Before the

Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights and Civil Liberties

Rayburn House Office Building

Washington, D.C. 20515

HEARING ON ECPA REFORM AND THE REVOLUTION IN LOCATION BASED TECHNOLOGIES AND SERVICES

June 24, 2010

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

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, 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 across Tennessee use communications records in support of their criminal investigations. I have personally used these techniques for the better part of fifteen years in support of everything from fugitive investigations to efforts to recover abducted children.

I am grateful to the Subcommittee for giving me the opportunity to share my perspective on how location information derived from communications technologies can be invaluable in the most critical of law enforcement investigations. I offer testimony here today on my own behalf, based on my own experiences.

Utility of Location Evidence

The value of evidence of a person's location at a particular moment in time cannot be overstated. A criminal investigator can use the information to find a kidnapped child, apprehend a dangerous fugitive before they can harm the public, or prevent a terrorist from following through on a violent plan. Technology-based evidence is particularly valuable to law enforcement because the evidence is drawn from reliable, unbiased sources that maintain the evidence for some period of time – typically as business records in the ordinary course of the services they offer.

The various records created when a mobile device like a cellular phone interacts with its network have become a tremendous resource for law enforcement. Particularly when used in concert with traditional investigative techniques, cell phone location information frequently permits law enforcement an opportunity to find and rescue a victim or apprehend an offender in a matter of hours -- whereas other methods may consume many days and may not prove fruitful at all. Take the case of a carjacking-kidnapping victim who has a cellular telephone with her, but is unable to use it to call 911 as her assailant speeds away with her held hostage. A witness to the crime reported the license number to the police, and they used that information to identify the victim. A call to a friend or relative reveals the cell phone number. Interaction with the cellular service provider will allow law enforcement to determine a cell site that the phone recently hit, sending patrol cars to the area to look for the car. Without that evidence, the police department would have only the witness's location as a reference point for a search.

Cell site information is certainly one of the most useful location-based forms of evidence available to law enforcement, but it is by no means the only one. Increasingly,

law enforcement is required to develop location information from other methods of communication. Suppose, for example, that a pedophile is grooming a child in an internet chat room in an effort to get that child to travel to meet with him so that he can victimize the child. Suppose further that the pedophile uses a computer that is part of a particular network to access the chat room in question. A series of subpoenas to service providers will allow law enforcement to identify the subject's "virtual" location on the network (in the form of an IP address) so that the pedophile can be identified and located (by resolving the date and time of the IP assignment to a particular subscriber account and service address) – resulting in the child being spared from unspeakable harm.

Legal Requirements to Obtain Communications Records

At this point, it is useful to separate the issues of updating language to deal with new technologies and fundamentally altering the level of proof needed by law enforcement to access information. Generally speaking, the law enforcement community believes that the balance currently struck by ECPA and related statutes and case law is an appropriate balance. Any change to that balance should be broadly discussed and carefully considered, as it will have substantial and far-reaching secondary consequences. Having said that, there is certainly room to discuss the matter, and as communications technology evolves, so too must the laws that govern it.

Why the current legal framework makes sense

At present, law enforcement generally distinguishes between network *transactional* location records (ordinary records of communications captured, stored and recorded by the service provider in the ordinary course of its business as a necessary incident to providing the services they provide) and *demand*-based location information (manufactured information generated solely based on a law enforcement demand pursuant to lawful emergency or court authorization). Because the latter is not a record that already exists, it is commonly believed to require a higher standard of proof because it is more invasive.

Cell site location records are routinely generated in the normal course of a cellular provider's business. They indicate nothing more that which piece of the telephone company's equipment (the particular cell tower and sector) that a particular customer's cellular handset was communicating with on a particular call event began or concluded. Those records would be created whether or not law enforcement would later attempt to obtain them or to receive them contemporaneous with their creation; and they would be kept for a certain period of time and then discarded or archived.

Contrast this with a demand-based location request. In that instance, at law enforcement's direction and based on lawful emergency or court authorization, the

service provider causes a more precise location record to be generated – one that would not otherwise exist at all. That record would not have been created "but for" the law enforcement demand; as a result, it is reasonable and prudent to suggest that a higher level of proof be met for that information to be turned over.

This framework is reasonable because it is consistent with other ways location information can be obtained and used by law enforcement and because it is consistent with the view that information voluntarily turned over to a third party enjoys less privacy than those things we keep from the outside world. It is worth considering that a person's location at a particular time can be derived from any number of sources other than mobile devices, sometimes in very precise ways. A bank will have records of a customer's use of a credit or ATM card in their possession that would show exactly when and where that particular card was used. A transportation authority might have records of when a commuter passed by particular tollbooths based on the information provided by their electronic commuter pass. Those records can currently be obtained with a subpoena in most cases – and when they relate to communications records, Congress has already acted to afford them greater protections under ECPA's existing framework. Should that standard change? If not, how can the inconsistency be explained, if the purpose of reform is to bring clarity and consistency to the law?

Why not always require probable cause?

If governing law is changed to require probable cause for any type of location information, there will be a reduction in the effectiveness of this technique for law enforcement. First, location information can be used to good effect in many instances where law enforcement may not have generated probable cause sufficient to satisfy the warrant requirement. Further, the time required to generate a search warrant and have it signed, even in cases where probable cause exists, may in-and-of itself hamper law enforcement's efforts to move quickly in an investigation.

I fully acknowledge that the above argument could also be used in favor of relaxing the search warrant requirement completely in order to make law enforcement "more efficient" in *all* investigations. Of course, such a thing would be foreign to our bedrock legal principles. In this case, however, the present balance of judicial supervision and law enforcement efficiency has existed for some time, and should not be abandoned without a demonstrated need for an increase in privacy and a demonstrated pattern of abuse – presently nonexistent -- by government officials. Time is always a factor in investigations; and the more important the investigation, the more important time can become.

Take as an example a recent case that my unit worked in Tennessee. Local, state, and federal law enforcement agencies were engaged in a massive (and, thankfully, successful) search for a 4-day-old infant abducted after a stranger stabbed his mother and left her for dead. During a five-day period, my unit obtained communications

records through 15 pen register orders, 9 search warrants, and 377 administrative subpoenas and Sec. 2703 "specific and articulable facts" orders. When you are talking about that volume of process, any change in the type of process required will have an impact on how rapidly law enforcement can process leads and resolve the case, and in a case of this type, every minute counts.

This is not to say that law enforcement cannot continue if the standard for location information is elevated to probable cause. It will, however, mean some decrease in the number of leads we can pursue; and in some cases, it will inevitably prevent us from obtaining records that will be helpful and will result in some measurable – albeit unknowable – harm to the public. If the privacy trade-off is worth it in the eyes of lawmakers, then law enforcement will adapt. What is critical is that everyone involved takes steps to understand the full downstream consequences of what may appear to be minor changes to governing law, so that they may be considered in the proper context.

In addition, adopting a probable cause standard for cell site location information may not fully answer the question. Suppose for a moment that Congress adopts a probable cause standard for cell site location information. How that standard was drafted would raise a new set of issues outside of the cellular network. Suppose a customer with a "smart-phone" accesses the wireless access point of a coffee shop with the phone's Wi-Fi capability, and that generates an internet protocol address that can be localized to that particular shop at a particular time. That is location information far more accurate than a cell sector, but at no time is that information traveling over the phone company's network. Instead, the information could be obtained from the coffee shop's internet service provider. Would that require a search warrant? If so, generating a search warrant for each and every lead passed on to law enforcement of an individual who may be attempting to victimize a child over the internet will have a significant slowing effect on the processing of child exploitation leads. If that is acceptable, so be it, but it is a downstream affect that must be considered.

The Technology Gap

I would be remiss in any discussion of the utility of technology-based evidence if I did not point out 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.

The gap between what law enforcement is legally entitled to access under current law and what is actually available is already wide -- and it is growing wider all the time. Encryption, smart-phone countermeasure applications and a dizzying variety

of communications streams are walling off more of the evidence we need at a steadily increasing rate. If the law enforcement community does not successfully bridge this gap with legal reform, training, solutions development, and funding, then our ability to protect the public using this information will degrade at the same breakneck pace.

As Congress moves forward with discussions of how it might simplify the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to get the records it wants, the technology gap has a place in the discussion. I would urge that Congress ensure that whatever level of process it decides is appropriate, that steps are taken to guarantee that law enforcement will be able to access the required communications technologies once that process is obtained.

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…location, communication, the sundry details of lives lived in the modern world…lie in storage and move in transit across a vast landscape of devices. 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. 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 private corporations 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.

As an American law enforcement officer, I know that I am a guardian 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. Ours is also a society that requires an open exchange of ideas on topics critical to the public interest, and today's topic is such an issue. 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 committee 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.