Testimony and Statement for the Record of

Alan Butler
Appellate Advocacy Counsel
Electronic Privacy Information Center

Hearing on H.B. 887, "An Act concerning Criminal Procedure – Search Warrants – Location Privacy?"

Before the

Maryland House,
Committee on the Judiciary

February 26, 2013
100 State Circle
Annapolis, MD 21401

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. 887, a bill that would establish a warrant requirement for access to location data and mandate annual reporting of executed warrants. I will also describe the unique threats to privacy posed by warrantless collection of location information from electronic devices, including cell phones. These devices have become an essential component of our modern lives, and we keep them with us at all times. The location data generated by our phones and other 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 Maryland.

I. Analysis of H.B. 887

H.B. 887 would establish a search warrant requirement for the collection of location information with limited exceptions for emergency circumstances and user consent. In addition, the bill would establish notice and reporting requirements for executed location warrants. The bill would also limit abuse by prohibiting the use of unlawfully obtained location evidence.

The warrant requirement contained in this bill 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 federal and state Constitutions. Officers in many states, including Maryland, already recognize the constitutional protections for location data and obtain warrants in investigations.[6] The exclusionary provision is also important to ensure compliance with the legal standards.

---

[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] *See United States v. Jones*, 132 S.Ct. 945 (2012) (warrant obtained for GPS tracking in Maryland, but collection was ruled unconstitutional where the search occurred in a different state when the warrant was expired).

This bill is technology neutral in order to protect location data, regardless of the technique. Many electronic devices generate location data, including cell phones, cameras, cars, and others. Not all these devices enable access to remote computing or electronic communications services, but the law should make clear that any device generating location data is covered because it enables a "location information service."[7] This will ensure that technological adaptations do not erode these important location privacy protections.

Location information is generated by many of the electronic devices we use every day, including cell phones,[8] cameras,[9] computers,[10] cars,[11] and others. This location data is increasingly precise and is in many cases stored for months or even years without user knowledge or consent. Modern surveillance technologies also enable collection of location data from cell phones in real time through a process called triangulation.[12] These advanced location capabilities highlight the need for judicial oversight, procedural protections, and transparency.

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

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.

User privacy expectations were recently reaffirmed by the Supreme Court in the *Jones* case. The U.S. Congress has also recognized consumer privacy interests in location information and provided for explicit protections in the Communications Act.[13] Courts are now grappling with the difficult task of applying privacy rules created for low-tech "beeper technology" to the current advanced location tracking capabilities. It is necessary to provide additional safeguards to the use of these new techniques to avoid permitting "police technology to erode the privacy guaranteed by the Fourth Amendment."[14]

---

[7] This includes devices such as cameras and car data recorders that gther and store location information.

[8] *See* Larry Bodine, *The Legal Battle Over Cell Phone Location Privacy*, Huffington Post (Oct. 24, 2012), http://www.huffingtonpost.com/larry-bodine/the-legal-battle-over-cel_b_2003190.html.

[9] *See* Mark Millian, *Digital Photos Can Reveal Your Location, Raise Privacy Fears*, CNN Tech (Oct. 15, 2010), http://articles.cnn.com/2010-10-15/tech/photo.gps.privacy_1_smartphone-exif-gps?_s=PM:TECH.

[10] *See* Amir Efrati & Jennifer Valentino-Devries, *Computers, Too, Can Give Away Location*, Wall St. J. (Apr. 26, 2011), http://online.wsj.com/article/SB10001424052748703778104576287401134790790.html.

[11] *See* Kashmir Hill, *The Big Privacy Takeaway From Tesla vs. The New York Times*, Forbes (Feb. 19, 2013), http://www.forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-takeaway-from-tesla-vs-the-new-york-times/.

[12] *See* Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

[13] See, 47 U.S.C. § 222(f):

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4) of this section; or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

[14] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

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]

III. Current Reporting Requirements Do Not Provide Adequate Transparency

There are currently no reporting requirements for location-data collection in the state of Maryland. 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 information proved relevant to an investigation. 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 and federal courts 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.

IV. Conclusion

The increased collection and use of location data should be accompanied by increased privacy protections. H.B. 887 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.

---

[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*.

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