

Appellate Case No. H045415

**IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
SIXTH APPELLATE DISTRICT**

GARY PHILLIPS KLUGMAN,

Petitioner and Appellant,

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA,
IN AND FOR THE COUNTY OF MONTEREY,

Respondent.

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff and Real Party in Interest.

Appeal from the Superior Court for the County of Monterey
The Honorable Julie R. Culver, Judge
Case No. SS160207A

**AMICI CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN
CALIFORNIA IN SUPPORT OF PETITIONER AND APPELLANT**

STEPHANIE LACAMBRA
(SBN 232517)
stephanie@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: 415.436.9333
F: 415.436.9993

Counsel for Amici Curiae

NICOLE OZER (SBN 228643)
nozer@aclunc.org
JACOB A. SNOW (SBN 270988)
jsnow@aclunc.org
SHILPI AGARWAL (SBN 270749)
sagarwal@aclunc.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T: 415.621.2493
F: 415.255.8437

COURT OF APPEAL SIXTH APPELLATE DISTRICT, DIVISION		COURT OF APPEAL CASE NUMBER: H045415
ATTORNEY OR PARTY WITHOUT ATTORNEY: STATE BAR NUMBER: 232517		SUPERIOR COURT CASE NUMBER: SS160207A
NAME: Stephanie Lacambra FIRM NAME: Electronic Frontier Foundation STREET ADDRESS: 815 Eddy Street CITY: San Francisco STATE: CA ZIP CODE: 94109 TELEPHONE NO.: (415) 436-9333 FAX NO.: (415) 436-9993 E-MAIL ADDRESS: stephanie@eff.org ATTORNEY FOR (name): Electronic Frontier Foundation (EFF)		
APPELLANT/ Gary Phillips Klugman PETITIONER: RESPONDENT/ The People of the State of California REAL PARTY IN INTEREST:		
CERTIFICATE OF INTERESTED ENTITIES OR PERSONS		
(Check one): <input checked="" type="checkbox"/> INITIAL CERTIFICATE <input type="checkbox"/> SUPPLEMENTAL CERTIFICATE		
Notice: Please read rules 8.208 and 8.488 before completing this form. You may use this form for the initial certificate in an appeal when you file your brief or a prebriefing motion, application, or opposition to such a motion or application in the Court of Appeal, and when you file a petition for an extraordinary writ. You may also use this form as a supplemental certificate when you learn of changed or additional information that must be disclosed.		

1. This form is being submitted on behalf of the following party (name): EFF and American Civil Liberties Union of Northern CA
2. a. There are no interested entities or persons that must be listed in this certificate under rule 8.208.
- b. Interested entities or persons required to be listed under rule 8.208 are as follows:

Full name of interested entity or person	Nature of interest (Explain):
--	-------------------------------

- (1)
- (2)
- (3)
- (4)
- (5)

Continued on attachment 2.

The undersigned certifies that the above-listed persons or entities (corporations, partnerships, firms, or any other association, but not including government entities or their agencies) have either (1) an ownership interest of 10 percent or more in the party if it is an entity; or (2) a financial or other interest in the outcome of the proceeding that the justices should consider in determining whether to disqualify themselves, as defined in rule 8.208(e)(2).

Date: March 27, 2019

Stephanie Lacambra
(TYPE OR PRINT NAME)


(SIGNATURE OF APPELLANT OR ATTORNEY)

TABLE OF CONTENTS

CERTIFICATE OF INTERESTED ENTITIES 2

I. INTRODUCTION 7

II. ARGUMENT 8

 A. CalECPA Provides Robust Digital Privacy Rules for the Government,
 Companies, and the Public That Go Beyond Those that Existed Prior to Its
 Passage..... 8

 B. The Search Warrant At Issue Here Violated CalECPA. 13

 C. Any Evidence Obtained in Violation of CalECPA Must Be Suppressed. 15

 1. CalECPA’s Suppression Remedy is More Robust Than Suppression
 Remedies Under the Fourth Amendment or Other California Statutes.
 16

 2. CalECPA’s Structure and Language Indicate that Information
 Collected in Violation of the Statute Must Be Suppressed. 17

 3. The Legislature’s Intent in Enacting CalECPA Will Be Undermined if
 Violations Do Not Result in Suppression. 18

III. CONCLUSION 20

CERTIFICATE OF WORD COUNT 22

PROOF OF SERVICE 23

TABLE OF AUTHORITIES

Cases

Boyd v. United States,
116 U.S. 616 (1886) 13

California v. Ciraolo,
476 U.S. 207 (1986) 9

Carpenter v. U.S.,
138 S. Ct. 2206 (2018)..... 13

Demaree v. Pederson,
887 F.3d 870 (9th Cir. 2018) 13

Dow Chemical Co. v. United States,
476 U.S. 227 (1986) 9

Elkins v. United States,
364 U.S. 206 (1960) 21

In re Lance W.,
37 Cal.3d 873 (1985)..... 9, 21

People v. Brisendine,
13 Cal.3d 528 (1975) 9

People v. Chapman,
36 Cal.3d 98 (1984)..... 9

People v. Hoag,
83 Cal. App. 4th 1198 (2000) 18

People v. Jackson, 129 Cal. App. 4th 129 (2005) 18

People v. Mayoff,
42 Cal.3d 1302 (1986)..... 9

Riley v. California,
573 U.S. 373 (2014) 13

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010)..... 13

White v. Davis,
13 Cal.3d 757 (1975)..... 9

Statutes

Cal. Penal Code § 1524(c)..... 18

Cal. Penal Code § 1538.5(a)..... 13

Cal. Penal Code § 1538.5(b)–(q) 13, 18

Cal. Penal Code § 1538.5(n)..... 18

Cal. Penal Code § 1546.1(a)(2), (a)(3)..... 11

Cal. Penal Code § 1546.1(d)(1) 11

Cal. Penal Code § 1546.1(d)(2) 11

Cal. Penal Code § 1546.1(e)..... 17

Cal. Penal Code § 1546.1(e)(1) 18

Cal. Penal Code § 1546.1(e)(2) 18

Cal. Penal Code § 1546.1(g)..... 17

Cal. Penal Code § 1546.1(h)..... 17

Cal. Penal Code § 1546.4(a)..... 13, 15, 18

Cal. Penal Code § 1546.4(c)..... 17

Cal. Penal Code § 1546(l) 11

Constitutional Provisions

Cal. Const., Article 1, § 28 16

Cal. Const., Article I, § 28(d) 19

Legislative Materials

S.B. 178, 2015–16 Session, Legislative Counsel’s Digest (Ca. 2015)..... 19

SB 178 (Leno) Committee Analysis, Assembly Committee on Public Safety
(July 13, 2015)..... 20

SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations
(April 27, 2015)..... 19

SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations
(May 28, 2015)..... 19

SB 178 (Leno) Committee Analysis, Senate Committee on Public Safety
(March 23, 2015).....19

SB 178 (Leno) Committee Analysis, Senate Rules Committee
(June 2, 2015).....20

Summary of the California Electronic Communications Privacy Act, Senators Leno and
Anderson (September 2, 2015)19

Other Authorities

*ECPA Part 1: Lawful Access to Stored Content: Hearing Before the H. Judiciary
Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations, 113th Cong. 113-16
(2013).....10*

Facebook Letter in Support of SB 178 (March 13, 2015)10

Google Letter in Support of SB 178 (March 12, 2015).....10

Internet Association Statement in Support of the Introduction of Cal-ECPA Legislation
(SB 178) in the California Legislature (February 9, 2015).....10

Kim Zetter, *California Now Has the Nation’s Best Digital Privacy Law*, Wired (Oct. 8,
2015).....10

Metadata: Piecing Together a Privacy Solution, Report of the ACLU of California
(February 2014).....11

Nicole Ozer, *California is Winning the Digital Privacy Fight*, Tech Crunch (Nov. 7,
2015).....10

I. INTRODUCTION

The Electronic Frontier Foundation (“EFF”) and the American Civil Liberties Union Foundation of Northern California (“ACLU of Northern California”) urge the Court to uphold the California Electronic Communications Privacy Act’s (“CalECPA”) robust statutory suppression safeguard. CalECPA’s suppression remedy is integral to the legislature’s intent to enforce Californians’ fundamental constitutional privacy rights at a time when technological change presents challenges to traditional privacy safeguards.

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 21st century by clearly defining our privacy rights with respect to the mobile devices and online services that have become ubiquitous in modern life. The consequence for violating CalECPA’s robust privacy protections is clear: suppression and deletion of any information obtained or retained in violation of the statute’s provisions.

This case comes from the superior court of California in Monterey County, which issued a search warrant, just weeks after CalECPA went into effect, authorizing an effectively unlimited search, seizure, and extraction of electronic devices and information from a dentist’s office in Salinas, California. The dentist, defendant Gary Phillips Klugman, was later charged based on evidence seized from these devices and moved to suppress the evidence under CalECPA. While the superior court agreed with Klugman

that CalECPA had “not [been] specifically complied with,”¹ it denied his motion to suppress under both CalECPA and the Fourth Amendment, concluding incorrectly 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.

CalECPA was a watershed statute that established bright-line rules for California government entities seeking to obtain, retain, and use digital information. It includes an express suppression remedy for any violation of its provisions. The superior court’s decision 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 reverse the superior court’s denial of the motion to suppress and issue immediate guidance to lower courts to ensure that the Legislature’s mandate is properly understood and implemented.

II. ARGUMENT

A. **CalECPA Provides Robust Digital Privacy Rules for the Government, Companies, and the Public That Go Beyond Those that Existed Prior to Its Passage.**

California has a long tradition of providing privacy protections that are more robust than those found under federal law. The California Constitution guarantees an inalienable right to privacy for all Californians, articulated in the Privacy Amendment to

¹ App. Vol. II, pp. 343–344.

Article 1, Section 1, which protects the privacy rights of “all people.” The Privacy Amendment was a 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).

Indeed, the California Supreme Court has consistently held that the California Constitution provides more expansive privacy protection than does 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 law did not properly protect 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 infirmities.³

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); *In re Lance W.*, 37 Cal.3d 873 (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)).

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 California privacy law was similarly “stuck in the digital dark ages”⁴ and in need of revision.⁵

CalECPA filled this gap. It was drafted with the specific intention of giving force to the privacy rights enshrined in 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 to seize and search their electronic communications and device information in the digital age.

CalECPA’s privacy protections are far more robust than those provided by the Fourth Amendment and other preceding federal and state privacy statutes. CalECPA

and baffling rules that are both difficult to explain to users and difficult to apply.” *ECPA Part 1: Lawful Access to Stored Content: Hearing 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/>).

requires California law enforcement agencies to obtain a probable-cause warrant for almost all electronic information, including information sought from third-party service providers or from personal electronic devices.⁶ This includes everything from text messages, emails, digital documents and media, to location and medical information.⁷

CalECPA also increases the degree of detail with which a warrant must describe its scope. 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 particularity requirements are more specific—and more extensive—than currently required by the Fourth Amendment, California constitutional jurisprudence or prior statutory law.

CalECPA also requires that information unrelated to the objective of the warrant “shall be sealed and shall not be subject to further review, use, or disclosure.”⁹ This

⁶ Cal. Penal Code § 1546.1(a)(2), (a)(3). The only type of information that does not require a warrant is “subscriber information,” which includes the name and other identifying details of a subscriber to a service. *Id.* § 1546(l). All subsequent statutory references are made with respect to the California Penal Code.

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>).

⁸ § 1546.1(d)(1).

⁹ §1546.1(d)(2).

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 U.S. Supreme Court cases like *Riley*¹¹ and *Carpenter*¹² make clear that one of the gravest risks of device searches is that so many intimate details of our lives are stored on our mobile phones and other personal electronic devices. CalECPA’s mandate that irrelevant information be segregated and sealed is integral to protecting against the “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.”¹³

CalECPA contains robust remedies to give weight to these privacy protections. Chief among them is its strong suppression remedy, enacted by a two-thirds majority of both houses of the California legislature, demanding exclusion of “any electronic information obtained or retained in violation of the Fourth Amendment to the United

¹⁰ *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (abrogation recognized in *Demaree v. Pederson*, 887 F.3d 870 (9th Cir. 2018)).

¹¹ *Riley v. California*, 573 U.S. 373, 403 (2014) (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886) (“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life’”)).

¹² *Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018) (citing *United States v. Jones*, 565 U.S. 400 (2012) (“Mapping a cell phone’s location over [time] provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations’”)).

¹³ *U.S. v. Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176.

States Constitution or of [CalECPA].” § 1546.4(a). To this end, CalECPA was carefully crafted to only incorporate the procedural structure for suppression motions set forth in § 1538.5(b)–(q), but not the basis for bringing those motions in § 1538.5(a).¹⁴

In sum, CalECPA’s protections go far *beyond* those that governed electronic communications prior to its passage—the statute did not merely recite pre-existing standards under the Fourth Amendment or any other statutory scheme, but transcended them. CalECPA is the legislature’s answer to the gap between California’s constitutional privacy principles and the digital privacy laws that existed prior to its passage. Only robust enforcement of its suppression remedy can accomplish CalECPA’s aims.

B. The Search Warrant At Issue Here Violated CalECPA.

The search warrant in this case, issued after CalECPA went into effect, violated the statute’s bright-line rules requiring specificity as to information sought 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 § 1546.1(d)(1). The warrant in this case falls short: it 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

¹⁴ § 1546.4(a)(“The [suppression] motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of § 1538.5.”)

sought.” Appendix in Support of Petition for Writ of Mandate, Prohibition or Other Appropriate Relief (“App”), Vol. I, pp. 79, 82. It summarily fails every particularity requirement set forth in the statute.

Moreover, the warrant was in no way tailored to the alleged crime: it failed to 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.* The warrant broadly sought “evidence including but not limited to the content of electronic devices that tended to show the possession of child pornography and the sexual exploitation of children” (*see* State’s opposition brief filed February 21 (“State Opp.”), p.23) found on any “[p]agers, cell phones, electronic notebooks, digital assistants and their related manuals and documentation” regardless of its possessor or operator. App. Vol. I, p. 82 (Search Warrant filed on Jan 21, 2016).

Nor did the warrant clearly exclude devices or accounts for which there was no probable cause. The warrant failed to limit its search to target individuals or devices and accounts possessed by targeted individuals that contained the sought-after digital information, the applications or services covered, or the types of information sought. § 1546.1(d)(1). To the contrary, the warrant expressly provided that, “[i]f any computers, cellular phones, or electronic data storage devices [we]re found,” a search of the hypothetical “hard drive, floppy disks or software applications or cellular phones” was allowed. App. Vol. I, p. 82. As written, then, the warrant encompasses all digital devices found at the dentist’s office—including those owned and operated by staff and clients for which the supporting affidavit offers no probable cause. App. Vol. I, p. 79–84. A warrant

of such unlimited scope fails to comply with CalECPA's particularity requirements.

CalECPA also mandates that warrants shall "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." § 1546.1(d)(2). The warrant is silent as to how this requirement was to be observed and complied with. App. Vol. I, p. 79–83. Such omission renders the warrant facially invalid under CalECPA.¹⁵

The warrant in this case presents precisely what CalECPA was designed to prevent. It is impermissibly overbroad, lacks particularity, and failed to mandate the sealing of irrelevant evidence. In denying petitioner's motion to suppress, the superior court ignored the legislature's clear mandate. App. Vol. II, pp. 340–344 (transcript of superior court ruling denying suppression).

C. Any Evidence Obtained in Violation of CalECPA Must Be Suppressed.

CalECPA's suppression remedy mandates that all information obtained or retained in violation of its terms must be suppressed. § 1546.4(a). This suppression remedy is broader than that under the Fourth Amendment, and is more robust than remedies available for traditional searches under California law. Consistent enforcement of the suppression remedy is critical to the overall statutory framework.

¹⁵ In addition, the particularity and sealing requirements under CalECPA are separate and independent; failure to comply with either cannot be cured by satisfying the other.

1. CalECPA’s Suppression Remedy is More Robust Than Suppression Remedies Under the Fourth Amendment or Other California Statutes.

Article 1, § 28 of the California Constitution provides that evidence in a criminal trial may only be suppressed if suppression is required by the Fourth Amendment or “as provided by statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature.” CalECPA is one of the few statutes to satisfy that super-majority requirement. Indeed, both its history and its language demonstrate that CalECPA’s suppression remedy reaches beyond information protected by the Fourth Amendment. In enacting CalECPA with a two-thirds majority, the legislature evinced a clear intent to extend its suppression remedy beyond those constraints.¹⁶

Accordingly, Fourth Amendment cases—like *People v. Hoag*, which the government references—cannot govern the Court’s determination of the scope of CalECPA’s suppression remedy.¹⁷ CalECPA is not bound by the totality of the circumstances analysis articulated in federal constitutional jurisprudence, but instead lays out a set of bright-line rules defining a valid digital search warrant. A violation of any of CalECPA’s provisions triggers its strong suppression remedy.

¹⁶ This scope of CalECPA—to extend protections beyond federal law—stands in stark contrast to the California Wiretap Act, which was explicitly intended to “conform to federal law.” *People v. Jackson*, 129 Cal. App. 4th 129, 152 (2005) *as modified on denial of reh’g* (June 7, 2005) (citing Senate Committee on Criminal Procedure, Report on Assembly Bill Number 1016 (1995-1996 Regular Session) as amended April 3, 1995).

¹⁷ See *People v. Hoag*, 83 Cal. App. 4th 1198, 1211 (2000) (“[T]he essential *Fourth Amendment* inquiry is whether, under the totality of the circumstances, the policies underlying the knock-notice requirement have nevertheless been served.” (emphasis added)).

2. CalECPA’s Structure and Language Indicate that Information Collected in Violation of the Statute Must Be Suppressed.

CalECPA governs the lifecycle of information as it is obtained, retained, and used by law enforcement. When those restrictions are violated, CalECPA makes clear that law enforcement’s possession of electronic information must come to a swift and conclusive end in two ways: (1) the government must destroy the information at issue, and (2) courts must suppress any attempt to use that information in court.

CalECPA’s rules operate—by design—with clarity and finality. Destruction is mandatory within 90 days when information is voluntarily provided by a service provider to the government, unless special procedures are followed and retention is approved by the court. § 1546.1(g). Similarly, when information is acquired pursuant to the emergency exception, but the court finds that the facts did not give rise to an emergency, the court must “order the immediate destruction of all information obtained.” § 1546.1(h). Finally, any individual whose information is swept up in an unlawful warrant may (if they so choose) petition the issuing court “to order the destruction of any information” unlawfully obtained. § 1546.4(c). CalECPA’s destruction remedy works in tandem with the suppression remedy required when the government violates any provision of CalECPA. § 1546.4(a).

These mandatory destruction and suppression requirements stand in contrast to the two (and only two) actions in CalECPA that are left to the court’s discretion.¹⁸ First, a

¹⁸ “When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do any

court has discretion, subject to the imperatives codified in § 1524(c), whether to appoint a special master to ensure that information unrelated to the objective of the warrant is not produced or accessed. § 1546.1(e)(1). And second, a court has discretion to decide whether to order that unrelated information be destroyed at the end of the investigation. Penal Code § 1546.1(e)(2).

Suppression is the primary mechanism through which CalECPA’s mandatory requirements are to be enforced. For the Court to permit the government to offer evidence that is tainted by a violation of CalECPA’s provisions would be to rewrite the clear and mandatory language presented in the statute. Indeed, the government’s attempt to inject flexibility into unambiguous, mandatory provisions of CalECPA disregards the legislature’s careful crafting. The Court should construe the statute in accordance with its plain language. Suppression must result when CalECPA is violated.¹⁹

3. The Legislature’s Intent in Enacting CalECPA Will Be Undermined if Violations Do Not Result in Suppression.

CalECPA was enacted to ensure greater judicial oversight of law enforcement

or all of the following . . .” Penal Code § 1546.1(e).

¹⁹ The Court should not import suppression standards into a statute that expressly carves them out. CalECPA carefully incorporates only the procedural structure for the filing of suppression motions codified in § 1538.5(b)–(q) and does not incorporate § 1538.5(a), which provides the basis for motions to suppress under the Penal Code. See § 1546.4(a). In fact, Section 1538.5(n)—which is referenced by CalECPA—is explicit that it establishes only the procedure for suppression, and “does not establish or alter any ground for suppression of evidence.” § 1538.5(n). The standard for granting a suppression motion must arise, therefore, from CalECPA itself, rather than from inferences drawn from 1538.5 or cases interpreting it. And CalECPA requires suppression when the statute is violated.

access to information, supported by mandatory compliance measures like statutory suppression. Limiting CalECPA’s suppression remedy would undermine the will of the California legislature, which enacted CalECPA by a two-thirds majority²⁰ of both houses to ensure that non-compliance would be punished by suppression sought by “any person in a trial, hearing, or proceeding.” This super-majority requirement, which few laws have met, ensures that lawmakers are keenly aware when laws mandate suppression above and beyond that required under the Fourth Amendment.

The legislative history makes clear that CalECPA requires this robust suppression remedy for violations of its provisions. The statute’s authors highlighted the importance of the suppression remedy as the best way to ensure compliance with the statute’s rules.²¹ Discussion of the suppression remedy appears in the law’s preamble²² and every substantive legislative analysis.²³ Only mandatory suppression is consistent with the

²⁰ 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 at 879. If only the federally mandated suppression was intended in CalECPA, a simple majority in both houses would have sufficed.

²¹ 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.”).

²² 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.”).

²³ *See* SB 178 (Leno) Committee Analysis, Senate Committee on Public Safety, March 23, 2015, p. 5; SB 178 (Leno) Committee Analysis, Senate Committee on

statute’s clear purpose of increasing privacy protections for Californians and its intent to suppress any evidence gathered in violation of those rules.

III. 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.²⁴ These two errors eviscerate CalECPA’s privacy 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 reverse the trial court’s error in failing to uphold CalECPA’s suppression remedy for the government’s statutory violations.

Dated: March 27, 2019

Respectfully submitted,

/s/ Stephanie Lacambra

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.

²⁴ App. Vol. II, pp. 343–344.

NICOLE OZER (SBN 228643)
nozer@aclunc.org
JACOB A. SNOW (SBN 270988)
jsnow@aclunc.org
SHILPI AGARWAL (SBN 270749)
sagarwal@aclunc.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T: 415.621.2493
F: 415.255.8437

STEPHANIE LACAMBRA
(SBN 232517)
stephanie@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: 415.436.9333
F: 415.436.9993

Counsel for Amici Curiae

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this *Amici Curiae* Brief of Electronic Frontier Foundation and American Civil Liberties Union Foundation of Northern California is proportionally spaced, has a typeface of 13 points or more, contains 3,784 words, excluding the cover, the tables, the signature block, verification, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: March 27, 2019

/s/ Stephanie Lacambra
Stephanie Lacambra

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

Document received by the CA 6th District Court of Appeal.

PROOF OF SERVICE

I, Victoria Python, declare:

I am a resident of the state of California and over the age of eighteen years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On March 27, 2019, I served the foregoing documents:

***AMICI CURIAE* BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN
CALIFORNIA IN SUPPORT OF PETITIONER AND APPELLANT**

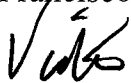
on the interested parties in this action as stated in the service list below:

X BY TRUEFILING: I caused to be electronically filed the foregoing document with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website.

X BY FIRST CLASS MAIL: I caused to be placed the envelope for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid.

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

Executed on March 27, 2019 at San Francisco, California.



Victoria Python

Document received by the CA 6th District Court of Appeal.

SERVICE LIST

Dean D. Flippo, Esq.
District Attorney
Elaine McCleaf, Esq.
Deputy District Attorney
Office of the Monterey County
District Attorney
230 Church Street
P.O. Pox 1131
Salinas, CA 93902-1131
Telephone: (831) 755-5070
McCleafE@co.monterey.ca.us

*Via TrueFiling
and
Via First Class Mail*

Office of the Attorney General
State of California
455 Golden Gate Avenue
Suite 11000
San Francisco, CA 94102
Tel: (415) 510-4400

*Via Truefiling
and
Via First Class Mail*

*Attorneys for Plaintiff and Respondent
The People of California*

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

*Via Truefiling
and
Via First Class Mail*

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

Via First Class Mail

*Attorneys for Defendant and Appellant
Gary Phillips Klugman*

Clerk of the Court
Monterey County Superior Court
Salinas Branch
240 Church Street
Salinas, CA 93901-2695

Via First Class Mail

Document received by the CA 6th District Court of Appeal.

for delivery to the
Hon. Julie R. Culver

Clerk of the Court
Sixth District Court of Appeal
333 West Santa Clara Street
Suite 1060
San Jose, CA 95113-1717

Via First Class Mail

Document received by the CA 6th District Court of Appeal.