December 7, 2022

Honorable Chief Justice Tani Cantil-Sakauye
and Associate Justices
Supreme Court of California
350 McAllister Street
San Francisco, CA 94102-4783
Submitted via TrueFiling


Dear Chief Justice Cantil-Sakauye and Associate Justices of the Court,

Pursuant to Rule 8.500(g) of the California Rules of Court, Amici Curiae the American Civil Liberties Union of Northern California and the American Civil Liberties Union of Southern California (collectively, “Amici”) respectfully submit this letter in support of the petition for review filed in Electronic Frontier Foundation v. Superior Court of San Bernardino County, Case Number S277036, on October 25, 2022. We urge the Court to grant petitioner’s request for review.

I. Interests of Amici

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization with more than 2 million members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions and our nation's civil rights law. The ACLU affiliates in California have a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil rights and liberties.

II. Cellphone-based Location Surveillance Poses Grave Threats to Civil Rights.

The cellular phones and other devices we all carry are rich repositories of intimate information, containing, in the words of the U.S. Supreme Court, “the privacies of life.” (Carpenter v. United States (2018) 138 S.Ct. 2206, 2217.) Location information is particularly revealing, potentially exposing a person’s “familial, political, professional, religious, and sexual associations.” (Ibid. [internal quotations omitted].) For cell-site simulators, the risks of
inappropriate intrusion are even more profound. The devices are invisible to the public and inevitably collect information about people with no relationship to the underlying criminal investigation. In 2014, the ACLU of Northern California published a report titled “Stingrays: The Most Common Surveillance Tool the Government Won’t Tell You About,” elaborating on the technology and numerous legal infirmities of cell-site simulators.¹

Wireless cell carriers provide coverage through a network of cell towers, also called cell sites, that connect wireless devices to the terrestrial telephone network.² Cell phones periodically identify themselves to the strongest cell tower they can detect and automatically transmit data that includes the phone’s unique numeric identifier and location information.³ A cell-site simulator masquerades as a wireless carrier’s tower, thereby prompting cell phones to communicate with it as though it were actually the carrier’s tower.⁴ Cell-site simulators are “portable, briefcase-sized devices” and can be carried or mounted on cars or aircrafts.⁵

Cell-site simulators allow law enforcement to reveal a device’s unique identifier if the location is known. They can also reveal the location if the unique identifier is known.⁶ And critically, cell-site simulators gather information, by design, about people who have no relation

---

⁴ See Stephanie K. Pell & Christopher Soghoian, A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities (Fn2), 16 YALE JOURNAL OF LAW & TECHNOLOGY 134, 145–46 (2014); 2015 DOJ Policy, supra note 3, at p. 2 (“In response to the signals emitted by the simulator, cellular devices . . . identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.”).
⁶ See 2015 DOJ Policy, supra note 3, at p. 2; Pell & Soghoian, supra note 4, at p. 147 (“Investigators can position a StingRay in the vicinity of the target to capture the unique serial number of the target’s phone.”); United States v. Artís (9th Cir. 2019) 919 F.3d 1123, 1128 (requiring warrant for use of cell-site simulator to track location of defendant’s cell phone).
to a pending criminal investigation or alleged unlawful conduct. Anyone in the vicinity of the cell-site simulator will likely have information about their device gathered, stored, and analyzed by the simulator, potentially revealing their movements, associations, political and religious affiliations, and even the content of their communications. A cell-site simulator near a doctor’s office could reveal someone’s use of reproductive or otherwise sensitive health care services; a simulator near an apartment building could reveal people’s movements in private spaces, their associations with others, and the details of their daily lives. The inherent invasiveness of cell-site simulators requires rigorous scrutiny by courts. And it demands robust transparency guarantees for the public and policymakers as the democratic process determines how much power the government should have to secretly monitor people as they go about their lives.

III. Transparency is the Foundation of Accountability for Limits on Surveillance Technology and Government Power.

The threats to communities from government surveillance—both from cell-site simulators and other forms of intrusion—are the subjects of active democratic discussion and policymaking at the local, state, and federal level. This discussion requires information, both so people know what is being done by their governments and so policymakers can assess whether laws are properly constraining government power. As Justice Brennan observed, rights of open access have a “structural role to play in securing and fostering our republican system of self-government.” (NBC Subsidiary (KNBC-TV), Inc. v. Superior Court (1999) 20 Cal.4th 1178, 1200-01 [quoting Richmond Newspapers, Inc. v. Virginia (1980) 448 U.S. 555, 587, Brennan, J., concurring].)

Open access rights should take on special importance when our society is actively grappling with policy questions that require access to the challenged information. That is doubtless the case here: California, like the rest of the country, is engaged in an extensive conversation about the impact of surveillance technology on people’s lives, when the government should be allowed to use surveillance technology, and whether certain highly intrusive means of tracking should be allowed at all. Cities and counties around the country

---

7 See Pell & Soghoian, supra note 4, at p. 148; 2015 DOJ Policy, supra note 3, at p.2 (explaining collection from multiple devices in vicinity of simulator); see, e.g., In re the Application of the U.S. for an Ord. Authorizing the Installation & Use of a Pen Reg. & Trap & Trace Device (S.D. Tex. 2012) 890 F.Supp.2d 747, 748 (reviewing application to “detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject]”).

8 See Pell & Soghoian, supra note 4, at p. 146 (noting Stingray can intercept communications content, including calls, text messages, and visited web pages); cf. 2015 DOJ Policy, supra note 3, at p. 2 (explaining DOJ specifically prohibits using cell-site simulators to collect contents of communication).

have passed ordinances mandating transparency, oversight, and accountability measures before surveillance technology can be deployed in communities. These measures underscore the vital role transparency plays in the democratic process as our society decides what limits there should be on surveillance technology.¹⁰

The recent groundswell of activism and legislation in surveillance policy underscores the public’s need to know how the government monitors and tracks people. From restrictions on the use of particular technology (like cell-site simulators and facial recognition) to more expansive limits, the public debate around surveillance requires more—not less—information about the government’s use of technology to gather information about people. That information promises to inform the public about how they are being watched, and it also serves another equally important purpose: allowing the public to ascertain whether law enforcement is complying with laws already on the books.

Cloaking warrant affidavits in secrecy deprives the public and policymakers of the opportunity to assess whether cell-site simulator warrants comply with the United States and California Constitutions. The Constitutional requirement—under both the Fourth Amendment and Article I, Section 13 of the California Constitution—that warrants not be overbroad is a significant legal hurdle for warrants ostensibly authorizing the use of cell-site simulators. “Courts have repeatedly invalidated warrants authorizing a search which exceeded the scope of the probable cause shown in the affidavit.” (In re Grand Jury Subpoenas Dated Dec. 10, 1987 (9th Cir. 1991) 926 F.2d 847, 857.) A warrant is overbroad where the affidavit establishes probable cause to seize some, but not all, materials from the target of an investigation. (See, e.g., United States v. Kow (9th Cir. 1995) 58 F.3d 423, 427–28 [warrant overbroad where it authorized widespread seizure of documents at business even though affidavit contained only probable cause pertaining to profit skimming and tax violations].) A warrant that authorizes the search that a cell-site simulator actually performs—a dragnet collection of all signaling information from a suspect’s wireless device and all other devices in the vicinity of the simulator—would require probable cause to establish that every device in the vicinity of the simulator contains evidence of criminal activity. Only with access to the warrant affidavit can it be ascertained whether a warrant meets this standard in a particular case.

The inalienable privacy right in Article I, Section 1 of the California Constitution also imposes limits on police use of cell-site simulators, both for suspects of criminal investigations and other members of the public, whose devices happen to be in range of the simulator when it is in use. Article I, Section 1 limits invasions of privacy when: (1) people have a legally protected privacy interest; (2) a reasonable expectation of privacy exists under the circumstances (“REP”);

¹⁰ The ACLU maintains a national map identifying the cities that have passed laws regulating the use of surveillance technology. Community Control Over Police Surveillance, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance#map.
and (3) conduct by the defendant constitutes a serious invasion of privacy. *(Hill v. National Collegiate Athletic Association* (1994) 7 Cal.4th 1, 39.) A defendant can prove, as an affirmative defense to an Article I, Section 1 claim, that the invasion of privacy is justified because it substantially furthers one or more countervailing interests. *(Hill, supra, 7 Cal.4th at p. 40.)* These elements depend on the particular facts of the intrusion: where the cell-site simulator was used, what justifications are offered, and whose information was captured by law enforcement. Therefore, without access to the warrant affidavits, people potentially swept up in the cell-site simulator’s dragnet will have no ability to determine whether their constitutional privacy rights have been violated.

The same is true of California statutory law. Signed by the Governor in 2015 as Senate Bill 741 (“SB 741”), Section 53166 of the Government Code requires law enforcement to inform the public, get approval, and publish a “use policy” before using cell-site simulators. As the author of the bill wrote, “[r]esidents should be made aware of what type of surveillance technology law enforcement agencies use within their community. Residents should also be able to participate in a public process to decide whether or not those surveillance technologies should be used in their communities and if adopted, how the technology should be used.”¹1 The use policies promulgated as a result of SB 741 impose important limits on how cell-site simulators can be used and what evidence is necessary for the government to provide to judges in order to deploy one. The policies for Alameda and Los Angeles counties, for example, require that the affidavit include an explanation of the technology, impact on other devices, and a plan to delete non-relevant information.¹² And the San Bernardino policy requires that warrant affidavits describe the purpose and activities for which an order is sought, and how the technology functions.¹³ Without access to the underlying affidavits, the public will have no ability to determine whether SB 741 is being complied with in individual cases.

Similarly, the California Electronic Communications Privacy Act (“CalECPA”), set forth at Penal Code sections 1546-1546.5 and also passed in 2015, requires a probable-cause warrant whenever law enforcement accesses information from a person’s device through electronic communication with the device, as a cell-site simulator does.¹⁴ CalECPA enjoyed widespread support from civil rights organizations and business interests, and moved to update California law to take modern threats to electronic privacy into account.¹⁵ The warrants required by

---


¹⁴ See Cal. Penal Code, § 1546.1, subd. (a)(3) (prohibiting accessing device information by means of electronic communication with electronic device, as cell-site simulators do, without a warrant or other legal process).

CalECPA must be narrowly particularized to identify, as appropriate and reasonable, “the target individuals or accounts, the applications or services covered, and the types of information sought.” (Id., § 1546.1, subd. (d)(1).) The probable cause laid out in the warrant affidavit must justify the particular search into the people, applications or services, and information sought.\(^{16}\)

Again, only with access to the warrant affidavits can the public meaningfully determine whether CalECPA’s strictures are being complied with.

IV. Article 1, Section 3 of the California Constitution Requires That This Court Reassess Pre-2004 Public Transparency Law, Including \textit{Hobbs}.

In 2004, over 82\% of voters chose to include a right of access in the California Constitution.\(^{17}\) By making “transparency a constitutional duty owed to the people,” Article I, Section 3(b) requires government entities to demonstrate “why information requested by the public should be kept private.” (Id.)\(^{18}\) The amendment requires that courts broadly construe law that furthers the right of access and narrowly construe law that limits this right. (Cal. Const., art. I, § 3, subd. (b), par. (2).) The constitutional amendment does not “repeal or nullify . . . any constitutional or statutory exception to the right of access.” (id., § 3, subd. (b), par. (5)). Nonetheless, courts should still construe those statutory exceptions narrowly. (See \textit{Sierra Club v. Superior Court} (2013) 57 Cal.4th 157, 166.)

In 1994, \textit{People v. Hobbs} created an exception to Penal Code section 1534, subdivision (a), which made executed warrants available to the public ten days after issuance. (\textit{People v. Hobbs} (1994) 7 Cal.4th 948, 962.) The Hobbs Court relied on the privilege articulated in Evidence Code section 1041 against disclosing informer identities if doing so would be against the public interest, and a corollary rule that extended the privilege to contents of informant statements if it would “tend to disclose the identity of the informer.” (Id. at pp. 1251–52.) In this case, the appeals court interpreted \textit{Hobbs} and Evidence Code section 1041 broadly, finding that Hobbs affidavits were beyond the scope of the constitutional access provision. (\textit{Electronic Frontier Foundation, Inc. v. Superior Court} (2022) 83 Cal.App.5th 407, 430.).

The appeals court’s broad interpretation of \textit{Hobbs} privilege conflicts with the court’s constitutional obligation to narrowly construe laws that limit the right of access. Evidence Code section 1041 requires a court to balance the public interest, considering both interests in informant confidentiality, the necessity of disclosure, and the interests of justice. (See Evid.

\(^{16}\) See Penal Code, § 1525 (“A search warrant cannot be issued but upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing, or things and the place to be searched.”); id., § 1527 (“The affidavit or affidavits must set forth the facts tending to establish the grounds of the application, or probable cause for believing that they exist.”); see also, e.g., \textit{People v. Frank} (1985) 38 Cal.3d 711 (invalidating portion of warrant where affidavit lacked probable cause); \textit{Matter of Residence in Oakland, California} (N.D. Cal. 2019) 354 F. Supp. 3d 1010, 1014 (holding the same where no probable cause to compel individuals to unlock seized devices); \textit{United States v. Spilotro}, 800 F.2d 959, 963–65 (9th Cir. 1986) (holding the same for jewels included in scope of warrant but not supported by probable cause).

\(^{17}\) Debra Bowen, Secretary of State, Official Voter Information Guide 16 (2014), https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2327&context=ca_ballot_props.
Code, § 1041, subd. (a)(2).) How courts strike that balance was transformed in 2004 when the voters added Article I, Section 3(b)(2) to the Constitution, which commands that a “statute, court rule, or other authority, including those in effect on the effective date of this subdivision, shall be broadly construed if it furthers the people’s right of access, and narrowly construed if it limits the right of access.” (Cal. Const., art. § 3, subd. (b), par. (2) [emphasis added].) This Court should construe the informant privilege in Evidence Code section 1041 narrowly, as the California Constitution commands.

This change to public transparency law was an explicit goal of the constitutional right of access. The 2004 Official Voter Guide emphasized that the amendment would “result in additional government documents being available to the public,” and that courts would eventually “limit or eliminate laws that don’t clear [the high] hurdle.”18

V. Public Warrant Affidavits Hold Some Promise of Accountability When Police Are Dishonest.

Public warrant affidavits are important for accountability because it is known that police officers lie in written statements, search-warrant hearings, suppression hearings, and trials.19 Former San Francisco police commissioner Peter Keane described police officer perjury as the “routine way of doing business in courtrooms everywhere in America.”20 In search-warrant hearings specifically, police have lied about what informants told them and even whether an informant exists.21 In interviews with lawyers, police officers, and judges, The New York Times identified more than twenty-five cases between 2015 and 2018 in which New York Police Department (NYPD) officers lied in a key part of their testimony.22 Because when a police officer lies, the case is often sealed, the actual number is likely significantly higher. (Id.)

Those lies often have serious consequences for people. In 2016, Xochitl Hernandez was detained for six months, then designated for deportation because a Los Angeles Police Department officer testified, without substantiating evidence, that Ms. Hernandez was affiliated with a gang.23 In 2017, Kimberly Thomas spent more than a year fighting gun charges after a

---

21 Dunkle, supra note 19, at pp. 2062–63.
New York Police Department officer alleged that she was carrying a laundry bag with a gun in her apartment hallway. Thomas’s lawyer ultimately obtained security footage that showed Thomas had no laundry bag or gun at the time. (Id.) While prosecutors dropped the case, the court sealed the case file. (Id.)

The search-warrant affidavits supporting dragnet surveillance technology should be public because they serve as an important check on government power and police lies. First, a policy of transparency can be expected to serve some deterrent effect, as awareness that these affidavits will be subject to public scrutiny may rein in the worst abuses or increase the likelihood that offending officers will be sanctioned. Second, public access will advance individual justice since defendants themselves often cannot access these affidavits in order to challenge them. (See Hobbs, supra, 7 Cal.4th at p. 972–73 [adopting in-camera process that excludes defendants to review sealed affidavits for validity].) Transparency promotes systemic reform; public awareness of police practices, including misconduct and dishonesty, is necessary to identify and implement needed regulations and changes in policy. But none of these is possible if the underlying affidavits are enshrouded in secrecy. To the contrary, that outcome would incentivize and insulate the worst practices, with great cost to justice in individual cases and to police–community relations as a whole.

---

24 Goldstein, supra note 22.
VI. Conclusion

The Court should grant the petition for review.

Dated: December 7, 2022

Respectfully submitted,

/s/Jacob A. Snow

Jacob A. Snow
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Counsel for Amici Curiae

/s/Mohammad Tajsar

Mohammad Tajsar
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN CALIFORNIA
Counsel for Amici Curiae

cc: All Counsel
    Honorable Manuel A. Ramirez
    Honorable Dwight W. Moore
PROOF OF SERVICE

I, Jacob Snow, declare that I am over the age of eighteen and not a party to the above action. My business address is 39 Drumm Street, San Francisco, California 94111. My electronic service address is jsnow@aclunc.org. On December 7, 2022, I caused the foregoing document to be served:


Declaration of Jacob Snow

BY ELECTRONIC TRANSMISSION: I caused to be transmitted to the following case participants a true electronic copy of the document via this Court’s TrueFiling system:

**Michael Temple Risher**  
San Bernardino County District Attorney's Office  
Law Office of Michael T. Risher  
2081 Center St # 154  
Berkeley, CA 94704-1204  
Email: Michael@risherlaw.com

**Mark Vos**  
Office of The District Attorney  
Appellate Services Unit  
303 West Third Street, 5th Floor  
San Bernardino, CA 92415  
Email: mvos@sbcda.org

**David Edward Snyder**  
First Amendment Coalition  
534 Fourth Street, Suite B  
San Rafael, CA 94901  
Email: dsnyder@firstamendmentcoalition.org

**Miles Abernathy Kowalski**  
Office of County Counsel  
385 N Arrowhead Avenue  
San Bernardino, CA 92415  
Email: miles.kowalski@cc.sbcounty.gov

**Katielynn Boyd Townsend**  
Reporters Committee for Freedom of the Press  
1156 15th St NW Ste 1020  
Washington, DC 20005-1754  
Email: ktownsend@rcfp.org

**Aaron David Mackey**  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109-7701  
Email: amackey@eff.org

**Aaron R. Field**  
Cannata, O’Toole, Fickes & Olson LLP  
100 Pine Street, Suite 350  
San Francisco, CA 94111  
afield@cofolaw.com
BY MAIL: I mailed a copy of the document identified above by depositing the sealed envelope with the U.S. Postal Service, with the postage fully prepaid.

Honorable Manuel A. Ramirez
Presiding Justice
Court of Appeal, Fourth Appellate District
Division 2
3389 Twelfth Street
Riverside, CA 92501

Honorable Dwight W. Moore
Supervising Justice
Superior Court of California
County of San Bernardino
San Bernardino District
247 West Third Street
San Bernardino, CA 92415-0210

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on December 7, 2022 in San Francisco, CA.

/s/ Jacob Snow