ACLU Northern California ACLU Southern California ACLU

June 1, 2023

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

RE: Letter of Amici Curiae in Support of Petition for Review in *People v. Meza*, Supreme Court Case No. S280089 (Court of Appeal, Second Appellate District, Case No. B318310).

Dear Chief Justice Guerrero and Associate Justices of the Court,

The undersigned Amici urge the Court to grant petitioner's request for review in this matter. The court below concluded that the warrant in question violated the Fourth Amendment to the U.S. Constitution, calling the constitutional question "not a particularly close" one. But the court refused to suppress the evidence, first because it misinterpreted the California Electronic Communications Privacy Act ("CalECPA") by reading core protections—including the requirements that CalECPA warrants comply with federal law and also include heightened particularity—out of existence. Next, the court wrongly concluded that the good-faith exception to the exclusionary rule under the Fourth Amendment applied, with reasoning that would allow law enforcement using novel surveillance technology to violate people's rights with impunity. Recent history shows that encouraging honesty and candor by law enforcement is vital when officers use novel technology, and the ruling below would impede these important incentives.

These serious errors led the court to deny suppression of evidence gathered from a geofence warrant covering six locations in Los Angeles, California. Geofence warrants are a surveillance technique that law enforcement uses to comb through millions of people's location history records in order to identify people near a geographic area during a period of time. In this case, the geofence locations were both residential and commercial, and each of the six areas was approximately the size of a city block. The warrant likely swept in a large number of people going about their daily lives with no connection to the crime under investigation. During the five morning hours covered by the warrant, many people would have moved through these six areas, driving to work and school, going to stores, and perhaps traveling to doctors' offices and places of worship. To respond to the warrant, Google not only had to search the places covered by the

geofence warrant, but to search through the personal, private records of millions of Google users to identify which of them was near a given area.

As explained below, the warrant failed to comply with CalECPA and the Fourth Amendment, and the good-faith exception should not apply. These legal errors justify granting the petition for review. And beyond this case, the legal status of geofence warrants under the Fourth Amendment and CalECPA needs urgent attention from this Court. Every year, Google receives thousands of geofence warrants. And law enforcement use of these warrants is increasing significantly: in 2018 Google received 982 geofence warrants; in 2020 it received over ten times that: 11,554 warrants.[1] In fact, California law enforcement seeks more geofence warrants than any other state, and even more than the federal government does. In 2020 alone California law enforcement sent Google over 1,900 geofence warrants.[2]

The privacy rights of thousands of people accused of crimes, and many millions more whose personal information is searched whenever a geofence warrant is executed, depend on this Court's guidance. That guidance is particularly necessary here because CalECPA only took effect in 2016, so neither this Court nor any other courts of appeal have had occasion to interpret it in a published opinion. As a result, the error of the Court of Appeal's decision, which threatens to gut core protections in CalECPA, is binding on all Superior Courts in California. (*Auto Equity Sales, Inc. v. Superior Ct. of Santa Clara Cnty.* (1962) 57 Cal.2d 450, 455.)

Pursuant to Rule 8.500(g) of the California Rules of Court, Amici Curiae the American Civil Liberties Union, 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 *People v. Meza,* Supreme Court Case No. S280089 (Court of Appeal, Second Appellate District, Case No. B318310) on May 22, 2023.

I. Interests of Amici

The American Civil Liberties Union ("ACLU") is a national, non-profit, non-partisan civil liberties organization dedicated to the principles of liberty and equality embodied in both the United States and California constitutions and our nation's civil rights law. Amici are the ACLU, the ACLU of Northern California, and the ACLU of Southern California. 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.

Amici supported the passage of CalECPA and served as key advisors to the law's authors, Senators Mark Leno and Joel Anderson, throughout the legislative process.

[1] See *Supplemental Information on Geofence Warrants in the United States, Google*, *available at* https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (calculation performed by adding up the warrants received by each state and the federal government for the years 2018 and 2020 in the supplemental spreadsheet).

[2] *Id.* (Google's supplementary spreadsheet includes warrant counts broken out by state).

Accordingly, Amici are uniquely positioned to provide the Court with a comprehensive perspective on the purpose and meaning of CalECPA's provisions.

II. CalECPA provides stronger protections than the Fourth Amendment and Article I, Section 13 of the California Constitution do.

California has a long tradition of providing stronger privacy protections than federal law, and CalECPA continues that tradition. The California Constitution guarantees an inalienable right to privacy for all Californians, articulated in The Privacy Amendment to Article I, Section 1, which protects the privacy rights of "all people." The Privacy Amendment was passed in response to the "modern threat to personal privacy" posed by increased surveillance and then-emerging data collection technology. (*White v. Davis* (1975) 13 Cal.3d 757, 774.) Article I, Section 1 also added an explicit right to privacy independent of the federal Constitution, protecting people's reproductive and bodily autonomy, in the state's constitution. (*Comm. To Defend Reproductive Rights v. Myers* (1981) 29 Cal.3d 252, 262.)

CalECPA, passed in 2015, built on the foundation of the California Constitution by establishing clear rules to protect Californians' privacy rights when a government entity seeks electronic information from a third-party service provider. CalECPA had two core purposes: first, to statutorily codify and create clear mechanisms to safeguard and enforce existing privacy rights governing electronic information in the digital age; and second, to provide new protections for electronic information, going beyond existing statutory and constitutional protections. (Assem. Com. on Privacy and Consumer Protection, Rep. on Sen. Bill No. 178 (2015–2016 Reg. Sess.) Jun. 23, 2015, p. 5.) ("This bill is intended to both codify and expand on existing" protections for electronic information).[3]

Three specific aspects of CalECPA are relevant here:

Particularity. CalECPA directs how specific a warrant must be in describing what the government has the power to seize. Warrants must "describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought." (Pen. Code, § 1546.1, subd. (d)(1).) These enumerated particularity requirements are *more specific*—and *more extensive*—than those imposed by the Fourth Amendment or the California Constitution. CalECPA specifically includes heightened particularity requirements to protect against improper government access to the vast amounts of personal information collected and retained by online services. Warrants that permit the search of an online service

[3] *Available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178#; see also Sen. Com. on Pub. Safety, Rep. on Bill No. SB 178 (2015–2016 Reg. Sess.) Mar. 23, 2015, p. 8 ("[CalECPA] updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information."), *available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178#.

threaten to intrude upon the privacy of not just one person, but potentially many (or even all) people that use an online service. CalECPA recognizes that, to effectively protect privacy, the law must narrowly constrain the reach of the government's power to intrude into our digital spaces.

Compliance with federal law. CalECPA has clear language requiring that "the warrant comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants." (Pen. Code, § 1546.1, subd. (d)(3).) This certainly includes the Fourth Amendment to the U.S. Constitution and Article I, Section 13 of the California Constitution. *Id.*

Suppression. CalECPA provides for suppression when "any electronic information [is] obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter [CalECPA]." (Pen. Code, § 1546.4, subd. (a).) Any California law requiring suppression of evidence requires a two-thirds majority vote in both chambers of the California legislature.[4] CalECPA surmounted this formidable threshold, and the suppression requirement is the cornerstone of the enforcement mechanism of this important privacy law. Where any provision of CalECPA has been violated—including that the warrant failed to comply with all other provisions of California and federal law—suppression is required.

III. Geofence warrants to Google do not target individual accounts as CalECPA requires.

Geofence warrants allow law enforcement to search through location records of millions of people to identify individuals who were near a geographic area during a given time frame. These warrants are not targeted to specific individuals or accounts; instead, in order to comply, providers must search their entire database of stored location information to find all users or devices near the geographic and time parameters of the warrant. Google's location database contains information about hundreds of millions of devices, going back a decade or more.[5] And for each geofence warrant, Google must search this entire location history database—encompassing the personal information of millions of people.[6]

It is critical to understand that Google must search the records of every Google user in order to comply with a geofence warrant. This means that anyone with a Google account—including members of this Court—may have their location records searched when Google

[4] Cal. Const., art. I, § 28, subd. (f)(2).
[5] Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.
[6] Brief of Amicus Curiae Google LLC in Support of Neither Party, filed December 20, 2019 in *United States v. Chatrie* (E.D.Va. 2019, No. 3:19-cr-00130-MHL) ("Google Amicus Brief"), at p. 11–12 ("[L]aw enforcement uses geofence requests in an attempt to identify all Google users who might have stored [location history] data in their accounts suggesting that they were near a given area in a given timeframe—and to do so at a level of precision not available through CSLI or similar data.""); *id*. at 14 ("Google has no way to identify which of its users were present in an area of interest without searching the [location history] information stored by every Google user who has chosen to store that information with Google.").

responds to a geofence warrant.[7] And those location records, just like emails, notes, messages, and documents, are the account-holder's personal files, not Google's business records.[8]

Geofence warrants, then, are not just a search of the places traced by the geographic boundaries they describe. They are also, in this case, a search through the personal location records of millions of people, as the warrant commands that Google search those personal records for information reflecting coordinates within a particular geographic area.

The digital nature of the search should not suggest that it is any less of a concern than physical ones. The general warrants in *Stanford v. Texas* (1965) *379 U.S. 476* (where a house was ransacked looking for Communist Party records) and *Wilkes v. Wood* (K.B. 1763) 98 Eng.Rep. 489, 490 (where houses were raided looking for unspecified people suspected of libel), involved agents of the state entering and rummaging through people's homes and files. In the digital realm an equivalent search can be instantaneous, invisible to the people searched, and performed at an immense scale. These factors make digital searches *more*—not less—invasive than the physical searches that motivated the Fourth Amendment and Article I, Section 13 of the California Constitution.

IV. The Geofence warrant in this case violated CalECPA.

The Court of Appeal's interpretation of CalECPA threatens to read core protections in the law out of existence. The court failed to properly take into account the text of the law, the legislative purpose, and the broader statutory scheme. *First*, the court flatly disregarded the plain text of the statute to conclude that violations of the Fourth Amendment do not constitute a violation of CalECPA, thereby eliminating CalECPA's explicit provision of a suppression remedy when Californian's Fourth Amendment rights are violated.

Second, read correctly, CalECPA requires that geofence warrants be particularized to the target individuals or accounts. The warrant at issue in this case targeted every account, and thus was not sufficiently particularized. It therefore violated CalECPA.

If allowed to stand as authoritative interpretations of CalECPA, the appellate court's errors would eviscerate the statute—which was explicitly intended to expand protections for privacy in the digital age and modernize California electronic surveillance law. CalECPA's protections, importantly, are not subject to a "good-faith" exception under California law;[9] therefore, when the statute is violated, suppression is required.

---

[7] Google Amicus Brief at 4 ("[T]he steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.").

[8] *See id*. at pp. 6–9.

[9] As Professor Freiwald noted, CalECPA's "state procedures do not incorporate the expansive exceptions that courts have used to deny suppression remedies in Fourth Amendment cases under the doctrine of good faith." (*Freiwald*, 33 Berkeley Tech. L.J. 131, 161, fn. omitted.) Judicially created exceptions to suppression under the Fourth Amendment do not apply to CalECPA's statutory suppression remedy. (See *People v. Jackson* (2005) 129 Cal.App.4th 129, 153–160.)

A. Under the law of statutory construction in California, a Fourth Amendment violation is a CalECPA violation.

CalECPA must be construed according to this Court's precedent on statutory construction. When construing statutes, the goal is "to ascertain the intent of the enacting legislative body so that we may adopt the construction that best effectuates the purpose of the law." (*City of Santa Monica v. Gonzalez* (2008) 43 Cal.4th 905, 919 [internal quotations omitted].) Statutory construction begins with "the plain, commonsense meaning of the language used by the Legislature. If the language is unambiguous, the plain meaning controls." (*Voices of the Wetlands v. State Water Resources Control Bd.* (2011) 52 Cal.4th 499, 519.) The actual words of the statute are considered first because "the statutory language is generally the most reliable indicator of legislative intent." (*People v. King* (2006) 38 Cal.4th 617, 622.) And critically, each word of the statute should be given significance in "pursuing the legislative purpose, and the court should avoid a construction that makes some words surplusage." (*Agnew v. State Bd. of Equalization* (1999) 21 Cal.4th 310, 330.)

If the statutory language may reasonably be given more than one interpretation, "courts may consider various extrinsic aids, including the purpose of the statute, the evils to be remedied, the legislative history, public policy, and the statutory scheme encompassing the statute." (*People v. King, supra*, 38 Cal.4th at p. 622.)

Turning to CalECPA, the statute operates by *prohibiting*—"except as provided in this section"—governmental entities from compelling the production of or access to electronic information from service providers. (Pen. Code § 1546.1, subd. (a)(1).) The section then goes on to enumerate the various ways in which governmental entities can compel production of electronic information, including by getting a warrant. (Pen. Code § 1546.1, subds. (b)(1), & (c)(1).) In addition to other requirements that apply to warrants, CalECPA adds three criteria that warrants for electronic information must satisfy: 1) new particularity mandates; 2) sealing and prohibition on further use; and 3) compliance with California and federal law, specifically law governing search warrants. (Pen. Code § 1546.1. subds. (d)(1), (d)(2), & (d)(3).) Without satisfying all three of these criteria, the warrant does not comply with CalECPA and cannot be the basis for compelling production of or access to electronic information.

Axiomatically, the Fourth Amendment prohibits, limits, and imposes requirements on the use of search warrants. (U.S. Const., 4th Amend. ["no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"].) Indeed, in this very case the Court of Appeal correctly concluded that the search warrant in question was overbroad and inadequately particularized in violation of the Fourth Amendment.

A warrant that does not comply with the Fourth Amendment cannot satisfy the requirements of Penal Code Section 1546.1, subdivision (d)(3). The fact that the requirements of the Fourth Amendment were incorporated into CalECPA is also evident from the statute's

remedies. Penal Code Section 1546.4, subdivision (a) provides that "[a]ny person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of *the Fourth Amendment* to the United States Constitution or of this chapter." (emphasis added).

Despite these unambiguous commands, the Court of Appeal erroneously held that a violation of the Fourth Amendment did not constitute a violation of CalECPA. *People v. Meza*, (Certified for Publication April 13, 2023), Second Appellate District, Civ. No. B318310 ("Court of Appeal's Opinion"), at 36. The court wrote that Penal Code Section 1546.1, subdivision (d)(3) and Section 1546.4, subdivision (a) "do nothing more than expressly preserve an individual's existing rights under the federal Constitution. There is nothing in the cited language that, without more, converts a Fourth Amendment violation into a statutory violation." *Id.*

It is not clear what "more" the Court of Appeal would demand in order to incorporate Fourth Amendment protections into a statutory framework. CalECPA states, clearly and explicitly, that warrants "shall comply with all other provisions of California and federal law," such that a violation of federal law governing search warrants—which the Fourth Amendment certainly is—represents a violation of CalECPA's warrant requirement. (Pen. Code § 1546.1, subd. (d)(3).) Further, the Court of Appeal's interpretation that the statute's language merely serves to "preserve an individual's existing rights under the federal Constitution" makes little sense: the federal Constitution is supreme, and it is not legally possible for state law to disrupt the federal Constitution. (U.S. Const., Art. VI, Clause 2 ["This Constitution . . . shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any thing in the Constitution or Laws of any State to the Contrary notwithstanding"].)

The Court of Appeal's reasoning would therefore have the effect of disregarding entire paragraphs and clauses of CalECPA and reducing them to a nullity. "In the construction of a statute or instrument, the office of the judge is simply to ascertain and declare what is in terms or in substance contained therein, not to insert what has been omitted, or to omit what has been inserted." (*Manufacturers Life Ins. Co. v. Superior Court* (1995) 10 Cal.4th 257, 274 [finding that the plain language and history of the UIPA did not suggest legislative intent to abolish the Cartwright Act or UCA remedies].)

Here the legislature *did* intend that violations of federal law (and in particular the Fourth Amendment) violate CalECPA, and it *did* say so. The court below properly held that the warrant in this case violated the Fourth Amendment. This Court should grant review to correct the Court of Appeal's decision to omit what the legislature carefully inserted.

B. The geofence warrant in this case failed to comply with CalECPA's particularity requirement.

CalECPA requires that all warrants satisfy stringent particularity requirements. These requirements limit the scope of electronic information law enforcement can obtain through a warrant. (Pen. Code § 1546.1, subd. (d)(1).) Thus, a warrant must specify, as "appropriate and

reasonable" "the time periods covered" by the warrant, the "target individuals or accounts, the applications or services covered, and the types of information sought." *Id.*

These particularity requirements should be understood in the context of the Fourth Amendment's requirements. Under the Fourth Amendment, warrants must particularly describe the things to be searched and seized. Particularity requires the warrant to state those limits clearly, to cabin an officer's discretion in conducting the search. And the Fourth Amendment recognizes that "[t]he modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." (*United States v. Otero* (10th Cir. 2009) 563 F.3d 1127, 1132 [collecting cases]; *United States v. Galpin*, (2d Cir. 2013) 720 F.3d 436 at 446; see also *Berger v. New York* (1967) 388 U.S. 41, 56 ["The need for particularity . . . is especially great" where the method of surveillance "involves an intrusion on privacy that is broad in scope"].) The particularity requirement is especially important when the information is stored in such a way as to implicate the privacy interests of numerous people.[10]

CalECPA's particularity requirements represent a statutory embodiment of these concerns. Indeed, CalECPA's legislative history demonstrates CalECPA's core concern that evolving technologies leave privacy unprotected by storing many users' information in the same central service, making them a target for overbroad searches.[11] The legislature also considered Google's statement in support that "[u]sers expect, as they should, that the documents they store online have the same Fourth Amendment protections as they do when the government wants to enter the home to seize documents stored in a desk drawer. There is no compelling policy or legal rationale for this dichotomy."[12] CalECPA was foundationally concerned with ensuring strong protections for information, no matter whether it was stored in a cloud service or in hard copy in a person's home.[13] In the words of the author, "Californians should not have to choose between using new technology and keeping their personal lives private."[14]

---

[10] See *Wilkes, supra,* 98 Eng.Rep. at p. 490 (breaking into multiple houses "without name of the person charged" "touched the liberty of every subject of this country"); see also *In re Warrant Application for Use of Canvassing Cell-Site Simulator* (N.D. Ill., Feb. 1, 2023, No. 22 M 00595) 2023 WL 1878636, at *20 (denying an application for a warrant to use canvassing cell-site simulator technology, finding that "the warrant…would enable the government to obtain and use data associated with possibly thousands…of uninvolved cellular users" and that "the Fourth Amendment's particularity and overbreadth requirements constrain the government from obtaining a warrant to search an entire neighborhood's hundreds of haystacks in search of a single needle.")

[11] See Assem. Com. On Public Safety, Analysis of SB 178, (2014–2015 Reg. Sess.) July 14, 2015, p. 6. (Author's statement explaining the purpose of the bill, and noting that "the emergence of new technology has left California's statutory protections behind, and currently, a handwritten letter in a citizen's mailbox enjoys more robust protection from warrantless surveillance than an email in someone's inbox. This is nonsensical, and SB 178, the California Electronic Communications Privacy Act (CalECPA) will restore needed protection against warrantless government access to mobile devices, email, text messages, digital documents, metadata, and location information.").

[12] *Id*. at 10.

[13] See *id*. at 9 (noting that CalECPA "addresses . . . privacy concerns" posed by "'cloud computing'" arising out of the fact that "the data viewed may not in fact be stored on the device itself.").

[14] *Id.* at 8.

The statute's central mandate directs that government entities get a warrant before they "compel the production of or access to electronic communication information from a service provider." (Pen. Code § 1546.1, subd. (a)(1).) "Service providers" under CalECPA are entities that "provide[] to its subscribers or users" the ability to send, receive, or store electronic communication information. (Pen. Code § 1546, subds. (e), (j).) Service providers, therefore, have the potential to store the personal information of enormous numbers of people—indeed, for the largest service providers today, whose users number in the billions, those personal information stores represent a significant fraction of the Earth's population.[15]

The privacy risks associated with service providers—operating at massive scale—motivated CalECPA's carefully chosen limits on search warrants to these entities. That is, warrants should be specific and particular with respect to time, individuals targeted, types of information sought, and services or applications reached. These constraints reflect a legislative judgment that grave privacy intrusions are enabled by expansive temporal boundaries, dragnet searches covering numerous individuals, and searches that span multiple services or applications. See Susan Freiwald, *CalECPA: At the Privacy Vanguard,* 33 Berkeley Tech. L.J. 131, 133 (2018) (noting that searches lacking CalECPA's particularity limits "can end up gathering so much information that they risk being fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment.").[16]

In light of CalECPA's purpose, the warrant here is inadequately particular with respect to "target individuals or accounts." The geofence warrant covered a large area at a busy time of day, such that the warrant commanded a search through the cell-phone location information of many people. The warrant covered typical early to mid-morning commuting hours for a total of five hours and reached six city-block sized areas in both neighborhoods and commercial areas, covering numerous stores, gas stations, banks, and a medical center.

And beyond the places covered by the geofence warrant, executing the warrant required Google to search the personal, private records of many millions of people. This reality—that modern software service providers store the records of millions in centralized databases—motivated the inclusion of CalECPA's requirement that warrants be particularized specifically to target individuals or accounts, with the goal that people not sacrifice their privacy by merely going about their lives in the digital age.

---

[15] See Cranz, *There are over 3 billion active Android devices*, The Verge (2021), https://www.theverge.com/2021/5/18/22440813/android-devices-active-number-smartphones-google-2021 (last visited May 15, 2023); Rodriguez, *Instagram surpasses 2 billion monthly users while powering through a year of turmoil*, CNBC (2021), https://www.cnbc.com/2021/12/14/instagram-surpasses-2-billion-monthly-users.html (last visited May 15, 2023).

[16] Professor Freiwald served as "an issue expert for CalECPA's authors, State Senators Mark Leno and Joel Anderson, and as a member of the bill's policy and language teams. In that capacity, [she] helped answer questions about the bill's language, testified at legislative committee hearings about its legal impact, and coordinated dozens of academic colleagues to send a scholarly support letter to California Governor Jerry Brown." *CalECPA: At the Privacy Vanguard,* 131 n. d1.

The geofence warrant here, therefore, was therefore not limited as "appropriate and reasonable" to the individuals or accounts likely to be reached by its expansive scope. The warrant violated CalECPA and the evidence should be suppressed.

V. The good-faith exception to suppression under the Fourth Amendment does not apply.

Amici agree with the Court of Appeal's that the warrants here violate the Fourth Amendment, but urge this Court to grant the petition to correct the Court of Appeal's analysis holding that the good-faith exception applies such that the evidence obtained should not be suppressed. Contrary to the Court of Appeal's analysis, it was objectively unreasonable to rely on a warrant when the Fourth Amendment deficiency was, in the Court of Appeal's own words "not a particularly close" issue. Court of Appeal's Opinion at 33.

Despite finding that a violation occurred, the Court of Appeal concluded that the good-faith exception applied "given the dearth of authority directly on point and the novelty of the particular surveillance technique at issue." *Id.* at 32–33. This is backwards. When surveillance technology is new, law enforcement should carefully understand the technology and present the new application clearly and honestly to the magistrate. Suppression is necessary to incentivize caution and candor, *especially* when law enforcement seeks authorization to use novel surveillance techniques.

For an officer's reliance on the magistrate's determination to be objectively reasonable, the officer must have supplied the magistrate with information "sufficient for a judge to exercise his independent judgment on issuing a search warrant." (*United States v. Tate* (4th Cir. 2008) 524 F.3d 449, 457.) Warrant proceedings, which are conducted *ex parte*, demand a heightened duty of candor from police, because there is no adversarial process to bring omitted facts, inaccurate statements, or countervailing legal arguments to the magistrate's attention. (See *Franks v. Delaware* (1978) 438 U.S. 154, 169; *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC* (FISA Ct. 2019) 411 F. Supp. 3d 333, 336 [observing that the government has a "heightened duty of candor . . . in *ex parte* proceedings . . . such as proceedings on electronic surveillance applications"] [quotation marks omitted].) This ever-present need for candor is especially acute when law enforcement seeks to use novel and complex technologies that have rarely been the subject of judicial review. Yet when police seek to use novel surveillance techniques, they often fail to provide the magistrate with sufficient information to ensure the search meets the Fourth Amendment's requirements.

For example, for many years, law enforcement agents and prosecutors sought authority to use cell site simulators (police-operated devices that mimic cell phone towers and can be used to locate phones) by submitting applications that camouflaged this technology—often by completely omitting its novel capabilities and Fourth Amendment implications. (See *Andrews v. Balt. City Police Dep't* (4th Cir. 2020) 8 F.4th 234, 235.) In Tacoma, Washington, for example, a press investigation revealed that police had used a cell site simulator more than 170 times over

five years but had concealed their intent to do so from judges, who then authorized the surveillance without a search warrant.[17] In Charlotte, North Carolina, a similar investigation revealed that police had been deploying cell site simulators for eight years pursuant to pen register orders, not warrants, without disclosing that fact to courts.[18] After—and only after—such cases came to light, legislatures and courts began to expressly direct police to include full explanations of the technology. As a result, law enforcement now must obtain a warrant based on probable cause, and not a lesser pen register or other court order, before using a cell site simulator. Further, the more honest disclosures in warrant applications enable magistrate judges to adequately assess whether to issue warrants and what limitations to place on them. (See, e.g., 725 Ill. Comp. Stat. 137/15; Wash. Rev. Code § 9.73.260; *In re Application of the U.S. for an Ord. Relating to Tels. Used by Suppressed*, (N.D. Ill., Nov. 9, 2015, No. 15 M 0021), 2015 WL 6871289.)

These examples underscore the need to require candor when the government is applying to use novel surveillance techniques that pose significant threats to privacy. The exclusionary rule is necessary to counter the incentives for police to withhold information from courts about how those tools are being deployed. If it is considered "objectively reasonable" for an officer to rely on a warrant issued for novel technology in the absence of constitutional authority (in the Court of Appeal's words) "directly on point," then police will continue to experiment with novel, powerful, and potentially unlawful forms of surveillance, while shrouding their operations in secrecy.[19]

//

//

//

//

//

//

//

//

//

//

[17] Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune (Nov. 15, 2014), https://www.thenewstribune.com/news/local/crime/article25894096.html.
[18] Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer (Nov. 25, 2014), https://www.wbtv.com/story/27473706/cmpds-cellphone-tracking-cracked-high-profile-cases/.
[19] Pell & 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* (2013) 16 Yale J.L. & Tech. 134.

VI. Conclusion

This Court should grant the petition for review.

Dated: June 1, 2023

Respectfully submitted,

/s/*Jacob A. Snow*

Jacob A. Snow
Nicole A. Ozer
Nicolas A. Hidalgo
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

/s/ Jennifer Granick

Jennifer Granick
AMERICAN CIVIL LIBERTIES UNION
Counsel for Amici Curiae

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 June 1, 2023, I caused the foregoing document to be served:

RE: Letter of Amici Curiae in Support of Petition for Review in *People v. Meza*, Supreme Court Case No. S280089 (Court of Appeal, Second Appellate District, Case No. B318310).

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:

Bess Louise Stiffelman 505 S. Flower St. #71892 Los Angeles, CA 90071 *Counsel for Defendant-Appellant Walter Meneses*	**Michael C. Keller** Office of the Attorney General 300 S. Spring St., Suite 1702 Los Angeles, CA 90013 *Counsel for Plaintiff and Respondent the People of California*
Sharon Fleming P.O. Box 803 Ben Lomond, CA 95005-0803 *Counsel for Defendant-Appellant Daniel Meza*	**Jennifer A. Lynch** **Andrew G. Crocker** Electronic Frontier Foundation 815 Eddy St. San Francisco, CA 94109 *Counsel for Amicus Curiae Electronic Frontier Foundation*

BY ELECTRONIC MAIL: I served the document identified above by transmitting a true copy via electronic mail using my email address as jsnow@aclunc.org to:

California Appellate Project
CapDocs@lacap.com
Counsel for Defendants-Appellants

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 Chief Justice Patricia Guerrero and Associate Justices Supreme Court of California 350 McAllister St. San Francisco, CA 94102-4783	**Supreme Court of California** 350 McAllister St. San Francisco, CA 94102-4783
Administrative Presiding Justice Elwood Lui California Court of Appeal, Second Appellate District, Division 7 Ronald Reagan State Building 300 S. Spring St., 2nd Floor, North Tower Los Angeles, CA 90013	**Court of Appeal, Second Appellate District, Seventh Division** Ronald Reagan State Building 300 S. Spring St., B-228 Los Angeles, CA 90013
Honorable Laura R. Walton, Judge c/o Clerk of Court Clara Shortridge Foltz Criminal Justice Center 210 W. Temple St. Los Angeles, CA 90012	**Clara Shortridge Foltz Criminal Justice Center** 210 W. Temple St. Los Angeles, CA 90012

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

Executed on June 1, 2023, in San Francisco, CA.

/s/ Jacob A. Snow