Written Statement of Marc J. Zwillinger

Partner

Zwillinger Genetski LLP

before the

U.S. House of Representatives Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

Hearing on

ECPA Reform and the Revolution in Location Based Technologies and Services

June 24, 2010

Chairman Nadler, Ranking Member Sensenbrenner and Members of the Subcommittee, thank you for the opportunity to testify about ECPA reform, and specifically about issues relating to historical and real-time location data. By way of background, I served as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last ten years I have been representing companies, including internet service providers, social networking companies, and wireless providers on issues related to electronic surveillance and the Electronic Communications Privacy Act. As part of that work, I have litigated surveillance-related issues in district and appellate courts across the United States. I also teach a course in cybercrime law as an adjunct professor at the Georgetown University Law Center in Washington, D.C. I have also been involved in the Digital Due Process Coalition for the last 2 years. I am testifying today solely in my individual capacity and not on behalf of any clients or the Digital Due Process Coalition.

Let me begin by saying that as someone who spends nearly every day dealing with complicated issues arising under ECPA, I believe that ECPA is in need of reform, especially to bring the privacy protections for both transactional and stored communications into the modern age of cloud computing, social networks and mobile devices. And while today's discussion of location-based data is important, the uncertainty of ECPA's application to content stored in the cloud and its flat prohibition on access to contents in civil matters and for criminal defendants provides even more justification for amending ECPA. In many ways, ECPA has done remarkably well in striking the right balance between law enforcement needs and users' privacy interests for the past 25 years. Unfortunately, there are several specific areas where ECPA's balance no longer works effectively. This has happened for the very reason that the Supreme Court recently noted in *Quon*, "rapid changes in the dynamics of communication and information transmission are evident, not just in the technology itself but in what society accepts as proper behavior." *City of Ontario, California, et al. v. Quon*, Dkt. No. 08-1332, slip. op at 11 (June 17, 2010).

Before examining how the statutory regime applies to location-based data, it is important to define the types of location-based information that are driving the concern about ECPA reform. Law enforcement certainly may obtain a broad array of information that provides knowledge about a person's location at a given moment in time. For example, law enforcement can use a record of a landline phone call, an in-person credit card transaction, or use of a rechargeable fare card for public transportation to pinpoint a person's location at a particular time. Traditionally, law enforcement has obtained these records for use in criminal investigations without causing significant privacy concerns. Presumably, this is for two reasons: (1) it was clear to the person engaging in such transactions that his or her interaction at that point in time was being recorded; (2) the transactions provide information about an individual's location at a specific moment in time, but do not provide a stream of continuous location data that could be used to track his or her specific whereabouts.

Consequently, the types of data that do raise serious privacy concerns under existing law are those that have the opposite characteristics: (1) information that may be collected without the subject's knowledge, like cell-site data that is collected even when a call is not in progress; and (2) data that provides the ability to track all of a person's movements on a relatively precise and continuous basis. This information tends to appear most often in electronic form and is maintained and collected by providers covered by ECPA. With regard to this type of location data, ECPA's statutory framework is profoundly unsatisfying. It creates a different set of rules for historical and prospective location data, and it fails to provide clear guidance for situations in which the government seeks to track an individual's precise movements, leaving the answer to the general application of Fourth Amendment principles and significant variation across jurisdictions.

To explain why legislation is appropriate, I will first examine how the DOJ currently obtains historical location data including Cell Site Location Information, also known as CSLI. Next, I will discuss how DOJ seeks to obtain prospective location data. Finally, I will conclude by pointing out the flaws in DOJ's approach and the benefits of legislative reform.

Historical Location Data:

Most of the established precedent on location-based data relates to law enforcement requests for historical CSLI. There should be no real question that the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et. seq*. currently governs the government's authority to obtain this type of data. The SCA describes the circumstances in which an electronic communications provider can disclose records or other information pertaining to a subscriber or customer (with the exception of the contents of the subscriber's communications). As the SCA makes clear, every piece of information maintained by an electronic communications service provider must fit into one of the four categories of data described by the statute: (1) contents of communications in electronic storage; (2) contents of wire or electronic communications in a remote computing service; (3) records or other information pertaining to a subscriber or customer; or (4) basic subscriber information of the type described in 18 USC § 2703(c)(2). Of those categories, nearly every bit of non-content transactional information a provider maintains falls into the 3rd category – "records or other information pertaining to a subscriber or customer," all of which is obtainable though an order issued pursuant to 18 U.S.C. § 2703(d).

For historical location data to be available to the government under the provisions of 18 U.S.C. §2703(d) only three things have to be true: (1) the provider has to be a "provider of electronic communication service"; (2) the data has to be "a record or other information pertaining to a subscriber or customer of" an electronic communications service; and (3) the data may not be "content" information, which is defined by the SCA as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). For the most part, location data that accompanies a call does not provide information related to the substance of the communication, rather it is ancillary data conveyed so that the wireless telephone can connect with the nearest cell tower. It is not the content of the communication.

This may not continue to be the case, however, with regard to new location-based Internet services, which, unlike cell site location data, are designed to track location data, either because the user voluntarily enters their location in text-based fields (like on Facebook) or specifically authorizes the transmission of GPS information so that the user can get directions through Google Maps or connect with friends (as on Foursquare). In these instances, there is certainly an argument that the uploaded and/or transmitted location data is in fact the "content" of the communication because it is not information necessary for the connection of some other communication, but is rather information the user intentionally transmits to a third party (directly or through an application) because communicating the location information itself is the purpose of the transmission.

This is why thinking about location data only in the context of cell tower data is misleading and should not be the paradigm through which Congress views ECPA reform. But in the specific context of information collected by wireless service providers as an integral step in providing wireless service, the information should be obtainable through the use of an Order under 18 U.S.C. § 2703(d), which requires the government to proffer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

Real-Time Location Data:

The current process through which the government may obtain real-time or prospective location data, whether for cell sites, or otherwise, is more complicated and uncertain, especially because it implicates statutes beyond ECPA. The starting point for understanding this process is the language of the pen register/trap and trace ("PRTT") statutes,[1] which, on their face, allow the government to obtain an order to get access to "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," and/or "dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. §§ 3127(3) and (4). If this were the only relevant authority, the analysis for cell site location data would likely end here, because the location data transmitted by a cell phone at the outset or receipt of a call has been held to fall within this definition. Again, if we consider location-based data provided by other devices, such as GPS or navigation devices whose main purpose is to transmit location data, it is not at all clear that the PRTT statutes would continue to apply.

Where they do apply, however, the showing applicants must make in order to obtain a PRTT order is less than the showing they must make under the 2703(d) standard for historical location data, at least with regard to devices that send or receive electronic communications. Under the PRTT statutes, to obtain a pen/trap order, applicants must only identify themselves and the law enforcement agency conducting the investigation and certify their belief that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. *See* 18 U.S.C. § 3122(b)(1)-(2). So long as the application contains

[1] 18 U.S.C. § 3121, *et seq.*

these elements and the issuing court has jurisdiction over the offense being investigated the court is required under the statute to authorize the installation and use of a pen/trap device anywhere in the United States. *See* 18 U.S.C. § 3122(a); 18 U.S.C. § 3127(2)(A).

Under the SCA and PRTT, it appears that prospective location data (at least with regard to devices that send or receive electronic communications) receives less protection than historical location data. However, the analysis extends beyond the scope of these statutes. When Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") in 1994, it included a provision now codified at 47 U.S.C § 1002(a)(2), which states that "[w]ith regard to information acquired solely pursuant to the authority of pen registers and trap and trace devices, such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." Absent this prohibition, it is likely that the pen register and trap and trace statutes alone would be sufficient to authorize the collection of location data. Therefore, it is CALEA, and not ECPA, that precludes the collection of location data from cell phones under the standard for Pen Registers and Trap and Trace devices. It does not necessarily preclude their use for location information derived from other types of devices that are not subject to CALEA.

Given CALEA's language, the government has struggled to come up with an alternative theory for obtaining location data on a prospective basis without first obtaining a warrant under Rule 41 of the Federal Rules of Criminal Procedure. Given the state of Fourth Amendment jurisprudence, this is an understandable impulse because current Fourth Amendment case law suggests that a prior warrant may not be necessary to track an individual's location in purely public spaces.[2] The government's preferred method is to combine the authority of a pen register and trap and trace with the authority previously described under 18 U.S.C. 2703(d) for obtaining historical location data. The government's theory is essentially that by combining the authority to obtain prospective data under the PRTT statutes with the greater judicial showing necessary for historical data under the § 2703(d) standard, the government avoids the CALEA prohibition against "solely" relying on the authority of the PRTT statutes. This theory has been rejected by many courts, but accepted by some, as an acceptable method for obtaining prospective location data. [3]

---

[2] Thus, law enforcement has not been required to obtain a search warrant before affixing a GPS tracking device to the outside of an automobile that is parked on a public street. *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (placement of tracking device on exterior of vehicle while parked in defendant's driveway, while on public streets and while in a parking lot did not violate Fourth Amendment); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007) (installation of a battery-power GPS device on the exterior of a vehicle does not implicate Fourth Amendment rights); *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999) (installation of a magnetic GPS device and magnetic beeper on the outside of a vehicle does not constitute a search under the Fourth Amendment).

[3] *See e.g. In re Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Information*, 2005 WL 3658531 (D.D.C. Oct 26, 2005); *In re Application of the United States for Orders Authorizing Installation and Use of Pen Registers and Call Identification Devices*, 416 F. Supp.2d 390 (D. Md. 2006); *cf*. *In re Application of the U.S. for an Order for Disclosure of Telecommunications Records*

This theory has also been embraced by the Department of Justice in the 2009 Version of the Manual for Searching and Seizing Computers and Obtaining Electronic Evidence, published by the DOJ's Computer Crime and Intellectual Property Section. The manual states:

> The rationale behind this "hybrid" use of the Pen/Trap statute and § 2703(d) is as follows. Cell-site data is "dialing, routing, addressing, or signaling information," and therefore 18 U.S.C. § 3121(a) requires the government to obtain a pen/trap order to acquire this information. However, the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") precludes the government from relying "solely" on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone subscriber. 47 U.S.C. § 1002(a). Thus, some additional authority is required to obtain prospective cell-site information. Section 2703(d) provides this authority because, as discussed in Chapter 3, supra, it authorizes the government to use a court order to obtain all non-content information pertaining to a customer or subscriber of an electronic communication service.

Yet, despite the DOJ's endorsement, this theory is flawed. Its principal failing is that an order granted under Section 2703(d) cannot provide law enforcement with the authority to obtain prospective information; its reach is limited instead to historical records. There is not a single provision of the SCA that contemplates prospective surveillance, nor are there ancillary provisions that address the duration or scope of prospective monitoring activities. In contrast, such provisions are found in every other statute that contemplates future monitoring. Thus, it is apparent that §2703(d) as written was not intended to, and cannot, provide the requisite supplemental authority necessary under CALEA to permit law enforcement to capture real-time location based data. As a result, the hybrid theory must fail as a matter of statutory construction, leaving a Rule 41 Warrant (or a Title III Order) as the sole method of obtaining prospective location data.

In addition to the statutory construction argument, district courts have cited other reasons for rejecting the hybrid theory. For example, some courts have asserted that that cell phones are "electronic or mechanical device[s] which permit[] the tracking of the movement of a person or object" and therefore should be considered "tracking devices" under 18 U.S.C. § 3117(b). This is turn, they argue, would mean that cell site location information would be explicitly excluded from the definition of "electronic communications" under 18 U.S.C. 2510(12), and consequently that neither prospective nor historical location data could be provided to law enforcement under the authority of §2703(d). As applied to either prospective or historical data, this theory has two problems. First, it assumes that any device that a consumer chooses to carry that reports location information becomes a tracking device under

---

and Authorizing the use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *In re Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006).

federal law whenever the government seeks to have access to the information it provides – and there is simply no text or legislative history to support that conclusion. The tracking device statute is designed to cover tracking or homing devices surreptitiously installed by the government. The government may need to seek prior judicial authorization under Rule 41 to surreptitiously install a tracking device on a person or that person's property, but getting records for a device that the consumer voluntarily owns and operates appears to be a separate issue.

Second, and perhaps more importantly, the Stored Communications Act does not exclude tracking device communications from the category of information that can be provided pursuant to 18 U.S.C. § 2703(c). Once an entity is deemed to be a provider of electronic communications – that is a provider that allows users to send and receive either wire or electronic communications – it must provide "records and other information pertaining to [its] subscriber[s] to or customer[s] of such service (not including the contents of communications)" whenever it receives a Court Order issued under 2703(d). Nowhere in this section is it written that these records or other information must themselves be records of electronic communications. In fact, many are not. Further, while Congress chose to explicitly exclude the contents of communications from the records to be provided, it did not provide an exception for communications that may reveal location information. Whereas a provider that solely provides communication services to tracking devices might not be an eligible recipient of a 2703(d) Order, entities that provide tracking device services in addition to other communications services are certainly obliged to provide location-based data when the statutory prerequisites are met.

The search for creative solutions – such as leaning on tracking device provisions – by both privacy advocates and courts is strong evidence of an emerging desire to ensure that reasonably precise real-time and historical location-based information is treated similarly under the law and that a properly robust standard must be met before this type of data is obtained. This makes sense, because information on where an individual has traveled for the hour before a request is made has the same level of intrusiveness as to the information about where the same individual is going to be for the next hour on a real-time basis. But, given the current state of the law, Congressional action is needed to bring about this result.

Without legislative intervention, courts will continue to issue conflicting decisions with differing standards and exacerbate uncertainty amongst law enforcement agencies and providers as they struggle to apply a 1986 law to technology that is only becoming more precise in its ability to pinpoint location and provide an ever expanding universe of information. Further, Congress cannot wait and expect that courts will sort out this problem through proper application of Fourth Amendment doctrine. This is partly because of the Private/Public line that courts have drawn in Fourth Amendment jurisprudence. Even if all devices that provide location-based information were deemed to be "tracking devices" under existing law, the Fourth Amendment would not necessarily require a prior warrant to get information from these devices. The Supreme Court has held that the Fourth Amendment Warrant requirement is applicable only where the information provided by a tracking device reveals information about a person's activities in the interior of constitutionally-protected private spaces, rather

than a public space.[4] So, government would not necessarily need a warrant – either historically or prospectively – to obtain location data about an individual whenever he ventures into a non-constitutionally protected space, but would likely need a warrant when the device is transmitting information from a private space. Such jurisprudence makes it difficult to determine the appropriate standard in advance in all circumstances without statutory guidance. Moreover, we certainly cannot expect the courts, especially the Supreme Court, to address the issue with any alacrity. When presented this past month with an opportunity to apply the Fourth Amendment to text messages sent by public employees, the Court declined indicating that:

> [It] must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. *City of Ontario, California, et al. v. Quon*, Dkt. No. 08-1332, slip. op at 10 (June 17, 2010).

Nor would a court-devised solution be necessarily preferable. Addressing this issue legislatively has benefits both for law enforcement and for privacy rights. For users, amending ECPA to cover this issue would allow Congress to also cover the ancillary issues raised by such surveillance, such as the appropriate duration for orders, need for record-keeping, immunity for providers who comply with orders, emergency disclosure and consent exceptions, and other types of issues found in the prospective monitoring statutes. As for Law Enforcement, a Congressional solution would recognize that the entirety of Fourth Amendment doctrine need not be imported into the new statute and could allow the government more flexibility on issues of particularity and minimization, than if this issue were covered by the Fourth Amendment.

In conclusion, Congress should not mimic the Court's reluctance to move Fourth Amendment doctrine into the 21st century, but instead should take it as a call to arms. Competing claims over privacy rights are contested daily; and in some ways the need for legislative action is even greater now than it was in 1986 when ECPA was originally passed. As the courts and law enforcement struggle to keep pace with rapidly evolving technology and the accompanying expanding universe of information available from service providers, the time is ripe for Congress to set forth clear and sustainable ground rules that balance user expectations and law enforcement needs.

Thank you for the opportunity to testify today. I would be pleased to continue to work with the Committee as the ECPA reform process moves forward.

---

[4] *United States v.* Karo, 468 U.S. 705 (1984) (finding once a beeper has been taken inside a private residence law enforcement must acquire a warrant to monitor it); *United States v. Knotts*, 460 U.S. 276, 282 (1983) (finding that when officers monitor a "beeper" to assist them in conducting surveillance of a vehicle's movements along public roadways, they are not conducting a Fourth Amendment search, as there is no reasonable expectation of privacy on a public road).