epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Alan Butler
Appellate Advocacy Counsel
Electronic Privacy Information Center

Hearing on H.B. 1608, "An Act relating to warrants issued to obtain location information from wireless communications devices and to public access to law enforcement or prosecutor requests for certain related location or communication information"

Before the

Texas House of Representatives,
Committee on Criminal Jurisprudence

March 26, 2013
Texas Capitol
112 E. 11th St.
Austin, TX 78701

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the important issue of location privacy. My name is Alan Butler, and I am the Appellate Advocacy Counsel at the Electronic Privacy Information Center ("EPIC").

EPIC is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] We have a particular interest in protecting individual privacy by limiting unwarranted government surveillance. For many years, we have tracked the government's use of electronic surveillance authority.[3] Over the last several years, EPIC has taken an interest in the growing problem of location privacy,[4] which the Supreme Court recently addressed in its landmark opinion, *United States v. Jones*.[5]

In my statement today, I will discuss H.B. No. 1608 and the need for legislative clarity regarding law enforcement authority to collect subscriber location data. In addition, I will highlight the need for comprehensive reporting of location surveillance to ensure that legal authority is properly exercised. Communications devices have become an essential component of our modern lives, and we keep them with us at all times. The location data generated by these devices reveals a great deal of private information about our activities, associations, habits, and beliefs. Due to the highly sensitive nature of this data and its widespread use in state and federal investigations, it is necessary to establish strong procedural safeguards.

We appreciate the Committee's interest in this topic and support your efforts to establish stronger privacy safeguards in the state of Texas.

I. Analysis of H.B. No. 1608

The proposed bill would provide much needed clarity in an increasingly confusing area of the law: government authority to conduct location surveillance. A warrant requirement is necessary to ensure that there is an independent determination, by a judge or magistrate, that the collection and use of location information is consistent with the standard applied under the federal and state Constitutions. In addition, this bill would create a comprehensive reporting scheme, similar to the wiretap reporting conducted by the Administrative Office of the Courts, that would ensure proper administration of the system and limit surveillance abuses.

Since 2005 there have been more than a hundred state and federal cases involving location data requests. These increasingly complex legal opinions draw on such diverse sources of law as the Electronic Communications Privacy Act,[6] the Pen Register Act,[7] the Communications Assistance for Law Enforcement Act,[8] various state procedural laws, the

[1] *About EPIC*, http://www.epic.org/about (last visited Feb. 20, 2013).
[2] *EPIC Advisory Board*, http://www.epic.org/epic/advisory_board.html (last visited Feb. 20, 2013).
[3] *See* EPIC, *Wiretapping*, http://epic.org/privacy/wiretap/ (last visited Feb. 20, 2013).
[4] *See*, *e.g.*, Supplemental Brief of Amicus Curiae EPIC, *State v. Earls*, 209 N.J. 97 (2011), *available at* http://epic.org/amicus/location/earls/EPIC-Supplemental-Amicus-Brief.pdf; Brief of Amicus Curiae EPIC Urging Affirmance, *In re U.S.*, No. 11-20884 (5th Cir. Mar. 16, 2012), *available at* http://epic.org/amicus/location/cell-phone-tracking/EPIC-5th-Cir-Amicus.pdf; Brief of Amicus Curiae EPIC, *State v. Earls*, 209 N.J. 97 (2011), *available at* http://epic.org/amicus/location/earls/EPIC-Earls-Amicus-NJ-SCt.pdf.
[5] 132 S.Ct. 945 (2012).
[6] Title II is commonly referred to as the "Stored Communications Act," 18 U.S.C. §§ 2701-2712.
[7] Title III of ECPA, 18 U.S.C. §§ 3121-3127.
[8] *See* 47 U.S.C. § 1002(a)(2)(B).

Fourth Amendment, and equivalent state constitutional provisions. Judges have drawn distinctions between real-time versus historical location data, between precise versus general location information, and between passive versus active surveillance. The resulting legal patchwork provides neither a workable system for law enforcement officials and communications providers nor an adequate framework to protect user privacy. The United States Supreme Court recently made clear in *Jones* that location tracking implicates the Fourth Amendment, and a warrant requirement comports with that understanding.

It will be difficult to have any in-depth discussion of location surveillance based on the limited information now available about its scope and operation. There are currently no state or federal reporting requirements for government location data requests, and most service providers are reluctant to discuss details about their law enforcement compliance programs. The reporting provisions in H.B. 1608 would provide the information necessary to ensure that this private data is only being collected and used to further criminal investigations.

Without these changes there will be substantial legal uncertainty while government investigators and communications providers continue to struggle to ensure that their requests comport with federal and state constitutional requirements.

II. Federal Law Does Not Directly Address Location Surveillance, and Lower Courts Disagree Over Whether a Warrant Is Necessary

There is substantial confusion in the application of federal and state authorities to location surveillance, which underscores the need to establish clear rules. The Electronic Communications Privacy Act ("ECPA") governs surveillance authority on the federal level, and also sets a baseline for state government authority. However, the ECPA does not distinguish between location records and other "non-content" subscriber records, such as toll billing records. The Department of Justice ("DOJ") currently interprets ECPA to authorize collection of location data with a court order upon a showing that the information is "relevant and material" to an ongoing criminal investigation.[9] But even the DOJ requires a warrant to collect "more precise" location data generated by GPS or similar technologies.[10]

Many courts, including federal courts here in Texas, have rejected the DOJ's broad view of location surveillance authority under ECPA. Some courts have found that the collection of real-time cell phone location data is akin to a "tracking device."[11] Other courts have granted location surveillance orders based on the limited precision of the technology available at the time.[12] One court of appeals has held that magistrate judges have the discretion to require a probable cause showing to grant a location surveillance order.[13] And Magistrate Judge Smith in

[9] For prospective, real-time location data the DOJ also requires a Pen Register order. The combination of the two is referred to as a "hybrid order." U.S. DEP'T OF JUSTICE (DOJ), SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 160 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[10] *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice), *available at* http://1.usa.gov/IsojNy.

[11] *In re U.S.*, 396 F. Supp. 2d 747, 753-64 (S.D. Tex. 2005); *In re U.S.*, 396 F. Sup. 2d 294, 322 (E.D.N.Y. 2005).

[12] *In re U.S.*, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005).

[13] *In re U.S.*, 620 F.3d 304, 313 (3d Cir. 2010).

the Southern District of Texas recently held that a compelled warrantless disclosure of location data generated by current technology would violate the Fourth Amendment.[14]

III. Users Have a Reasonable Expectation of Privacy in Their Location Records

While these lower court opinions have created a chaotic and unpredictable privacy regime, the Supreme Court recently reaffirmed the importance of protecting individual privacy under the Fourth Amendment. The *Jones* opinion, combined with prior location surveillance and technological search precedents, leans heavily in favor of finding strong Fourth Amendment protections for location data, even though it did not directly address the question of subscriber location data requests.

The collection and use of location data implicates constitutional privacy interests as the data necessarily reveals intimate details of user activities, associations, and habits within private spaces such as homes. Society recognizes that individuals have an objective expectation of privacy in this information. A subscriber's reasonable expectation is not eliminated by their use of a cell phone, which is a basic component of modern life.

Five Supreme Court Justices, writing in concurrence in *Jones*, agreed that "longer term" monitoring of location "impinges on expectations of privacy."[15] This view has been supported by other recent federal and state court opinions.[16] However, the current procedural standards for acquiring location data are inconsistent and the collection and use of location data by government is not subject to public reporting or notice requirements.[17]

IV. Location Surveillance Should Be Subject to the Same Reporting Requirements as Similar Investigative Searches

There are currently no reporting requirements for location-data collection in the state of Texas. Recent disclosures by cell phone service providers give a rough estimate of the scale of this surveillance activity, and the numbers are staggering – 1.3 million requests across the country for subscriber information in 2011 alone.[18] Without adequate reporting, we cannot know how many of these requests involved location information, or whether the data collected supported any criminal convictions.

---

[14] *In re U.S.*, 747 F. Supp. 2d 847, 830 (S.D. Tex. 2010).

[15] *See Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring); *id*. at 964 (Alito, J., concurring).

[16] *See State v. Zahn*, 812 N.W.2d 490 (S.C. 2012); *People v. Weaver*, 12 N.Y.3d 433 (2009); *State v. Jackson*, 150 Wash.2d 251, 262 (2003); *In U.S.*, 620 F.3d 304 (3d Cir. 2010); *In re U.S.*, 747 F. Supp. 2d 827 (S.D. Tex. 2010); *State v. Holden*, 54 A.3d 1123 (Del. Super. Ct. 2010); *Commonwealth v. Wyatt*, 30 Mass.L.Rptr. 270 (Mass. Sup. Ct. 2012). As the New York Court of Appeals noted in *Weaver*:

> Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which it takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.

Weaver, 12 N.Y.3d at 441-42.

[17] *See* Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, N.Y. Times (Jul. 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all.

[18] *Id*.

In contrast, our current state and federal wiretap reporting system provides a wealth of useful information about law enforcement efforts. The Administrative Office of the United States Courts works closely with prosecutors, judges, and law enforcement officers to provide a detailed overview of the cost, duration, and effectiveness of wiretap surveillance.[19] The annual report breaks requests down into useful statistical categories, including the type of crimes involved. Such information is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities.

The annual wiretap report provides a basis to evaluate the effectiveness of surveillance authority, to measure its cost, and to determine whether the private data captured is relevant to an investigation. These reporting requirements ensure that law enforcement resources are appropriately and efficiently used while safeguarding important constitutional privacy interests.

V. Conclusion

The increased collection and use of location data should be accompanied by increased privacy protections. H.B. No. 1608 sets out a reasonable framework to regulate the collection of personal location data gathered in the course of a criminal investigation.. In addition, the reporting requirement will go a long way to providing a basis to evaluate this new investigative technique.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

[19] Admin. Office of the U.S. Courts, *Wiretap Reports*, http://www.uscourts.gov/Statistics/WiretapReports.aspx (last visited Feb. 20, 2013).