ACLU AMERICAN CIVIL LIBERTIES UNION FOUNDATION Northern California

ACLU AMERICAN CIVIL LIBERTIES UNION FOUNDATION Southern California

ELECTRONIC FRONTIER FOUNDATION

November 25, 2019

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*, Court of Appeal Sixth Appellate District Case No. H045415, Supreme Court of California Case No. S258818, petition filed October 28, 2019.

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

Officers in this case executed a warrant in January of 2016 to search two places: a home and a dentist's office. That warrant empowered the officers to confiscate, comprehensively analyze, and retain information from every mobile phone, every laptop computer, and every portable storage device at either location, no matter where they were found and regardless of who they belonged to. The mobile phone of the office receptionist, for example, could have been confiscated and searched. So could a tablet computer in possession of a dental patient or the laptop of any member of the public who happened to be present. So could a small storage device in the center console of a car in the parking lot.

Computing devices contain a rich intimate repository of information about not only the holder of the device but also any family, friends, and colleagues who might appear in the communications, photos, and documents accessible from the device. In the words of *Riley v. California*, mobile phones contain "the privacies of life." 134 S.Ct. 2473, 2496–96 (2014). It is those privacies—of *all* Californians and not just of the accused—that the California Electronic Communication Privacy Act ("CalECPA") protects with its clear and robust warrant requirements and suppression remedy for any violations.

The warrant in this case egregiously violated multiple provisions of CalECPA. But rather than suppressing the unlawfully gathered evidence, the Court of Appeals failed to enforce the critical digital privacy protections due to all Californians. The Court of Appeals decision threatens to undermine the will of the California legislature to properly safeguard the privacy of Californians. We urge the Court to grant petitioner's request for review.[1]

[1] In the alternative, amici request that the Court order, under rule 8.1125(a) of the California Rules of Court, that the Sixth District Court of Appeals' decision in *Klugman v. Superior Court*, filed August 30, 2019, be depublished.

I. Interests of Amici

Proposed Amici are the ACLU Foundation of Northern California, the ACLU Foundation of Southern California, and the Electronic Frontier Foundation.

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. Proposed Amici are the ACLU of Northern California and the ACLU of Southern California ("ACLU of Northern and Southern California"). The ACLU of Northern and Southern California participate in 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.

The Electronic Frontier Foundation ("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.

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 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*, 13 Cal.3d 757, 774 (1975). This Court has consistently held that the California Constitution provides more robust privacy protection than does the Fourth Amendment.[2] 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)

[2] *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).

(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).[3] 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 failed to properly safeguard modern electronic communication information in a way that was consistent with the California Constitution, particularly in light of the rapid spread of new information and communication technologies. The antiquated federal Stored Communications Act has not been meaningfully updated in more than thirty years and suffers from numerous infirmities.[4] California privacy law in the digital context was similarly "stuck in the digital dark ages"[5] and in need of revision.[6]

CalECPA, passed in 2015, was enacted specifically to address this deficit. It built on the robust foundation of the California Constitution by establishing clear rules to protect

---

[3] 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).

[4] "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." *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).

[5] 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/).

[6] *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/).

Californians' privacy rights when a government entity seeks electronic communications and device information.

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.[7] 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.[8]

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."[9] These enumerated warrant-particularity requirements are *more specific—and more extensive*—than currently required by Fourth Amendment or California constitutional jurisprudence. CalECPA includes heightened particularity requirements specifically because online services and devices house vast amounts of personal information. As a result, a warrant that permits the search of a device or online service threatens to intrude upon the privacy not just of the user of the online service or the holder of the device, but also upon countless others. CalECPA recognizes that, to effectively protect people's electronic privacy, the *warrant itself* must restrain the reach of the government's power to intrude into our most private digital spaces.

Third, CalECPA requires that the warrant explicitly provide that information unrelated to its objective "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."[10]

Finally, a core provision of CalECPA is its clear and robust remedies, including 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).

---

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

[8] 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).

[9] Cal. Penal Code § 1546.1(d)(1).

[10] *See, e.g.*, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc).

III. The Search Warrant Failed to Comply with CalECPA.

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

First, the warrant violated CalECPA's sealing mandate, which dictates that warrants "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). Here, the warrant did not contain that explicitly required provision. That omission was particularly egregious here, where the warrant countenanced the search of a dentist's office that swept up information entirely unrelated to the objective of the warrant, including patient medical information protected by the federal Health Insurance Portability and Accountability Act. *E.g.*, Appendix in Support of Petition for Writ of Mandate, Prohibition or Other Appropriate Relief ("App") Vol. II, pp. 265–260 (referring to medical information captured by the search), 272–273 (referring to patient information). The Court of Appeals agreed that the warrant failed entirely to comply with CalECPA's sealing requirement. *Klugman v. Superior Court*, Docket No. H045415, August 30, 2019 ("Slip Op.").

Second, the warrant failed to specify with particularity the scope of the permitted search. 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 authorized 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." App. Vol. I, pp. 79, 82. Instead of limiting the scope of the warrant to relevant devices or applications, the warrant swept broadly, encompassing devices and information pertaining to third parties for whom there was no probable cause or suspicion of any wrongdoing whatsoever. *Id.*

IV. Because CalECPA Was Violated, Suppression Was Required.

Intervention by this Court is necessary to make clear that CalECPA's suppression remedy applies when the statute is violated and to provide guidance for lower courts faced with potential violations of CalECPA. In the opinion below, the Court of Appeals held that the trial judge could deny a motion to suppress evidence that was undisputedly collected in violation of CalECPA. While *People v. Jackson*, 129 Cal.App.4th 129 (2005) clarified the suppression remedy for the California Wiretap Act, this Court must provide guidance that it is not the standard for CalECPA suppression. The California Wiretap Act and CalECPA are completely different statutory schema separated by decades of technological change and motivated by fundamentally different purposes.

The Court of Appeals erred in holding that suppression was not required when CalECPA was violated. *See* Slip Op. p. 19. None of the cases the Court of Appeals cited justify a holding

that would effectively eliminate CalECPA's core remedy. Both *Jackson* and *People v. Roberts*, 184 Cal.App.4th 1149 (2010) arise under the California Wiretap Act, a statute driven by a fundamentally different purpose from CalECPA. The California Wiretap Act was enacted more than two decades before CalECPA with the purpose of "expand[ing] California wiretap law to conform to the federal law." *People v. Zepeda*, 87 Cal. App. 4th 1183, 1196 (2001) (citing Senate Committee on Crim. Proc., Rep. on Assem. Bill No. 1016, (1995–1996 Reg. Sess.) as amended Apr. 3, 1995). CalECPA, by comparison, expanded protections *beyond* those available under applicable federal law. Analogies between remedies under the two laws are inappropriate.

The text of CalECPA dictates unambiguous mandatory rules for government entities seeking electronic communications and device information. 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 Court of Appeals based its decision on an erroneous statutory interpretation that contorted a drafting change into a wholesale elimination of rights. *See* Slip Op. p. 19, n. 10. During the legislative process, CalECPA was amended from providing that evidence "shall not be admissible" if it violates the law to the current version, which states that any person "may move to suppress" information obtained in violation of CalECPA.[11] The purpose of this amendment was to incorporate the existing procedures for filing motions to suppress under Penal Code Section 1538.5(b)–(q). But that amendment did nothing to eliminate the requirement that unlawfully collected evidence be suppressed.

It would make no sense for a statute—especially a statute intended to clarify and strengthen privacy protections and with suppression as its primary enforcement remedy—to merely permit the *filing* of a motion. CalECPA's authors highlighted the importance of the suppression remedy as the best way to ensure compliance with the statute's rules.[12] Discussion of

[11] Senate Bill No. 178 (2015–2016) Reg. Sess.) as introduced Feb. 9, 2015.
[12] 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.").

the suppression remedy appears in the law's preamble[13] and every substantive legislative analysis.[14] Indeed, CalECPA had to pass both houses of the California legislature by a two-thirds vote because the Truth in Evidence Act[15] requires a supermajority for any law that results in evidence being excluded in criminal proceedings.[16] This high legislative barrier for suppression remedies, which few laws have met, ensures that lawmakers are keenly aware when suppression will be mandated by a law. An empty suppression remedy is entirely inconsistent with CalECPA's purpose of safeguarding privacy rights and excluding unlawfully collected evidence.

V. Conclusion

The errors of the Court of Appeals 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 Court of Appeals found that CalECPA effectively required no more than the federal and state constitutions. The Court of Appeals decision threatens to 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.

---

[13] 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.").

[14] 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 analysis available at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178.

[15] 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.

[16] 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.").

Respectfully submitted,

Jacob A. Snow, No. 270988
Christopher J. Conley, No. 270749
Counsel for the American Civil Liberties Union Foundation of Northern California and the American Civil Liberties Union Foundation of Southern California

Lee Tien, No. 148216
Counsel for Electronic Frontier Foundation

cc: All Counsel

PROOF OF SERVICE BY MAIL

Re: Amicus letter supporting request for review in *Gary Phillips Klugman v. The Superior Court of Monterey County*, Court of Appeal Sixth Appellate District Case No. H045415, Supreme Court of California Case No. S258818, petition filed October 28, 2019.

I, Angela Castellanos, declare that I am over the age of 18 and not a party to the within action. My business address is 39 Drumm St, San Francisco, CA 94111. I served a true copy of the attached Amicus Letter Brief of the ACLU Foundation of Northern California, ACLU Foundation of Southern California, and 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 November 25, 2019.

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

Joel Franklin
Law Offices of Joel Franklin
225 Crossroads Boulevard, Suite 407
Carmel, CA 93293-8674

Counsel for Gary Phillips Klugman: Petitioner

Superior Court of Monterey County
Honorable Julie R. Culver
240 Church Street
Salinas, CA 93901

Counsel for Superior Court of Monterey County: Respondent

Attorney General - San Francisco Office
Office of the Attorney General
Amit Arun Kurlekar
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

Clerk of the Court
Sixth Appellate District
333 W. Santa Clara Street
Suite 1060
San Jose, CA 95113-1717

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 25, 2019 at San Francisco, California.

Angela Castellanos