Written Testimony of Nathan Freed Wessler on behalf of the American Civil Liberties Union Before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology

Hearing on

"Seven Communications Bills" including H.R. 4889, the Kelsey Smith Act of 2016

Wednesday, April 13, 2016, at 10:15am

Submitted by the
ACLU Washington Legislative Office

[redacted]

Chairman Walden, Ranking Member Eshoo, and Members of the Committee:

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) regarding H.R. 4889, the Kelsey Smith Act.[1] Although the impetus behind this legislation is commendable, as currently drafted the bill raises a number of concerns.

When used properly, cell phone location information can be a powerful public safety or law enforcement tool. But, because of the sensitivity of this data, it is crucial that government access be permitted only in the context of strong safeguards that protect Americans' privacy. Because H.R. 4889 does not include sufficient safeguards, the ACLU opposes the legislation in its current form. However, if the bill moves forward, we urge the subcommittee to amend it to include the following protections:

- Make emergency disclosure of location information by service providers voluntary rather than mandatory, in order to protect against disclosure when there is no genuine emergency, or when criminals seek location records by impersonating law enforcement officials.

- Require after-the-fact judicial review and prompt notice to the person whose location information was obtained.

- Require judicially enforceable remedies when location information is acquired in violation of the law.

- Raise the legal standard governing access to location information in an emergency from "reasonable belief" to "probable cause" in order to avoid disclosure of sensitive location information in the absence of a genuine emergency.

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than a million members, activists and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

I. The Fourth Amendment protects individuals' location information.

Under current law, providers of electronic communications are required to keep the records and personal information of users confidential from the general public and the government.[2] Given the technical realities of modern communications, this protection is critical. Cell phones are capable of tracking every American's movements continuously and for an extended duration. As such, location information is some of the most revealing data possessed by carriers. As Justice Sonia Sotomayor wrote in her concurrence in a recent Supreme Court decision regarding location tracking, *United States v. Jones*:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . Disclosed in [GPS] data . . . will be trips the indisputably private nature of which 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. . . . The Government can store such records and efficiently mine them for information years into the future.[3]

The full Supreme Court recently reiterated this concern when it recognized that strong Fourth Amendment protections are needed for cell phones in part because "location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[4] Other federal and state courts have likewise held that people have a reasonable expectation of privacy in their cell phone location information, and therefore

[2] 18 U.S.C. § 2701 et. seq.; 47 U.S.C. § 222.
[3] *United States v. Jones*, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, concurring); *accord id*. at 963–64 (Alito, J., concurring in the judgment) (recognizing that "cell phones and other wireless devices now permit wireless carriers to track and record the location of users" and explaining that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").
[4] *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

that the full protections of the Fourth Amendment apply.[5] As the Florida Supreme Court put it:

> because cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs, is clearly a Fourth Amendment violation.[6]

In light of the deep privacy interest in cell phone location information, it is critical that any legislation permitting law enforcement access to that data include strong privacy protections.

II. Mandatory disclosure would facilitate abuse of emergency requests.

In its current form, H.R. 4889 requires certain telecommunications carriers to provide cell phone location information to law enforcement any time a "law enforcement officer reasonably believes [the individual in possession of the phone] is in an emergency situation that involves the risk of death or serious physical harm to the individual." This disclosure would be mandatory on the part of the provider. While the objectives of this legislation are laudable—to assure speedy access to location information in the case of emergencies—there are already effective and timely mechanisms in place to share location information. The danger is that this legislation will not improve on those mechanisms, but instead simply expand the number of wrongful disclosures in non-emergency circumstances.

---

[5] *See United States v. Graham*, 796 F.3d 332 (4th Cir. 2015), *rehearing en banc pending*; *Tracey v. State*, 152 So. 3d 504 (Fla. 2014); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); *State v. Andrews*, __ A.3d __, 2016 WL 1254567 (Md. Ct. Spec. App. March 30, 2016); *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); *In re Application for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone*, 849 F. Supp. 2d 526 (D. Md. 2011).

[6] *Tracey*, 152 So. 3d at 524.

Congress has recognized that there are times when, consistent with the exception for warrantless exigent searches under the Fourth Amendment, cellular service providers must breach this confidentiality and share information, including location information, with the government. As such, an existing federal statute already allows disclosure by a provider "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[7]

This current process works. According to the transparency reports of two major providers, AT&T and Verizon, those companies processed more than 81,000 requests for emergency information (unrelated to 911 calls) just in 2015.[8] Cellular service providers take seriously their responsibility to respond to law enforcement requests in emergencies, maintaining large law enforcement compliance teams that operate around the clock and can respond to requests at any hour.[9] In order to facilitate emergency requests, the

[7] 18 U.S.C. § 2702(c)(4).

[8] AT&T, Transparency Report (2016), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf; *United States Report*, Verizon https://www.verizon.com/about/portal/transparency-report/us-report/ (last visited April 11, 2016).

[9] *See, e.g.*, Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T, to Sen. Edward Markey (Oct. 13, 2013), https://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf ("AT&T employs more than 100 full time workers and operates on a 24x7 basis for the purposes of satisfying law enforcement requests for information."); *Law Enforcement Relations*, T-Mobile USA, Inc., , https://www.t-mobile.com/Cms/Files/Published/0000BDF20016F5DD010312E2BDE4AE9B/0000BDF20016F5DE011CB9630A8D07DE/file/Law%20Enforcement%20Security%20Procedures%20For%20T-Mobile%20Website.pdf (explaining that "[t]he T-Mobile USA, Inc. Law Enforcement Relations Group (LER Group) is committed to efficiently assisting the law enforcement community with all lawfully authorized activities" and that it operates "24 x 7"); Letter from Charles W. McKee, Vice President, Government Affairs, Federal and State Regulatory, Sprint Corporation, to Sen. Edward Markey (Oct. 25, 2013), https://assets.documentcloud.org/documents/889100/response-sprint.pdf ("Pursuant to the legal requirements of CALEA, Sprint is required to have a team available 24 hours per day, 7 days per week to respond to demands form law enforcement.").

providers even waive the fees they charge for normal (non-exigent) cell phone tracking requests.[10]

Not all emergency requests meet the existing standard for emergencies, however, meaning that there must be some mechanism for curbing unjustified attempts to obtain location information. If providers must turn over records any time law enforcement asserts an emergency, there is a real danger of significant oversharing stemming from law enforcement's incorrect use of the emergency exception. Indeed, there is a record of law enforcement pushing the envelope and using the emergency procedure to avoid seeking judicial review of a request. In a number of cases involving requests under the emergency provisions of the Electronic Communications Privacy Act[11] or analogous state laws, courts have criticized law enforcement for illegally seeking emergency disclosure on "a speculative basis,"[12] or otherwise without justification. Recent examples of abuse of the emergency request process include:

- Police in Anderson, California, coerced a person seeking a restraining order into saying she had been held against her will for six hours, and then sent a false emergency request for location information to the purported kidnapper's cellular service provider.[13]

- A police officer in Lewisville, Texas, obtained a suspect's cell phone location information through an emergency request, but under questioning "could not say specifically whose life he thought was in danger."[14]

- Police in Rochester, New York, obtained location information about a suspect's cell phone when they already knew the suspect's location but wanted to build a better case by obtaining information from the phone.[15]

---

[10] *See* AT&T Letter to Sen. Markey, *supra* note 9 ("AT&T imposes no charges for handling emergency requests."); Sprint Letter to Sen. Markey, *supra* note 9 ("No fee in exigent . . . situations.").
[11] 18 U.S.C. § 2702.
[12] *Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121, 128 (D. Conn. 2004).
[13] *Jayne v. Sprint PCS*, No. CIVS072522LKKGGHP, 2009 WL 426117, at *2 (E.D. Cal. Feb. 20, 2009).
[14] *State v. Harrison*, No. 02-13-00255-CR, 2014 WL 2466369, at *4–5 (Tex. App. May 30, 2014).
[15] *People v. Moorer*, 959 N.Y.S.2d 868, 872, 875 (N.Y. Co. Ct. 2013).

- A police officer in Princess Anne County, Maryland, used an emergency request form to obtain records from Sprint, but later conceded in sworn testimony that "there was no such emergency at the time he requested the records."[16]

Likewise, records obtained from police departments by the ACLU have revealed "some departments specifically warn[ing] officers about the past misuse of cellphone surveillance in nonemergency situations."[17] In Reno, Nevada, for example, a law enforcement training document cautioned that warrantless cell phone tracking "IS ONLY AUTHORIZED FOR LIFE-THREATENING EMERGENCIES!!" Emergency tracking had been "misused," however, leading the police department to warn officers that "[s]ome cell carriers have been complying with such requests, but they cannot be expected to continue to do so as it is outside the scope of the law. Continued misuse by law enforcement agencies will undoubtedly backfire."[18]

Indeed, providers have had to deny emergency requests for cell phone location records in cases where "they determined that a true emergency did not exist."[19] At least in some contexts, emergency requests are denied by providers with a level of frequency suggesting that there are numerous instances where such requests fail to meet the appropriate standards. For example, from January to June 2015, Google denied 31% of the emergency requests it received.[20] Even the U.S. Department of Justice has recognized its own abuse of emergency requests. In a comprehensive 2010 investigation, the DOJ

[16] *Upshur v. State*, 56 A.3d 620, 625–26 (Md. App. 2012).
[17] Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. Times, July 8, 2012, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html.
[18] Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. Times, Mar. 31, 2012, http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html; *see also* Response to ACLU Public Records Request from the Reno, Nevada, Police Department (Aug. 5, 2011), *available at* https://www.aclu.org/cell-phone-location-tracking-documents-nevada?redirect=protecting-civil-liberties-digital-age/cell-phone-location-tracking-documents-nevada#Reno..
[19] Lichtblau, *More Demands on Cell Carriers in Surveillance*, *supra* note 17.
[20] *Transparency Report: United States*, Google, , https://www.google.com/transparencyreport/userdatarequests/US/ (last visited April 11, 2016). Those rejections include cases where Google did not have any responsive records as well as cases where law enforcement failed to substantiate the claimed emergency.

Inspector General found that, in the years following the 9/11 attacks, the FBI repeatedly misused so-called "exigent letters" and other informal requests to compel the production of telephone records and other material. In many cases, the FBI presented the request as exigent when it was not, in fact, an emergency.[21] As the Chief Justice of the Georgia Supreme Court has explained, we should be wary of attempts by "law enforcement to circumvent the strict procedural requirements for accessing protected records by simply 'requesting' such records with a tone of sufficient urgency so as to generate a belief on the part of the custodian that an emergency exists."[22]

Additionally, mandatory emergency disclosure coupled with the potential for thieves to impersonate law enforcement when "dialing for data" poses serious privacy concerns. Recognizing the danger of thieves calling service providers and asking for customer records under false pretenses, Congress enacted the Telephone Records and Privacy Protection Act of 2006,[23] which makes it a federal felony, punishable by up to 10 years in prison, to use "pretexting" to obtain call records.[24] Tellingly, the statute includes heightened penalties if the records are used to facilitate cyber-stalking, one of the primary concerns driving the legislation.[25] The law's passage followed disclosures that Hewlett

[21] In other cases, the FBI failed to provide the relevant details and the providers just assumed that the requests were exigent. Dep't of Justice, Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records 257–72 (2010) (detailing the IG's findings with respect to improper FBI use of exigent letters and other informal requests in violation of 18 U.S.C. § 2702's emergency exception).
[22] *Registe v. State*, 734 S.E.2d 19, 22 (Ga. 2012) (Hunstein, C.J., concurring).
[23] Pub. L. No. 109-476, 120 Stat. 3568 (2007).
[24] 18 U.S.C. § 1039(a).
[25] *Id.* § 1039(d). Reinforcing this concern, Louisiana and Washington State's versions of the Kelsey Smith Act includes specific protections against release of device location information "to a person who either has a history of domestic violence or stalking or who is subject to any court order restricting contact with the device user." La. Stat. Ann. § 45:844.9(B)(5); *accord* Wash. Rev. Code § 80.36.570(1)(d), (f).

Packard had used false pretenses to obtain the phone records of journalists in an attempt to undercover the source of media leaks.[26]

Although service providers comply with most emergency requests, the ability to reject a request functions as an important safety valve. In the face of emergency requests by individuals falsely claiming to be law enforcement or by law enforcement agents in the absence of a true emergency, communications providers must be given the discretion to resist the request. Under current law, service providers are able to do just that.[27] This discretion is particularly important given the unique time pressures and heightened emotion attendant in an emergency request.

III. Any mandatory emergency disclosure should include after-the-fact judicial review, judicially enforceable remedies, and notice.

Although the ACLU opposes a mandatory emergency disclosure requirement, if adopted, any such requirement must incorporate strong protections against abuse. Those protections should include after-the-fact judicial review, a judicially enforceable remedy for any person whose location information is illegally obtained, and notice to the person whose location information was sought.

As currently written, H.R. 4889 provides no opportunity for judicial review of emergency requests by law enforcement. In a true emergency, where there is no time to obtain a court order prior to seeking and obtaining location records, it is crucial that law

[26] Anne Broache, *The President Signs Pretexting Bill into Law*, CNET, Jan. 17, 2007, http://www.cnet.com/news/president-signs-pretexting-bill-into-law/.

[27] *See* AT&T Letter to Sen. Markey, *supra* note 9 ("Before responding to emergency tracking requests, AT&T requires law enforcement to provide a written description of the emergency and to certify the facts presented are true and that they constitute an emergency involving danger of death or serious physical injury to a person, requiring disclosure without delay."); Sprint Letter to Sen. Markey, *supra* note 9 ("Sprint's processes require law enforcement to fax in a form that Sprint uses to authenticate the law enforcement requestor and to verify that an appropriate emergency exists."); T-Mobile, *Law Enforcement Relations*, *supra* note 9 ("During an emergency, the Law Enforcement Relations Group (LER Group) will attempt to verify the caller's identity as a legitimate representative of the Public Safety Answering Point (PSAP or 911 Emergency Dispatcher).").

enforcement be required to seek judicial approval as soon as possible after making the request. Doing so will deter abuse of the emergency requests process and provide a check on unjustified emergency demands. Indeed, the version of this legislation introduced in the 113th Congress contained such a requirement, providing:

> Not later than 48 hours after an investigative or law enforcement officer makes a request for call location information under subsection (a), the law enforcement agency of such officer shall request a court order stating whether such officer had probable cause to believe that the conditions described in subsection (b)(1) or subsection (b)(2) existed at the time of the request under subsection (a).[28]

Just last month, the Indiana legislature enacted similar legislation that includes a requirement for retroactive judicial approval following an emergency request for location information.[29] California and Colorado law likewise includes this requirement.[30]

The requirement that law enforcement secure retroactive judicial approval after obtaining communication records in an emergency is longstanding. The Pen Register Statute, which provides for law enforcement monitoring of "dialing, routing, addressing, or signaling information" transmitted or received by a phone,[31] permits emergency requests only if, "within forty-eight hours after the [monitoring] has occurred, or begins

[28] H.R. 1575, 113th Cong. (2d Sess. 2015).
[29] Ind. Pub. L. 57 (H.B. 1013), § 3 (2016) (to be codified at Ind. Code § 35-33-5-15(b)) ("If law enforcement makes a request for geolocation information under this subsection [in an emergency] without first obtaining a search warrant or another judicial order, the law enforcement agency shall seek to obtain the search warrant or other judicial order issued by a court based upon a finding of probable cause that would otherwise be required to obtain the geolocation information not later than seventy-two (72) hours after making the request for the geolocation information.").
[30] Cal. Penal Code § 1546.1(h) ("If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the entity shall, within three days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information . . . ."); Colo. Rev. Stat. § 18-9-312(1.5)(e) ("Not more than forty-eight hours after ordering a previously designated security employee of a wireless telecommunications provider to provide [emergency] information as described in paragraph (a) of this subsection (1.5), a law enforcement agency shall request a court order . . . .").
[31] 18 U.S.C. §§ 3122–23, 3127(3)–(4).

to occur, an order approving the installation or use is issued" by a judge.[32] "In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier."[33] Congress has likewise recognized the importance of retroactive judicial approval following emergency requests even in the national security context. The recently passed USA Freedom Act requires that the government apply for a court order following an emergency request for records obtained under Section 215 of the Patriot Act, which the government asserts is used in national security-related investigations.[34]

The Pen Register Statute provides a mechanism for law enforcement access to basic information like the phone numbers dialed on a telephone to connect a call. Recognizing that cell phone location information is even more sensitive than these dialing records, and thus deserving of a higher level of protection, in 1994 Congress explicitly prohibited use of the Pen Register Statute to obtain "information that may disclose the physical location of the subscriber."[35] It would be a step backward to now provide *lesser* protection to location information, which Congress and the courts have explicitly recognized to be deserving of *greater* safeguards against unjustified government access. Requiring after-the-fact judicial approval protects against abuse

[32] *Id.* § 3125(a).
[33] *Id.* § 3125(b).
[34] 50 U.S.C. § 1861(i)(1)(D), as enacted by USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 ("[T]he Attorney General may require the emergency production of tangible things if the Attorney General . . . makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.").
[35] 47 U.S.C. § 1002(a), enacted by Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

without interfering with law enforcement's ability to quickly obtain location information in a genuine emergency.

The legislation should also provide a remedy in cases where the court finds a violation of the law or fails to provide retroactive authorization. In criminal, immigration, or administrative proceedings, the illegally obtained location information and any evidence derived from it should be suppressed. Without suppression, an individual could be harmed by clearly illegal conduct, but have no remedy—a gross injustice that is at odds with criminal procedural remedies in other contexts. The legislation should also provide a civil remedy so that all people, including those never charged with a crime, can obtain relief from the courts when a judge has determined that law enforcement violated the law. These protections will not only provide redress to people harmed by illegal searches of their location information, but will also deter law enforcement officers from violating the law in the first place. Suppression and civil remedies are common and important features of other electronic surveillance statutes, and should be included here.[36]

Finally, the legislation should mandate prompt notice to the person whose location information is obtained. Without notice, that person cannot know that police sought and obtained his or her records, and cannot pursue judicial remedies in cases where the location tracking request violated the law. California's recently enacted statute addressing emergency requests for location information requires such notice,[37] and this

[36] *See, e.g.*, 50 U.S.C. § 1861(i)(5) ("If such application for [emergency] approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding."); 18 U.S.C. § 2707 (providing civil remedy for violation of emergency disclosure provisions of Electronic Communications Privacy Act); Cal. Penal Code § 1546.4 (providing for suppression of evidence obtained in violation of emergency request procedures).

[37] Cal. Penal Code § 1546.1(h).

legislation can easily incorporate it without jeopardizing legitimate law enforcement investigations.

IV. The standard for emergency disclosure should be raised.

The current version of H.R. 4889 mandates disclosure of location information whenever a law enforcement officer "reasonably believes" an individual "is in an emergency situation that involves the risk of death or serious physical harm to that individual." The "reasonable belief" standard is too low, and will result in disclosure of sensitive location information when there is not actually a qualifying emergency. Instead, any mandatory emergency disclosure should be permitted only when law enforcement has probable cause to believe immediate disclosure is required by an emergency involving death or serious physical harm and that the records sought relate to the emergency. A probable cause standard will ensure that law enforcement can only access sensitive location information without a prior court order when officers have good reason to believe an emergency exists.

The probable cause standard is familiar to law enforcement, who apply it daily when applying for search warrants,[38] conducting warrantless searches of vehicles,[39] and engaging in exigent searches without a warrant.[40] Probable cause has the twin virtues of being familiar to law enforcement and protective of individual privacy rights in the context of sensitive information recognized as deserving of the highest protections of the Fourth Amendment.[41] Indeed, law enforcement in several states already abide by a

[38] *See, e.g.*, U.S. Const. amend. IV ("no Warrants shall issue, but upon probable cause").
[39] *See California v. Acevedo*, 500 U.S. 565, 579–80 (1991) ("[T]he police may search [a vehicle and its contents] without a warrant if their search is supported by probable cause.").
[40] *See, e.g.*, *Welsh v. Wisconsin*, 466 U.S. 740 (1984).
[41] *See supra* cases cited in note 5.

probable cause standard for emergency requests for location information,[42] and the version of this legislation introduced in the 113th Congress included a probable cause standard.[43]

V. Conclusion.

The ACLU respectfully urges the Committee to reject the current version of H.R. 4889. Current law already provides an effective mechanism for emergency requests for cell phone location information, making this legislation unnecessary. If a bill is to move forward, however, it should include safeguards to protect personal privacy, including eliminating the mandatory disclosure provision, providing for after-the-fact judicial review, judicial remedies for violation of the law, and notice, and incorporating a probable cause standard for emergency requests.

[42] *See* Colo. Rev. Stat. § 18-9-312(1.5)(a); Ind. Pub. L. 57 (H.B. 1013), § 3 (2016) (to be codified at Ind. Code § 35-33-5-15(b)).

[43] H.R. 1575, 113th Cong. (2d Sess. 2015) ("A request to a provider of a covered service by an investigative or law enforcement officer for call location information under subsection (a) shall be accompanied by a sworn written statement from such officer stating facts that support such officer's *probable cause* to believe that disclosure without delay is required—(1) by an emergency involving risk of death or serious physical injury . . . ." (emphasis added)).