AMERICAN CIVIL LIBERTIES UNION
Wisconsin

207 East Buffalo Street, Ste 325
Milwaukee, WI 53202
(414) 272-4032
aclu-wi.org

February 1, 2024

Chair Spiros, Vice-Chair Schutt, and Honorable Members of the Assembly Committee on Criminal Justice and Public Safety:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide comments detailing our constitutional concerns with Assembly Bill 960. When used properly, cell phone location information can be a powerful public safety or law enforcement tool. However, because of the sensitivity of this data, it is critical that government access be permitted only when strong safeguards are in place to protect Wisconsinites' privacy. While ACLU-WI is opposed to AB-960 in its current form, suggested amendments are included at the end of these comments.

Under the bill, an electronic communication service provider *must* disclose the location of a communications device to law enforcement without a warrant if "[t]he customer or subscriber provides consent" or the law enforcement agency sends a written request stating (or "attesting" under Assembly Amendment 1) the following:

- Disclosure of device location information is needed for law enforcement to respond to a call for emergency services; or
- Disclosure of device location information is needed to allow a law enforcement agency to respond to an emergency situation that involves the danger of death or serious physical injury to any person and disclosure of device location information is necessary to prevent or mitigate that danger

Cell Phone Location Information is Highly Sensitive

The proliferation of cell site simulators (aka "Stingrays"),[1] geofence warrants,[2] and other cellphone tracking tools[3] used by law enforcement in Wisconsin and nationwide has triggered constitutional alarm bells for privacy experts. The government knowing where a person's phone is located—tracking their every move—can reveal highly private and sensitive information.

---

[1] Isiah Holmes, "How the Milwaukee PD uses cell phone surveillance technology," Wisconsin Examiner (July 15, 2022), https://wisconsinexaminer.com/2022/07/15/how-the-milwaukee-pd-uses-cell-phone-surveillance-technology/; "Stingray Tracking Devices: Who's Got Them?," ACLU (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them.

[2] Bobby Allyn, "Privacy advocates fear Google will be used to prosecute abortion seekers," NPR (July 11, 2022), https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions; Matthew Guariglia, "Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide," Electronic Frontier Foundation (Sept. 10, 2021), https://www.eff.org/deeplinks/2021/09/geofence-warrants-threaten-civil-liberties-and-free-speech-rights-kenosha-and.

[3] Garance Burke and Jason Dearen, "Tech tool offers police 'mass surveillance on a budget,'" AP (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.

As the U.S. Supreme Court noted in *Carpenter v. United States*, cell phone location information provides, "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the 'privacies of life.'"[4] Congress has recognized how sensitive this data is, enacting legislation that requires electronic communication service providers to keep this information confidential from the general public and the government.[5]

Cell phone location information is protected by the Fourth Amendment, which means law enforcement either needs a warrant or an exception to the warrant requirement to access this information. While exigent circumstances constitute an exception to the warrant requirement, this exception requires exigency, plus probable cause, plus insufficient time to obtain a warrant. The provisions of the bill outlining the standard for law enforcement requests to electronic communication service providers falls short of what the government needs to prove to fit under this exception.

AB-960 Opens the Door to Abuse of Emergency Requests

Under the bill, telecommunications providers would be forced to comply with requests from law enforcement officers for cell phone location information under any alleged emergency circumstance, contrary to a longstanding protection in federal law and current state statute that grants providers discretion to reject data disclosure requests made in situations that are not true emergencies.[6]

The harms posed by removing checks on law enforcement access to cell phone location information are not hypothetical—for example, police in Texas,[7] Maryland,[8] New York,[9] and California[10] have made emergency requests for information when no true emergency existed. Records obtained from police departments by the ACLU have revealed "some departments specifically warn[ing] officers about the past misuse of cell phone surveillance in nonemergency situations."[11] For instance, a law enforcement training document in Reno, Nevada cautioned that warrantless cell phone tracking "IS ONLY AUTHORIZED FOR LIFE THREATENING EMERGENCIES!!" noting that emergency tracking has been "misused" and "continued misuse by law enforcement agencies will undoubtedly backfire."[12]

---

[4] *Carpenter v. United States,* 138 S.Ct. 2206, 2217 (2018).
[5] 18 U.S.C. § 2701 et. seq.; 47 U.S.C. § 222.
[6] 47 U.S.C. § 222 (d).
[7] 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." *State v. Harrison*, No. 02-13-00255-CR at *4–5 (Tex. App. May 30, 2014).
[8] 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." *Upshur v. State,* 56 A.3d 620, 625–26 (Md. App. 2012).
[9] 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. *People v. Moorer*, 959 N.Y.S.2d 868, 872, 875 (N.Y. Co. Ct. 2013).
[10] 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 cell service provider. *Jayne v. Sprint PCS*, No. CIVS072522LKKGGHP, 2009 WL 426117, at *2 (E.D. Cal. Feb. 20, 2009).
[11] Eric Lichtblau, More Demands on Cell Carriers in Surveillance, New York. Times (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html.
[12] Response to ACLU Public Records Request from the Reno, Nevada, Police Department (Aug. 5, 2011), https://www.aclu.org/documents/cell-phone-location-tracking-documents-nevada.

A 2010 investigation by the U.S. Department of Justice Office of Inspector General found systemic misuse of emergency disclosure requests at the hands of federal agencies,[13] such as the FBI repeatedly misusing so-called "exigent letters" and other informal requests to compel production of telephone records and other material.

ACLU-WI Urges the Committee to Adopt Privacy Protections

While ACLU-WI opposes a mandatory emergency disclosure requirement, if this legislation moves forward, we urge the committee to adopt the following protections against abuse of these warrantless information disclosures:

1. **Require after-the-fact judicial review and prompt notice to the person whose location information was obtained.** As currently written, AB-790 does not provide an opportunity for judicial review of emergency requests by law enforcement. In a true emergency when there is no time to obtain a warrant prior to seeking and obtaining location data, a provision requiring law enforcement to seek judicial approval after making the request provides a safeguard against abuse of the emergency requests process. This requirement is included in other states' emergency request statutes, including Indiana,[14] California,[15] and Colorado.[16]

2. **Require judicially enforceable remedies when location information is acquired in violation of the law.** AB-790 should provide a remedy in cases where a 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. A civil remedy could also protect individuals—including those never charged with a crime—by allowing them obtain relief when a judge has determined that law enforcement violated the law.

3. **Require prompt notice to the person whose location information is obtained.** Without notice, a person may never know that police sought and obtained their location information, and cannot pursue judicial remedies in cases where the location tracking request violated the law. Since location disclosure requests should only be made in true emergencies, notifying individuals that their location information was gathered after they are out of harm's way should not have a negative impact.

---

[13] U.S. Dept. 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," (2010), https://www.oversight.gov/sites/default/files/oig-reports/s1001r.pdf.

[14] Ind. Code § 35-33-5-15(b) ("If a law enforcement agency makes a request for geolocation information under this subsection 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.")

[15] 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...")

[16] 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…").

4. **Raise the legal standard governing access to location information to "probable cause" to avoid disclosure of sensitive location information in the absence of a genuine emergency.** As currently written, AB-790 mandates disclosure of location information whenever a law enforcement officer "states" (or "attests" under Assembly Amendment 1) that this data is needed to respond to an emergency situation. 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. This legal standard is familiar to law enforcement and analogous to the standard used when engaging in exigent searches without a warrant.