Illinois Legislates Privacy Protections for Cell Site Location Information

By Adam J. Sheppard

Justice Roberts accurately quipped that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). And because most smart phone users carry their phones everywhere – "with 12% admitting that they even use their phones in the shower" – if law enforcement officers can track the location of a cell phone, they can track its user. See Riley, 134 S.Ct. at 2490 (citing Harris Interactive, *2013 Mobile Consumer Habits Study* (June 2013)).

I. Cell Site Location Information

Cell site location information (CSLI) reveals the location of the cellular tower or cell site (a portion of the tower) that a cell phone "pings" off at any given time. Even if a cell phone is not making or receiving a call, it is almost constantly pinging off a cell tower. Knowing the location of the cell tower can reveal a phone's location within a relatively small geographic area. In densely populated areas where there are several smaller cell towers known as "base stations," officers may be able to pinpoint a phone's location to a floor or room within a building. *See In* re Application for Tel. Info. Needed for a Criminal Investigation, No. 15XR90304HRL1LHK, 2015 WL 4594558, at *2 (N.D. Cal. July 29, 2015)(citing expert testimony).

In Illinois, until recently, law enforcement officers did not need a search warrant to obtain CSLI. This was so because of the federal Stored Communication Act ("SCA"), enacted in 1986. Under Section 2703(c) of the SCA, a governmental entity may require a "provider of electronic communication service" to disclose cell site location information by obtaining a warrant, issued upon probable cause, *or* by obtaining a "court order" under 18 U.S.C. 2703(d). The latter merely requires the government to offer "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*." 18 U.S.C. §2703 (Emphasis added). Under this less exacting standard, government officers have obtained CSLI with relative ease.

II. The "Freedom from Location Surveillance Act"

In August 2014, Illinois passed the "Freedom from Location Surveillance Act," 725 ILCS 168/1 *et. seq.* Section 168/10 of the Act provides:

> "[A] law enforcement agency shall not obtain current or future location information pertaining to a person or his or her effects without first obtaining a court order based on probable cause to believe that the person whose location information is sought has committed, is committing, or is about to commit a crime or the effect [e.g., the cell phone] is evidence of a crime."

The statute also allows access to location information "if the location information is authorized under an arrest warrant." *Id.* The statute contains several exceptions to the court-order/probable cause requirement. *See* 725 ILCS 168/15. Most of the exceptions relate to "emergency circumstances." However, even in emergency circumstances, officers must apply "for an order approving the previous or continuing obtaining of location information . . . within 72 hours of its commencement." 725 ILCS 168/15.

The Act creates a presumption that information obtained in violation of the Act is inadmissible in any judicial or administrative proceeding. *See* 725 ILCS 168/20. The State may overcome that presumption by proving either a "judicially recognized exception to the exclusionary rule" or "by a preponderance of the evidence that the law enforcement officer was acting in good faith and reasonably believed that one or more of the exceptions identified in Section 15 existed at the time the location information was obtained." 725 ILCS 168/20. This latter provision will seemingly invite litigation; officers, in other fourth amendment contexts, routinely cite "good faith" beliefs that exigent circumstances justified bypassing the warrant requirement.

The Act also does not expressly apply to *historical* CSLI – i.e., CSLI that a service provider has already archived (e.g., CSLI for the last 60 days). The Act discusses "current or future location information." 725 ILCS 168/10. Illinois courts have not addressed whether an officer needs a court order pursuant to 725 ILCS 168/10 to obtain historical CSLI. Federal courts sitting in Illinois have held that officers do not need a warrant to obtain historical CSLI. See *United States v. Lang*, 2015 WL 327338, at *3 (N.D. Ill. Jan. 23, 2015). However, six states have legislated greater protection for historical CSLI. And at least one federal court recently required the government to apply for a warrant for historical CSLI. See *In re Application for Tel. Info. Needed for a Criminal Investigation*, 2015 WL 4594558, at *12.

III. Conclusion

Illinois's "Freedom from Location Surveillance Act" undoubtedly enhances privacy protections in the digital age. The Act could go further by expressly applying to historical location information. The Act also invites litigation by delineating a roadmap for officers seeking to bypass the warrant requirement. Accordingly, practitioners should carefully scrutinize applications for CSLI and, in particular, warrantless retrievals of CSLI.

About the Author: Adam J. Sheppard is a partner in Sheppard Law Firm, P.C. which concentrates in defense of criminal cases. Adam was recently the sole lecturer at the National Business Institute's national teleconference on digital searches and seizures. Adam serves on Decalogue's editorial board and the editorial board of the Chicago Bar Association Record magazine. Adam serves on the CJA federal defender panel. He has been published in various legal periodicals.