts and mechanisms

A particularly important part of this support system that deals with digital evidence is the National Domestic Communications Assistance Center. Congressional support for the NDCAC's mission of facilitating federal, state, and local access to electronic evidence. In addition, supporting programs to ensure that federal agencies have the funding and mandate to assist state and local law enforcement, and to ensure that federal law enforcement shares any and all technological solutions available to ensure state and local access to electronic evidence, will also foster interagency cooperation.

- **Are there notable differences in the collection of electronic information through ECPA at the federal level compared to the local level? If so, what can be done to ensure uniform processes for all law enforcement agencies?**

Response. Generally speaking, the legal demands used are similar, and the interaction with service providers is similar. One area of difference is the fact that the federal government has already implemented electronic systems for exchange of routine process, greatly improving response time. Any efforts to increase the availability of these systems to state and local law enforcement, and/or to develop them further to accommodate the wide range of requests and legal demands, would be a huge service to the state and local law enforcement community.