ELECTRONIC FRONTIER FOUNDATION

ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATIONS
California

August 30, 2018

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

Amicus letter supporting request for review in *Gary Phillips Klugman v. The Superior Court of Monterey County*, Monterey County No. SS160207, Supreme Court of California Case No. S250426, petition filed August 6, 2018.

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

The Electronic Frontier Foundation (EFF) and the American Civil Liberties Union Foundation of Northern California, American Civil Liberties Union Foundation of Southern California, and American Civil Liberties Union of San Diego and Imperial Counties ("ACLU Foundations of California") urge the Court to grant petitioner's request for review.

The California Electronic Communications Privacy Act (CalECPA) took effect on January 1, 2016, giving Californians the strongest digital privacy protections in the nation. CalECPA brings privacy protections for electronic communications into the twenty-first century and extends critical privacy protections to the mobile devices that are ubiquitous in modern life. The consequence for violation of CalECPA's robust privacy protections is clear: suppression of any information obtained or retained by any such violation.

In this case, the Superior Court of California in Monterey County issued a search warrant that failed to comply with CalECPA's requirements, authorizing an effectively unlimited search, seizure, and extraction of electronic devices and information from a dentist's office in Salinas, California. The Superior Court denied defendant's motion to suppress the evidence under both CalECPA and the Fourth Amendment, concluding that: (1) the particularity requirements of CalECPA were no stricter than those imposed under the federal and state constitutions; and (2) even though the warrant violated CalECPA, suppression was not appropriate. These dramatic errors warrant this Court's intervention.

815 EDDY STREET, SAN FRANCISCO, CA 94109 USA
phone +1.415.436.9333 fax +1.415.436.9993 eff.org

The Court should grant the petition for review and issue immediate guidance to lower courts to ensure that CalECPA's privacy provisions are properly understood and enforced by all California courts. CalECPA was a watershed statute that established bright-line rules for California government entities seeking digital information. It includes an express suppression remedy for any violations of its provisions. The decision of the Superior Court reflects a profound misunderstanding of CalECPA's requirements and remedy, threatens the privacy protections promised to all Californians by CalECPA, and creates uncertainty for technology companies who call the state home. This Court should grant review to ensure proper implementation of the Legislature's mandate.

I. Interests of Amici

Proposed Amici are the EFF and the ACLU Foundations of California.

EFF is a San Francisco-based, donor-supported, non-profit civil liberties organization working to protect and promote fundamental liberties in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support free expression, privacy, and transparency in the information society. EFF has over 38,000 dues-paying members, over 400,000 subscribers, and represents the interests of everyday users of the Internet.

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization with more than 1.6 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. It has three California affiliates: the ACLU of Northern California, the ACLU of Southern California, and the ACLU of San Diego & Imperial Counties. The California ACLU affiliates 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 liberties and civil rights.

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

II. CalECPA Provides Strong, Clear Digital Privacy Rules for Government, Companies, and the Public.

California has a long tradition of providing more robust privacy protections than federal law. CalECPA continues that tradition. The California Constitution guarantees an

inalienable right to privacy for all Californians, articulated in The Privacy Amendment to Article 1, 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*, 13 Cal.3d 757, 774 (1975). This Court has consistently held that the California Constitution provides more robust privacy protection than the Fourth Amendment.[1] In particular, this Court has rejected the "third party doctrine," holding instead that Californians do not forfeit their reasonable expectation of privacy when they share their information with a third party. *See Burrows v. Superior Court*, 13 Cal.3d 238 (1974) (recognizing expectation of privacy in bank records under California Constitution even though *United States v. Miller*, 425 U.S. 435 (1976) found none under the Fourth Amendment).[2] The California Constitution specifically protects information about an individual that amounts to a "virtual current biography." *People v. Chapman*, 36 Cal.3d 98, 108 (1984) (expectation of privacy in a person's unlisted name, phone number and address since information could "provide essential link to establish a 'virtual current biography'").

Before CalECPA, however, federal and state statutory law did not properly safeguard modern electronic communication information in a way that was consistent with the California Constitution. The federal Stored Communications Act ("SCA") has not been meaningfully updated in more than thirty years and suffers from numerous antiquated infirmities.[3] California privacy law in the digital context was similarly "stuck in the digital dark ages"[4] and in need of revision.[5]

---

[1] *See People v. Mayoff*, 42 Cal.3d 1302, 1312-1314 (1986) (rejecting *California v. Ciraolo*, 476 U.S. 207 (1986) and *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) to find expectation of privacy in backyard visible via aerial surveillance under California Constitution); *In re Lance W.*, 37 Cal.3d 873, 884 (1985) (citing *People v. Brisendine*, 13 Cal.3d 528, 549 (1975)("Our vicarious exclusionary rule has never been required under the Fourth Amendment but has been a continuing feature of California law under our ability to impose higher standards for searches and seizures than compelled by the federal Constitution.") (internal citations omitted)).

[2] After CalECPA's passage, the Supreme Court recently limited the third-party doctrine under the Fourth Amendment, holding that the government needs a warrant to access location information records held by a wireless carrier about a person's cellphone location history. *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).

[3] "In significant places, however, a large gap has grown between the technological assumptions made in [the federal Electronic Communications Privacy Act] and the reality of how the Internet works today. This leaves us, in some circumstances, with complex and baffling rules that are both difficult to explain to users and difficult to apply."

CalECPA built on the robust privacy foundation of the California Constitution by establishing clear rules necessary to: (1) guide service providers and government agencies; and (2) protect Californians' privacy rights when the government seeks electronic communications and device information in the digital age.

First, CalECPA requires a probable-cause warrant for all electronic information and device information, including information sought from third-party service providers or from personal electronic devices.[6] Thus, under CalECPA, law enforcement and other California government entities must obtain a warrant to demand people's electronic information. This includes everything from emails, digital documents, and text messages to location and medical information.[7]

Hearing on "ECPA Part 1: Lawful Access to Stored Content" Before the H. Judiciary Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations, 113th Cong. 113-16 (2013) (written testimony of Richard Salgado, Dir., Law Enf't & Info. Sec., Google Inc).

[4] Nicole Ozer, *California is Winning the Digital Privacy Fight*, Tech Crunch (Nov. 7, 2015) https://techcrunch.com/2015/11/07/california-now-has-the-strongest-digital-privacy-law-in-the-us-heres-why-that-matters/; Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, Wired (Oct. 8, 2015) (quoting CA State Senator Mark Leno) (available at https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/).

[5] *See* Facebook Letter in Support of SB 178, March 13, 2015 ("[P]eople deserve to connect with friends and loved ones knowing that their personal photos and messages are well-protected.") (available at https://www.eff.org/document/facebook-sb-178-support-letter); Google Letter in Support of SB 178, March 12, 2015 ("law enforcement needs a search warrant to enter your house or seize letters from your filing cabinet — the same sorts of protections should apply to electronic data stored with Internet companies.") (available at https://www.eff.org/document/google-sb-178-support-letter); Internet Association Statement in Support of the Introduction of Cal-ECPA Legislation (SB 178) in the California Legislature, February 9, 2015 ("California's Internet users expect their inbox to have the same kinds of safeguards that exist for their mailbox, and we look forward to working with policymakers in pursuit of this goal. It is time to update these laws for the digital age.") (available at https://internetassociation.org/020915cal-ecpa/).

[6] Cal. Penal Code § 1546.1(a)(2), (a)(3).

[7] People also have strong privacy interests in the metadata—which is fully protected by CalECPA—associated with their accounts, devices, and information. *See Metadata: Piecing Together a Privacy Solution*, Report of the ACLU of California, February 2014 (available at https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf).

Second, CalECPA specifies the degree of detail that a warrant must contain. 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."[8] These enumerated warrant-particularity requirements are more specific—and more extensive—than currently required by Fourth Amendment or California constitutional jurisprudence.

Third, CalECPA requires that information unrelated to the objective of the warrant "shall be sealed and shall not be subject to further review, use, or disclosure." This provision is intended to ensure that digital searches do "not become a vehicle for the government to gain access to data which it has no probable cause to collect."[9]

Finally, a core provision of CalECPA is its clear and robust remedy—suppression of evidence. It provides for suppression of "any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of [CalECPA]." Cal. Penal Code § 1546.4(a). To this end, CalECPA incorporates the procedural structure for suppression motions set forth in Cal. Penal Code § 1538.5(b)–(q).

III. The Search Warrant Failed to Comply with CalECPA.

The search warrant in this case blatantly violated CalECPA's bright-line rules governing the specification of information sought to be seized and the sealing of information unrelated to the warrant's objective.

CalECPA requires that all warrants to access electronic information particularly describe the information sought as defined in Cal. Penal Code § 1546.1(d)(1). The warrant in this case failed numerous particularity requirements, authorizing the sweeping seizure of "[a]ny computer equipment" and all "[p]agers, cell phones, electronic notebooks, digital assistants, and their related manuals and documentation"—without any limitations as to "the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought." Appendix in Support of Petition for Writ of Mandate, Prohibition or Other Appropriate Relief ("App"), Vol. I, pp. 79, 82.

---

[8] Cal. Penal Code § 1546.1(d)(1).
[9] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc).

The warrant was in no way tailored to the alleged crime: it did not limit the subject matter of the information sought and extended broadly to information pertaining to innocent third parties as to whom there was no probable cause or suspicion of any wrongdoing whatsoever. *Id.* Notably, the search of a dentist's office swept up information with patient medical information protected by the federal Health Insurance Portability and Accountability Act. *E.g.*, App. Vol. II, pp. 265–260 (referring to medical information captured by the search), 272–273 (referring to patient information). A warrant of such unlimited scope fails to comply with even the Fourth Amendment's particularity requirements. It fails even more egregiously with respect to CalECPA's detailed and heightened particularity requirements.

CalECPA also mandates that the warrant "require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order." Cal. Penal Code § 1546.1(d)(1). No such requirement appeared in the warrant here. App. Vol. I, p. 82.

In denying petitioner's motion to suppress, the Superior Court ignored express statutory requirements governing particularity and sealing. App. Vol. II, pp. 340–344 (transcript of Superior Court ruling denying suppression). Intervention by this Court is necessary to ensure that all courts understand and properly enforce California's robust digital privacy law.

IV. Because CalECPA Was Violated, Suppression Was Required.

In this case, electronic communications information was obtained and retained in violation of CalECPA. The court therefore erred in denying petitioner's motion to suppress. Failing to suppress unlawfully obtained evidence violates the statute's language and its purpose.

CalECPA's requirements are set forth in unambiguous mandatory rules for government entities. Any warrant seeking electronic information, according to the statute, "shall comply with" the statute's detailed instructions. Cal Penal Code § 1546.1(d). Those instructions direct that warrants *must*—without exception—comply with the statute's restrictive provisions. Warrants "*shall* describe with particularity the information to be seized" and "*shall* require" that unrelated information be sealed off from further review. Cal Penal Code § 1546.1(d)(1), (d)(2) (emphasis added). These protections are not recommendations. They are strict rules with which all warrants for electronic information must comply. Failing to suppress evidence obtained in violation of CalECPA would impermissibly rewrite unambiguously mandatory statutory directives into merely

advisory language. The statute's plain text—"shall comply," "shall describe," "shall require"—simply does not comport with such a result.

The legislative history makes clear CalECPA contains a robust suppression remedy. The statute's authors highlighted the importance of the suppression remedy as the best way to ensure compliance with the statute's rules.[10] Discussion of the suppression remedy appears in the law's preamble[11] and every substantive legislative analysis.[12] The suppression remedy was a particular point of focus for the legislature because any statute that imposes a suppression remedy beyond the federal Constitution must pass the legislature with a two-thirds majority of both the Senate and Assembly.[13] This high legislative barrier for suppression remedies, which few laws have met, ensures that lawmakers are keenly aware of the cost of suppression when it is mandated by law. The plain language and statutory purpose of CalECPA therefore mandate suppression.

---

[10] Summary of the California Electronic Communications Privacy Act, Senators Leno and Anderson, September 2, 2015 (available at https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf). *See also Elkins v. United States*, 364 U.S. 206, 217 (1960) (noting that the purpose of suppression "is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.").

[11] S.B. 178, 2015–16 Session, Legislative Counsel's Digest (Ca. 2015) ("Because this bill would exclude evidence obtained or retained in violation of its provisions in a criminal proceeding, it requires a 2/3 vote of the Legislature.").

[12] Indeed, it is likely that California lawmakers eventually grew tired of seeing reference to the suppression remedy in CalECPA. *See* SB 178 (Leno) Committee Analysis, Senate Committee on Public Safety, March 23, 2015, p. 5; SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations, April 27, 2015, p. 3; SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations, May 28, 2015, p. 6; SB 178 (Leno) Committee Analysis, Senate Rules Committee, June 2, 2015, p. 6; SB 178 (Leno) Committee Analysis, Assembly Committee on Privacy and Consumer Protection, June 19, 2015, p. 3; SB 178 (Leno) Committee Analysis, Assembly Committee on Public Safety, July 13, 2015, p. 3. Full committee analyses available at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178.

[13] Cal. Const., Article I, § 28(d). The two-thirds majority was only necessary for CalECPA because the law mandates suppression of information *beyond* that which is required by the United States Constitution. *In re Lance W.*, 37 Cal.3d 873, 879 (1985). If only the federally mandated suppression was intended in CalECPA, a simple majority in both houses would have been enough.

V. Conclusion

The errors of the Superior Court in this case, if left uncorrected, will severely undercut the privacy rights of all Californians. Instead of enforcing the enhanced digital privacy protections that CalECPA enacted, the Superior Court found that CalECPA required no more than the "traditional analysis" under the federal and state constitutions. The Superior Court also concluded that, although CalECPA was "not specifically complied with," suppression was not appropriate.[14] These two errors eviscerate CalECPA's protections, render its robust enforcement provision toothless, and undermine the will of the California legislature to properly safeguard the digital privacy of all Californians. The Court should therefore grant the petition for review and properly address these blatant errors.

Respectfully submitted,

Stephanie J. Lacambra, No. 232517
Lee Tien, No. 148216
Counsel for Electronic Frontier Foundation

Nicole Ozer, No. 228643
Jacob A. Snow, No. 270988
Shilpi Agarwal, No. 270749
Counsel for the American Civil Liberties Union Foundations of California

cc: All Counsel

[14] App. Vol. II, pp. 343–344.

PROOF OF SERVICE BY MAIL

Re: Amicus letter supporting request for review in *Gary Phillips Klugman v. The Superior Court of Monterey County*, Monterey County No. SS160207, Supreme Court of California Case No. S250426, petition filed August 6, 2018.

I, Stephanie Lacambra, declare that I am over the age of 18 and not a party to the within action. My business address is 815 Eddy Street, San Francisco, CA 94109. I served a true copy of the attached Amicus Letter Brief of the Electronic Frontier Foundation in Support of Review on the following by placing a copy in a sealed envelope addressed to the parties listed below, which envelope was then sealed by me and deposited in the United States Mail, postage prepaid, at San Francisco, California on August 30, 2018.

Michael Lawrence
Law Offices of Lawrence & Peck
220 Capitol Street
Salinas, CA 93901

Joel Franklin
Law Offices Of Joel Franklin
2100 Garden Road, Suite G
Monterey, CA 93940

Counsel for Gary Phillips Klugman : Petitioner

Superior Court of Monterey County
240 Church Street
Salinas, CA 93901

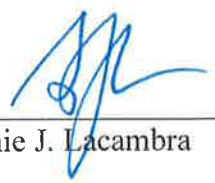
Counsel for Superior Court of Monterey County : Respondent

Attorney General - San Francisco Office
Office of the Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004

Elaine Susan McCleaf
Office of the District Attorney
230 Church Street
P.O. Box 1131
Salinas, CA 93902-1131

Counsel for The People : Real Party in Interest

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2018 at San Francisco, California.



Stephanie J. Lacambra