AT THE PRIVACY VANGUARD: CALIFORNIA'S ELECTRONIC COMMUNICATIONS PRIVACY ACT (CALECPA)

Susan Freiwald†

ABSTRACT

This Article engages with and contributes to the academic literature on electronic communications privacy by providing the first detailed assessment of California's groundbreaking legislation. It provides judges and practicing attorneys with practical information on how to interpret and apply CalECPA. In addition, because it analyzes the statute's innovations and the questions it leaves unanswered, those considering whether to replicate CalECPA's provisions in Congress, as well as statehouses across the country, will find it valuable.

DOI: https://doi.org/10.15779/Z388G8FH73

† Professor, USF School of Law. I owe thanks to Mario Iskander, Everett Monroe, Arlette Noujaim, and Chi Vu for their excellent research assistance and Chris Conley, Nicole Ozer, Lee Tien, and attendees of the Privacy Law Scholars' conference in June of 2016 for their exceptionally helpful editing suggestions and discussions about CalECPA. I 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, I 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.

TABLE OF CONTENTS

I. INTRODUCTION

In a significant and somewhat surprising development, the law governing access to electronic communications by law enforcement in California became much more protective of communications privacy a few years ago in 2016. The California Electronic Communications Privacy Act (CalECPA)[1]—the most privacy-protective legislation of its kind in the nation[2]—came into effect on January 1, 2016.[3] In many ways, CalECPA simplified electronic surveillance law in California by making it more uniform, but those lawyers, judges, and companies affected by it would benefit from clarification of its potentially confusing provisions.[4] Moreover, it makes sense to review what makes CalECPA a worthy model, as some states have patterned reform bills on CalECPA,[5] and other states and even Congress may want to do the same.[6] This Article explains CalECPA's intricate provisions, including how it significantly improves on federal law. It heralds the new law's statutory innovations and

1. California Electronic Communications Privacy Act, CAL. PENAL CODE § 1546 (West 2017).

2. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [http://perma.cc/DL9B-GTXH].

3. Governor Brown signed the bill, S.B. 178, into law on October 8, 2015. *In a Landmark Victory for Digital Privacy*, *Gov. Brown Signs California Electronic Communications Privacy Act into Law,* ACLU OF N. CAL. (Oct. 8, 2015), www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy [http://perma.cc/YN5W-KS6X].

4. Just after CalECPA's passage, lawyers offered companies help in understanding the new law's requirements. *See, e.g.*, Abby Liebeskind, *8 Things to Know About CalECPA*, ZWILLGEN BLOG (Dec. 4, 2015), http://blog.zwillgen.com/2015/12/04/8-things-to-know-about-calecpa/ [https://perma.cc/M79Z-4WXT]. Law enforcement agencies described the new law as needing clarification. *See, e.g.*, Mark Hutchins, *Electronic Communications Searches: The New California Law*, POINT VIEW, Winter 2016, at 2, http://le.alcoda.org/publications/point_of_view/files/POV_Winter_2016.pdf [http://perma.cc/U398-JU4H] (referring to "uncertainties and dubious provisions" in CalECPA).

5. *See, e.g.*, Assemb. B. No. 1895, 2017–2018 Gen. Assemb., 1st Reg. Sess. (N.Y. 2017) (basing the provisions of the "New York Electronic Communications Privacy Act" on CalECPA); S.B. 61, 1st Reg. Sess. (N.M. 2017) (basing provisions of the "Electronic Communications Privacy Act" on CalECPA).

6. *See, e.g.*, Chris Conley, *California Leads on Electronic Privacy*: *Other States Must Follow*, ACLU: SPEAK FREELY (Oct. 13, 2015, 5:15 PM), https://www.aclu.org/blog/speak-freely/california-leads-electronic-privacy-other-states-must-follow [http://perma.cc/WG65-KQMQ]; G.S. Hans, *California ECPA Coalition Looks to Modernize Email Privacy*, CTR. FOR DEMOCRACY & TECH. BLOG (Feb. 9, 2015), https://cdt.org/blog/california-ecpa-coalition-looks-to-modernize-email-privacy/ [http://perma.cc/P6QQ-ZR3C] ("As the most populous state and a key influencer on privacy issues, California addressing this pressing issue with strong language will help advance federal reform efforts.").

also identifies some of the complex questions in communications privacy law that CalECPA currently leaves unresolved.

The Article is organized in six parts. Part II describes CalECPA's passage. It lays out the legal backdrop for the bill and shows how its proponents used that backdrop to argue that CalECPA was both much needed and, at the same time, not a big stretch from current law. In addition, it identifies a social context of increased concern about online privacy that likely contributed to the bill's passage.[7] Part III carefully reviews each of CalECPA's chief provisions, describing what they do and how they interact with each other and with other parts of the California code. Part IV describes how CalECPA improves upon its namesake, the federal Electronic Communications Privacy Act (ECPA),[8] by illustrating CalECPA's expansiveness and its additional protections. Part V identifies some of the legal issues that CalECPA leaves open, issues that other states and Congress might well consider, and it suggests several ways that CalECPA may challenge the way judges, lawmakers and scholars think about electronic communications privacy. Part VI concludes.

II. WHAT IS CALECPA AND HOW DID IT GET PASSED?

CalECPA replaced a number of California state statutes that offered complex and incomplete protections with a relatively uniform approach that requires law enforcement[9] to obtain a warrant to access almost all electronic communication information.[10] To comply with CalECPA, government entities in California must obtain a circumscribed warrant based on probable cause before they may obtain a person's electronic communication information from either her service provider or her electronic device.[11] As Part IV explains in more detail, CalECPA goes much further than ECPA by requiring a warrant for access to all electronic communications content, not just a subset of it, and

7. *See, e.g.*, Eyragon Eidam, *California's New Law Affects Search Warrants for Electronic Communications, Data—But How Much?*, GOV'T TECH. (Jan. 6, 2016), http://www.govtech.com/state/Californias-New-Law-Affects-Search-Warrants-for-Electronic-Communications-Data-But-How-Much.html [http://perma.cc/PGT4-7K3B] (reporting that disclosures of National Security Agency surveillance had heightened concern about digital data collection and that CalECPA was an "impassioned issue").

8. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

9. CalECPA applies to all government entities but will chiefly regulate law enforcement investigations because its warrant requirement does not apply to investigations that lack a law enforcement purpose. CAL. PENAL CODE § 1546.1(a) (West 2017); *see also infra* Section III.B (offering a detailed discussion of CalECPA's provisions).

10. CalECPA also protects electronic device information that goes beyond electronic communication information. *See infra* Section III.A.2.

11. § 1546.1(a).

by extending the warrant requirement to metadata, including location data. As one of the bill's sponsors explained, CalECPA "protects most electronic information, including personal messages, passwords and PIN numbers, geolocation data, photos, medical and financial information, contacts, social networking content, web browsing history, and metadata."[12]

Unlike analogous statutes, CalECPA requires a warrant for access to information about an electronic device that is not associated with a particular communication, including information that the device generates or that is merely stored on the device.[13] Also unlike ECPA, CalECPA requires the government to furnish notice, in all cases, to the target of the investigation, and provides a suppression remedy for evidence gathered in violation of its terms. A suppression remedy significantly deters noncompliance by prohibiting the use of improperly obtained evidence in court.[14]

It is unsurprising that California would pioneer a comprehensive electronic communications privacy law, given the state's historic position at the vanguard of modern privacy regulators. But because CalECPA set out to do so much more to protect the privacy of electronic communications than ECPA and other analogous state laws, observers doubted the bill's prospects.[15] In addition, CalECPA's suppression remedy necessitated that two-thirds or more of the legislature approve it. In fact, obtaining Governor Brown's signature loomed as the biggest hurdle to passage because the Governor had previously vetoed bills of more limited scope.[16] In 2013, for example, the Governor had vetoed a bill that would have required a warrant and notice to the target when government entities compelled the disclosure of communications content

12. *Tech Industry Stands with Sen. Leno to Modernize Digital Privacy Protections*, ACLU OF N. CAL. (Feb. 9, 2015), www.aclunc.org/news/tech-industry-stands-sen-leno-modernize-digital-privacy-protections [http://perma.cc/W8BP-SJYY]. *See infra* Section V.A (discussing the ambiguity of the content of electronic communications).

13. CAL. PENAL CODE §§ 1546.1(a)(2), 1546(g).

14. CAL. PENAL CODE § 1546.4(a). *See infra* Section III.D.

15. This comment is based on the author's conversations with people involved with legislative reform efforts at the federal level.

16. S.B. 467, 2013-2014 Reg. Sess. (Cal. 2013) (vetoed Oct. 12, 2013); *see also* S.B. 1434, 2011-2012 Reg. Sess. (Cal. 2012) (vetoed Sep. 9, 2012). In his veto message for S.B. 467, Governor Brown complained that the bill's notice provision would go beyond federal law requirements. In vetoing S.B. 1434, which would have required a warrant for location data, Governor Brown remained unconvinced that the bill struck "the right balance between the operational needs of law enforcement and individual expectations of privacy." Letter from Edmund G. Brown, Jr., Governor of Cal., to Members of the Cal. State Assembly (Sept. 30, 2012), https://www.gov.ca.gov/docs/SB_1434_Veto_Message.pdf [http://perma.cc/PQ5N-NPQB].

from service providers. Unlike CalECPA, that bill omitted coverage of location data, metadata, or device-accessed data, and it lacked a suppression remedy.[17]

How did CalECPA, which was much more ambitious than such prior bills, then pass? A large coalition of technology companies, civil liberties and civil society groups, journalists, and academics spent over a year working hard to build a case for reform against a legal backdrop of existing state and federal law.[18] Of course, timing also helped; CalECPA passed in a social context in which concern had built about law enforcement use of private data.

A. CALIFORNIA LAW

For years, California has positioned itself as an early adopter of privacy-protective legislation in the commercial context. For example, California was one of the first states to pass aggressive anti-spam legislation to protect users from privacy-invasion by unwanted communications[19] and the first to pass a data breach notification law to protect consumers' data security.[20] California's requirement that online providers post their privacy policies in a conspicuous position has set the nationwide standard,[21] and California has been quick to implement a version of the "right to be forgotten" for minors.[22] In fact, a recently published book on California privacy law advised privacy compliance officers to plan to update their compliance policies regularly because "[t]he California legislature constantly enacts new laws."[23]

But California has been much slower to modernize its rules for law enforcement access to electronic communication information. With the exception of the Reader Privacy Act of 2011, which requires a warrant-like court order before government agents may obtain customer records pertaining to book services,[24] those laws have not changed much in recent years. As

17. Cal. S.B. 467 § 5 (providing for a civil action of $1,000).

18. *See generally* Dave Maas, *CalECPA and the Legacy of Digital Privacy: An Open Letter to Gov. Jerry Brown*, ELEC. FRONTIER FOUND. (Sept. 23, 2015), https://www.eff.org/deeplinks/2015/09/open-letter-gov-jerry-brown-calecpa-and-legacy-technology [http://perma.cc/X37D-KF3Y] (describing the extensive support for CalECPA).

19. CAL. BUS. & PROF. CODE § 17529–29.9 (West 2014).

20. CAL. CIV. CODE § 1798.82(a) (West 2017); *see also 10 Years After S.B. 1368 California Attorney General Issues First Ever Report and Recommendations on Data Breaches*, INFOLAWGROUP LLP (July 1, 2013), http://www.infolawgroup.com/2013/07/articles/breach-notice/10-years-after-sb-1386-california-attorney-general-issues-first-ever-report-and-recommendations-on-data-breaches/ [http://perma.cc/N43F-UYQ9].

21. California Online Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575(a) (West 2014).

22. CAL. BUS. & PROF. CODE § 22580–81 (West 2015).

23. LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY § 3-12 (2016).

24. Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

previously mentioned, bills updating the laws to adapt to new electronic communications technologies have made it through the legislature, only to be vetoed by the Governor.[25]

As a key backdrop, the California Constitution explicitly furnishes a right to privacy that restricts both private and public actors by conveying "inalienable rights," including "pursuing and obtaining safety, happiness, and privacy."[26] In addition, the California Supreme Court issued two opinions in the 1970's that specifically rejected the United States Supreme Court's "third-party doctrine," under which the Court had found no reasonable expectation of privacy, and therefore no Fourth Amendment protection, in business records and telephone numbers dialed.[27] In contrast, the California Supreme Court held that people do not forfeit their reasonable expectations of privacy by using third parties to store their records.[28] California's highest court determined that information sufficient to form a "virtual current biography" is subject to a reasonable expectation of privacy and California constitutional protection.[29] Because a list of telephone numbers could create such a virtual current biography,[30] the Court found a California constitutional right to privacy in an early form of metadata.[31]

Before California courts could apply those fundamental privacy protections to newly evolving communications technologies, California voters passed the Right to Truth in Evidence Initiative in 1984.[32] This initiative amended the California Constitution to prohibit California courts from using

25. *See supra* notes 16–17.

26. CAL. CONST. art. I, § 1 (1982).

27. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979); United States v. Miller, 425 U.S. 435, 443 (1976); *see also generally* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) (discussing the third-party doctrine); Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431 (2014) (same).

28. *See* People v. Chapman, 36 Cal. 3d. 98, 109 (1984), *abrogated on other grounds by* People v. Palmer, 24 Cal. 4th 856 (2001) (requiring a search warrant for police access to a person's name, phone number, and address when unlisted by a telephone company); People v. Blair, 25 Cal. 3d 640, 653–54 (1979) (protecting telephone numbers); Burrows v. Superior Court, 13 Cal. 3d 238, 243 (1974) (protecting bank records).

29. *Burrows*, 13 Cal. 3d at 247; *see also Blair*, 25 Cal. 3d at 652. The California Supreme Court in *Blair* did not require a warrant per se, but it reversed a denial of the defendant's motion to suppress a log of telephone numbers and explained the need, under California law, for "a judicial determination that law enforcement officials were entitled thereto." *Id.* at 655.

30. *Burrows*, 13 Cal. 3d at 247.

31. *See Blair*, 25 Cal. 3d at 652*; see also* White v. Davis, 13 Cal. 3d 757 (1975) (recognizing that government access to electronic communications, location data and metadata implicate rights of free expression and free association).

32. CAL. CONST. art. I, § 28(f)(2).

California law to grant suppression remedies to criminal defendants.[33] After 1984, a California judge could not grant a suppression remedy based on the California Constitution's protection of the telephone numbers dialed and disclosed by pen registers because the Fourth Amendment does not offer that protection.[34] Stated another way, since 1984 a California court may grant a suppression remedy based on California law only when the California legislature has passed, by at least a two-thirds majority, a new statute specifically permitting suppression.[35]

Before CalECPA, California statutory law had little to say about California government entities obtaining access to electronic communication information from California corporations. Besides California's Wiretap Act,[36] and its Reader Privacy Act,[37] California's statutory scheme was incomplete and rather odd.[38] California statutory law required a warrant for law enforcement access to communications in a patchwork of scenarios.[39] For example, it required that California law enforcement agents obtain a warrant before obtaining information held by out-of-state companies and that out-of-state law enforcement agents obtain a warrant to obtain information from in-state companies.[40] Regarding in-state law enforcement demands for information from in-state companies, however, California statutes required a warrant only for information associated with a small subset of crimes in a narrow set of contexts.[41] Promoters of CalECPA argued that, for much of the information

33. *Id.*

34. *See* 69 Ops. Cal. Att'y. Gen. 55, 55 (Cal. A.G. 1986) (opining that a search warrant could be used to authorize pen registers); 86 Ops. Cal. Att'y. Gen. 198, 198 (Cal. A.G. 2003) (clarifying that the federal pen register statute did not require adequate judicial review to authorize pen registers in California).

35. CAL. CONST. art. 1, § 28(f)(2).

36. CAL. PENAL CODE § 629.50 (West 2011); *see* Memorandum from the Cal. L. Revision Comm'n, State and Local Agency Access to Customer Information from Communication Service Providers: California Wiretap Statute and Related Law 8–17 (Oct. 1, 2014), www.clrc.ca.gov/pub/2014/MM14-50.pdf [http://perma.cc/C8GY-4AAK] [hereinafter CLRC MEMORANDUM 2014-50] (describing California's Wiretap Act, which closely parallels federal law).

37. *See* Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

38. CLRC MEMORANDUM 2014-50, *supra* note 36, at 18 (describing California's "fragmented statutory approach to government access to stored communications" and noting that it "has produced some odd inconsistencies").

39. *See id.* at 17–19.

40. CAL. PENAL CODE §§ 1524.2(b), 1524.3(a) (West 2017) (restricting affected companies to electronic communication services and remote computing services, as defined under federal law).

41. *See* CLRC MEMORANDUM 2014-50, *supra* note 36, at 18. The Commission discussed an identity theft statute requiring a warrant to request certain information associated with certain misdemeanor property crimes and certain crimes involving fraud or embezzlement,

CalECPA covers, Californians were left with a privacy right that lacked an effective enforcement remedy.[42]

B. FEDERAL LAW

In the period preceding CalECPA's passage, federal law operated similarly to California law in that it promised, or at least suggested, rights without effective remedies. Just a few years before CalECPA's passage, however, the Supreme Court affirmed electronic communications privacy claims in two important cases that strengthened the case for CalECPA. The Court considered GPS tracking to be a Fourth Amendment search in *United States v. Jones*,[43] and recognized enhanced privacy interests in cell phone contents in *Riley v. California*.[44] Both decisions had rejected precedents decided before the advent of powerful new communications technologies as inapplicable in modern times.[45] In that way, the Supreme Court supported the need for specially-tailored legislation like CalECPA. The Sixth Circuit's *Warshak* decision further supported electronic communications privacy by requiring a warrant before law enforcement agents may compel service providers to disclose the emails they store.[46]

At the same time, the Court has so constrained the availability of the suppression remedy in Fourth Amendment cases that many victims of unlawful searches have little incentive to challenge the constitutionality of warrantless practices. For example, the Sixth Circuit applied the Court's "good faith" doctrine to refuse to suppress more than 9,000 emails obtained without a warrant in violation of the *Warshak* defendant's Fourth Amendment rights.[47]

---

but noted that "staff could not find any California statute governing a search warrant issued by a California court for service on a California corporation." *Id.*

42. *See* Shahid Buttar, *California Leads the Way in Digital Privacy*, ELEC. FRONTIER FOUND. (Oct. 21, 2015), https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy [http://perma.cc/F8KV-SYH9]; Nicole A. Ozer, *California Is Winning the Digital Privacy Fight*, TECHCRUNCH (Nov. 7, 2015), http://techcrunch.com/2015/11/07/california-now-has-the-strongest-digital-privacy-law-in-the-us-heres-why-that-matters/ [http://perma.cc/VRL6-Z8LT].

43. 565 U.S. 400, 400 (2012) (finding long-term GPS tracking for an ordinary criminal investigation to be a Fourth Amendment search).

44. 134 S. Ct. 2473 (2014) (rejecting the search-incident-to-arrest exception to the warrant requirement for cell phone searches).

45. *See, e.g.*, *Jones*, 565 U.S. at 408–09; *id.* at 430–31 (Alito, J., concurring); *Riley*, 134 S. Ct. at 2484–91.

46. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). Even outside of the Sixth Circuit, major providers like Facebook, Google, Microsoft and Yahoo! require a warrant for access to email contents on the basis of *Warshak*. *See Who Has Your Back? Government Data Requests 2016*, ELEC. FRONTIER. FOUND., https://www.eff.org/who-has-your-back-2016 [http://perma.cc/9B5Z-2THA] (last visited Mar. 23, 2018).

47. *Warshak*, 631 F.3d at 282.

Similarly, the district court, on remand, denied the *Jones* defendant's suppression remedy, using an expansive application of the good faith doctrine.[48] While the Court held in *Riley* that the search-incident-to-arrest exception to the warrant requirement does not apply to cell phone searches, the Court nonetheless affirmed that exigent circumstances may still excuse the lack of warrant.[49] Reports are that, despite *Riley*, at least some law enforcement agents seize phones incident-to-arrest without a warrant and use forensic devices to offload their contents, because they consider the arrest context consistently to present the risk of data loss—an exigent circumstance.[50] Moreover, the Supreme Court has not yet addressed Fourth Amendment regulation of other means of gaining access to cell phones or other devices, such as the increasing use of cell phone simulators, or StingRays.[51]

Prior to CalECPA, federal courts left location data, an area of great concern to CalECPA's proponents, ambiguously or completely unprotected.[52] Federal appellate courts remain split on whether to require a warrant for location information stored with service providers. Most recent decisions have come out opposing such a requirement, although they have considered only a subset of location data and often assumed that it was not particularly revealing.[53] Meanwhile, the Supreme Court has indicated a concern for location

48. United States v. Jones, 908. F. Supp. 2d 203, 214–15 (D.D.C. 2012); Susan Freiwald, *The* Davis *Good Faith Rule and Getting Answers to the Questions* Jones *Left Open*, 14 N.C. J.L. & TECH. 341, 370 (2013). The Supreme Court's *Jones* decision, in fact, did not explicitly require a warrant or even probable cause for GPS tracking, which left the door open for arguments that the information could be acquired by satisfying a lower procedural hurdle like reasonable suspicion. *See id.* at 348–49.

49. *Riley*, 134 S. Ct. at 2494–95.

50. These reports are based on the author's conversations with those who have knowledge of law enforcement practices. Even though agents may not view the data until they obtain a warrant, the approach seems at odds with the Supreme Court's suggestion in *Riley* that placing a phone in a Faraday bag should suffice to protect against loss of data until a warrant may be obtained. *Id.* at 2487.

51. *See generally* Brian L. Owsley, *Triggerfish*, *Stingrays*, *and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134 (2013) (describing increasing use of StingRays in investigations).

52. The Supreme Court is considering the case of *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017), during the 2017 term. That case concerns whether the acquisition of historical cell site location data is a Fourth Amendment search and offers the Supreme Court the opportunity to clarify the question. The Sixth Circuit held that the compelled disclosure of that data from a provider is not a Fourth Amendment search. *Id.* at 887–90.

53. *See, e.g.*, United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (finding no reasonable expectation of privacy in limited set of location-data records); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (same). *But see In re*

data privacy,[54] without addressing it directly, and federal district courts in California have required a warrant when law enforcement agents compel the disclosure of cell site location data from providers.[55] Federal courts have withheld protection entirely from other types of metadata, following the same interpretation of the third-party doctrine that led them to withhold protection from location data.[56] As previously described, California does not interpret its own Constitution as subscribing to the third-party doctrine.[57]

As for federal statutory protection, CalECPA's proponents found ECPA to be outdated, incomplete, and ineffective.[58] As Part IV elaborates, ECPA requires a warrant for only a small subset of investigations and provides much weaker protections—or no protections at all—for the rest. Even when it does offer other protections, ECPA provides no suppression remedy, though it

---

Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3rd Cir. 2010) (rejecting application of the third-party doctrine to location data and leaving the statutory question of the need for a warrant open for magistrate judges to determine).

54. *See, e.g.*, *Riley*, 134 S. Ct. at 2490 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

55. *See, e.g.*, United States v. Williams, 161 F. Supp. 3d 846 (N.D. Cal. 2016) (granting motion to suppress cell site location information obtained using an improper warrant*)*; *In re* Application for Telephone Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) (rejecting application of the third-party doctrine and requiring a warrant for law enforcement access to historic location data); *see also* United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (following the Supreme Court's reasoning in *Riley* and refusing to rely on outdated precedents to regulate newly intrusive investigative methods, but applying the good faith exception to deny suppression).

56. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (finding no Fourth Amendment search when agents obtained "the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account"). *But see Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring) (expressing doubt about use of the third-party doctrine in modern communications context); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (rejecting the application of traditional third-party doctrine to the NSA's telephone metadata program).

57. *See supra* note 28 and accompanying text. The court in *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) required a warrant for access to historical location data and found reasonable expectations of privacy in the data based in part on the California Constitution. The court explained, "there is little doubt that the California Supreme Court's holding [in *Blair*] applies with full force to the government's application here, which seeks historical [location data] generated by a target cell phone's every call, text, or data connection, in addition to any telephone numbers dialed or texted." *Id.* at 1025. The court distinguished prior federal appellate decisions that found no warrant required for compelled location data. *Id.* at 1029.

58. *See* Jadzia Butler, *Eureka! More State "Laboratories of Democracy" Catalyze ECPA Reform*, CTR. FOR DEMOCRACY & TECH BLOG (Jan. 20, 2016), https://cdt.org/blog/eureka-more-state-laboratories-of-democracy-catalyze-ecpa-reform/ [http://perma.cc/N7MR-QNAN]; Ozer, *supra* note 42.

does offer civil damages that CalECPA does not.[59] Importantly, ECPA generally dispenses with notice when stored communications are involved, which may leave victims of unlawful acquisition or interception of their stored electronic communications in the dark.[60] One large company recently brought a First Amendment challenge to ECPA's indefinite nondisclosure orders, arguing that they prevented the company from discussing how the government conducted its investigations of customers' data.[61] Some bills to amend ECPA have gained traction, but they have merely clarified that the warrant requirement applies to the content of all electronic communications obtained from service providers.[62] They have not expanded the warrant requirement to cover other types of data nor addressed ECPA's other deficiencies such as the lack of a notice requirement and a suppression remedy.[63]

ECPA does set a floor upon which state statutes may enact more privacy-protective provisions.[64] Other states had already done so, though none in as comprehensive a fashion as CalECPA. For example, prior to CalECPA, several states had required a warrant for law enforcement access to all types of stored communications contents.[65] Several had required a warrant for law

59. 18 U.S.C. §§ 2707, 2708, 2712 (2012).

60. *See infra* Section IV.B.3 (explaining that notice is required only when content is acquired without a warrant, but not when a warrant is used or when non-content is acquired). Victims may learn of unlawful interceptions if they are charged with a crime, and the prosecutor discloses the evidence to them and reveals how it was obtained. *But see* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 208–16 (2009) (describing the substantial number of investigations under ECPA that do not lead to criminal charges, thus no notice to targets).

61. *See* Microsoft Corp. v. United States, 233 F. Supp. 3d 887, 899–900 (W.D. Wash. 2017). The court denied the government's motion to dismiss because Microsoft had alleged facially valid First Amendment claims. *Id.* at 904–12.

62. *See* Email Privacy Act of 2017, H.R. 387, 115th Cong. (2017); Email Privacy Act of 2015, H.R. 699, 114th Cong. (2015).

63. *Id.*

64. *See* Memorandum from the Cal. Law Revision Comm'n, State and Local Agency Access to Customer Information from Communication Service Providers: Electronic Communications Privacy Act of 1986 at 44 (Aug. 21, 2014), http://www.clrc.ca.gov/pub/2014/MM14-33.pdf [https://perma.cc/Y2CX-LBZP] [hereinafter CLRC MEMORANDUM 2014-33] (reviewing legislative history and precedents and concluding that federal law "leaves room" for a statute like CalECPA); *see also* 18 U.S.C. § 2703(d) (2012) ("In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such state.").

65. *See, e.g.*, TEX. CODE CRIM. PROC. ANN. art. 18.02, 18.20, 18.21 (West 2015) (requiring a warrant for electronic and wire communications content); MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-04 (West 2014) (same).

enforcement access to stored location data,[66] and some had required a warrant for access to electronic device information.[67] As of CalECPA's passage, however, no other state statute covered as many categories as comprehensively.[68]

C. CALECPA'S PASSAGE

CalECPA's proponents sought to bring clarity and uniformity to California law and to update it for the electronic age.[69] They argued that other states were leaving California behind by updating their laws to account for law enforcement acquisition of location data.[70] By increasing the types of information subject to judicial oversight, CalECPA would help ensure that law enforcement agents would not acquire, store, or potentially share more revealing electronic communication information than needed to investigate crimes and secure public safety. CalECPA would assure Californians that their use of essential modern technologies would be free from unjustified government surveillance.[71] At the same time, CalECPA would provide for emergencies and other means to accommodate important government interests and also to spur innovation.

---

66. *See, e.g.*, ME. REV. STAT. tit. 16, § 648 (West 2017) (requiring a warrant for access to "location information of an electronic device"); N.H. REV. STAT. ANN. § 644-A:2 (2015) (same).

67. *See* UTAH CODE ANN. § 77-23c-102(1)(b) (West 2016) (requiring a warrant to "use, copy, obtain, or disclose . . . the location information, stored data, or transmitted data of an electronic device"); VA. CODE ANN. § 19.2-70.3(K) (2011) (requiring a warrant for law enforcement use of a "device to obtain electronic communications or collect real-time location data from an electronic device"). A few states have recently enacted laws requiring a warrant to use cell site simulator devices like StingRays. *See, e.g.*, Wash. Rev. Code Ann. § 9.73.270 (West 2016). In addition, the Justice Department under President Obama announced a new policy under which the devices may not be used without a warrant, and the information they collect must be limited. U.S. DEP'T OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/V3ZK-FS2T].

68. Only two arguably require a warrant for metadata. *See* UTAH CODE ANN. §§ 77-23c-102(1)(a) (West 2016) (covering both location data and stored and transmitted data more generally); TEX. CODE CRIM. PROC. ANN. art. 18.21, § 4 (West 2015) (requiring a warrant for access to "electronic customer data" other than records that reveal a customer's identity or his use of the applicable service). Neither of those laws provides a suppression remedy.

69. *See* CAL. S. COMM. ON PUB. SAFETY, BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 7–8 (2015), http://spsf.senate.ca.gov/sites/spsf.senate.ca.gov/files/sb_178_analysis.pdf [https://perma.cc/87G5-LLAS]. S.B. 178 was the bill that became CalECPA.

70. *See* CAL. ASSEMB. COMM. ON PRIVACY & CONSUMER PROT., BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 4 (2015), http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_cfa_20150619_152455_asm_comm.html [https://perma.cc/UXS2-X9KP].

71. *See id.* at 3–4.

A small group of privacy activists from the American Civil Liberties Union (ACLU) of Northern California and the Electronic Frontier Foundation (EFF) advised the bill's sponsors, Senators Leno and Anderson. As cosponsors, they assisted with the drafting of CalECPA, the preparation of support documents, and the coordination of the communications and lobbying efforts.[72] Throughout the more than year-long process to make CalECPA a law, the sponsors and their advisors also received substantial support from a broad coalition of private and public enterprises.

CalECPA reflects its proponents' concern about the increase in law enforcement acquisition of electronic communications data for investigations.[73] In support letters, technology companies complained that current law was not providing enough certainty to build trust among their cloud customers.[74] Companies were likely especially interested in establishing the security of their customer data after the Snowden revelations about massive government surveillance for foreign intelligence purposes called that security into question.[75] Civil society organizations and journalists complained that the inadequate protection of electronic communication information

72. I was also a member of the small group of advisors on the bill's policy and language teams, as explained in the first footnote containing my author description. Staff members from the Center for Democracy and Technology also advised the bill's sponsors and the California Newspapers Associations was an additional official cosponsor.

73. *See, e.g.*, *S.B. 178 Fact Sheet*, ACLU OF N. CAL. (Sept. 2, 2015), www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_0.pdf [https://perma.cc/8HF7-76FV] (reporting that Google had experienced a 250% jump in government demands for information in "the last five years" and that AT&T experienced a 70% increase in government demands for location data in 2014—totaling more than 64,000 demands).

74. *See California's Electronic Communications Privacy Act – S.B. 178*, ELEC. FRONTIER FOUND. (Oct. 2015), https://www.eff.org/cases/californias-electronic-communications-privacy-act-calecpa [http://perma.cc/3XFW-7TQL] (posting support letters from sponsoring companies such as Adobe Inc., Airbnb, Apple, Dropbox, Facebook, Foursquare, Google, LinkedIn, Microsoft, Mozilla, Namecheap, Reddit, Snapchat and Twitter). Business organizations such as the California Chamber of Commerce, Small Business California, and the Internet Association also supported the bill. *Id.*

75. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 11:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/NR3V-CX3Z]. *See generally* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf [https://perma.cc/CKD4-FEF3] (discussing one of the programs that Mr. Snowden's disclosures made public); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), https://www.pclob.gov/library/702-Report.pdf [https://perma.cc/M7KT-9558] (discussing the other program).

chilled non-mainstream views and sources' speech.[76] Additionally, criminal defense organizations supported the bill's enhanced procedural protections.[77]

Somewhat unexpectedly, given their previous opposition to similar, though more modest, bills,[78] several major law enforcement groups ended up withdrawing their opposition to CalECPA, notwithstanding its ambitious scope and aggressive terms.[79] Some involved in the legislative process credited the lack of law enforcement opposition as being a key factor in the Governor's decision to sign CalECPA into law.[80] Law enforcement groups, for their part, credited the sponsors' responsiveness to law enforcement concerns in explaining the withdrawal of their opposition.[81] Over the course of several negotiated drafts of the bill, the sponsors made concessions to address law enforcement's needs.[82] For example, the sponsors amended the bill's consent

76. *See* Mark Leno & Joel Anderson, *California Electronic Communications Privacy Act (CalECPA) – S.B. 178*, ACLU OF N. CAL. (May 2017), https://www.aclunc.org/our-work/legislation/calecpa [https://perma.cc/T98L-MKGW] (listing support from such organizations as Asian Americans Advancing Justice, Centro Legal de la Raza, Council on American-Islamic Relations and the National Center for Lesbian Rights).

77. *Id.* (listing support from such groups as: California Attorneys for Criminal Justice, California Public Defenders Association, and Citizens for Criminal Justice Reform). Groups supporting online civil liberties such as Tech Freedom, New America: Open Technology Institute, and the Internet Archive also supported the bill. *Id.*

78. The California Sheriffs', District Attorneys' and Police Chiefs' associations had all opposed the predecessor to CalECPA, S.B. 467. *See* CAL. S. RULES COMM., BILL ANALYSIS, S.B. 467, 2013–2014 Leg., Reg. Sess., at 4 (2013), www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0451-0500/sb_467_cfa_20130910_003407_sen_floor.html [https://perma.cc/RM7D-KFXB]. The California District Attorneys and Sheriffs had also opposed S.B. 1434. *See* CAL. S. RULES COMM., BILL ANALYSIS, S.B. 1434, 2011–2012 Leg., Reg. Sess., at 4 (2012), http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_cfa_20120525_102616_sen_floor.html [https://perma.cc/XCH6-72J9]; *see also supra* notes 16–17.

79. The California Sheriffs', District Attorneys' and Police Chiefs' associations all eventually came out as neutral on S.B. 178, with the San Diego Police Officers' Association even coming out in support. Several law enforcement groups withdrew their previous opposition to the bill over the course of negotiated amendments. Still, a few local law enforcement groups and the California Correctional Peace Officers Association remained opposed to the bill. *See* CAL. S. RULES COMM., BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess. (2015), http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_cfa_20150909_094155_sen_floor.html [https://perma.cc/RGX3-NEZL].

80. This is based on my conversations with coalition members.

81. *See, e.g.*, Letter from Alan Wayne Barcelona, President, Cal. Statewide Law Enf't Ass'n., to Mark Leno, Senator, Cal. State Senate (Aug. 10, 2015), https://www.eff.org/document/california-statewide-law-enforcement-association-removes-opposition-sb-178-calecpa [https://perma.cc/6X6A-EPGU] (concluding that, after negotiations, CalECPA "is much closer to striking the appropriate balance between privacy concerns related to electronic communication, and the ability of law enforcement to effectively do its job keeping the public safe").

82. *See, e.g.*, CAL. PENAL CODE § 1546.1(c)(8) (West 2017) (permitting warrantless electronic device access in some correctional facilities in some circumstances). This section

provisions to facilitate online undercover investigations and added some specific exceptions to coverage during the legislative process.[83] But even with those concessions, as later Sections elaborate, CalECPA stands as an immensely privacy-protective statute.

CalECPA passed through the public safety committees with much legislative support.[84] The bill had to shed its detailed reporting requirements when it got to the Senate Appropriations Committee.[85] Those provisions would have facilitated study of the use and efficacy of new surveillance methods by requiring reports on the number and types of investigations conducted, the amount of information received, the number of users affected, the extent of information sharing, and other factors.[86] The committee determined that the record-keeping needed to permit government reporting would cost the state too much money.[87]

The bill faced some opposition on the floor of the Assembly. Protect.org, an advocacy group dedicated to protecting children from harm, opposed the bill on the ground that it would inhibit online investigations of child pornographers and other child predators.[88] The group marshaled considerable late-breaking support from lawmakers, which jeopardized getting the two-

was added to the September 4, 2015 version of the bill after it was introduced. *See also id.* § 1546.1(g)(3) (permitting government entities to retain voluntarily disclosed information pertaining to child pornography). This section was added to the August 28, 2017 version of the bill after it was introduced.

83. *See infra* Section III.C.4; *see also Can Californians' Privacy Be Protected in a Wired World?*, L.A. TIMES (Sept. 3, 2015, 5:00 AM), http://www.latimes.com/opinion/editorials/la-ed-privacy-20150903-story.html [https://perma.cc/WJ62-WM8X] (opining that the opposition's "legitimate concerns appear to have been addressed by the earlier amendments").

84. S.B. 178 passed the Senate Public Safety Committee 6 to 1, and the Assembly Public Safety Committee 5 to 0 with 2 abstentions. *S.B. 178 Privacy: Electronic Communications: Search Warrant (2015–2016)*, CAL. LEGISLATIVE INFO., https://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill_id=201520160SB178 [https://perma.cc/5GRD-SH4R] (last visited Mar. 26, 2018).

85. *See* CAL. S. COMM. ON APPROPRIATIONS, BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 2–5 (2015), https://www.eff.org/document/senate-appropriations-committee-sb-178-analysis [https://perma.cc/9WW3-2HZA].

86. *See* S.B. 178, 2015–2016 Leg., Reg. Sess. § 1546.6 (Cal. 2015).

87. CAL. SENATE COMM. ON APPROPRIATIONS, supra note 85, at 5 (finding that the data collection and reporting activities required "could result in major one-time and ongoing costs, potentially in the tens of millions of dollars annually").

88. *See PROTECT Analysis of S.B. 178, as Passed by the California Assembly, 9/8/15*, PROTECT (Sept. 9, 2015), http://protect.org/178 [https://perma.cc/XUE8-XZGJ].

thirds votes needed.[89] CalECPA's proponents ultimately prevailed in the legislature.[90] One month later, the Governor signed the bill into law.[91]

III. CALECPA'S PROVISIONS

Under CalECPA, and subject to limited exceptions, government entities in California must obtain a circumscribed warrant before they may compel the disclosure of electronic communication information from service providers or obtain such information directly from electronic devices. CalECPA provides both mandatory and discretionary means for judges to confine warrants to relevant information, and it provides for the sealing or destruction of irrelevant information collected pursuant to those warrants. It requires notice to the target, even in emergencies and even when the targets may not be identified, although notice may be delayed in some cases. CalECPA permits a variety of challenges to investigations conducted under it and affords a suppression remedy to successful challengers. The following Sections discuss CalECPA's provisions in more detail.[92]

A. WHO AND WHAT DATA IS PROTECTED?

1. Who Is Protected?

CalECPA protects those whose "service providers" hold their "electronic communication information."[93] Under CalECPA, "service provider" "means a person or entity offering an electronic communication service."[94] The statute defines an electronic communication service broadly to include "a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information."[95] Including those who merely act as intermediaries or store electronic communication information makes the

89. This is from the author's memory while working on the statute.

90. S.B. 178 passed the Senate by a vote of 34 to 4, with 2 abstentions, and passed the Assembly by a vote of 57 to 13 with 10 abstentions. CAL. LEGISLATIVE INFO., *supra* note 84.

91. *See* Zetter, *supra* note 2. In my view, the bill's opponents lost because they objected to the bill as a whole rather than offering tailored exceptions that would not gut the bill. Because there was so much support for at least some reform, blanket opposition did not carry the day.

92. The organization of this Section generally follows that used by Lothar Determann in his book on California privacy law. *See generally* DETERMANN, *supra* note 23. I am indebted to him for his expertise and practical wisdom.

93. CAL. PENAL CODE § 1546.1(a)(1) (West 2017).

94. *Id.* § 1546(j).

95. *Id.* § 1546(e).

definition particularly broad.[96] CalECPA service providers thus include cloud storage services such as Dropbox, social media sites such as Facebook, and traditional email providers like Google (Gmail). While the expansiveness of CalECPA's coverage establishes that it should sweep more broadly than federal law by covering much more than traditional communication providers, the outer boundary of CalECPA's service provider category and hence its coverage, remains unclear.[97]

CalECPA also protects those whose information is obtained directly from their devices rather than (or in addition to) from their service providers. CalECPA regulates law enforcement methods that target an electronic device, defined as "a device that stores, generates, or transmits information in electronic form."[98] CalECPA's device provisions are much more detailed than the few other device-access provisions that other states had previously passed.[99]

2. What Is Protected?

CalECPA imposes its warrant scheme on government entities' access to two types of information: electronic communication information and electronic device information, collectively called "electronic information."

Electronic communication information includes "any information about an electronic communication or the use of an electronic communication service."[100] This definition encompasses electronic communications content information, associated metadata, and location data.[101] It also explicitly includes IP addresses.[102] CalECPA's use of technologically-neutral language makes it forward looking; any device can generate electronic communication information. Its broad terms will allow the category of information investigated to expand as techniques of identification grow, such as through

96. This definition can be compared to the analogous definitions of service provider under federal law, *see infra* notes 211–213, which do not include those who act as intermediaries or store information.

97. *See infra* Section V.A (discussing the ambiguity of CalECPA's definition of "service provider").

98. CAL. PENAL CODE § 1546.1(a)(2)–(3) (West 2017); *id.* § 1546(f).

99. *See* UTAH CODE ANN. § 77-23c-101 (West 2016); TEX. CODE CRIM. PROC. ANN. art. 18.21 (West 2015). Federal law lacks a device provision.

100. CalECPA defines an electronic communication as "the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system." CAL. PENAL CODE § 1546(c) (West 2017). CalECPA's definition closely tracks the federal version. 18 U.S.C. § 2510(12) (2012).

101. CAL. PENAL CODE § 1546(d) (West 2017).

102. *Id.* Section V.A also discusses the ambiguity of the content of electronic communications, particularly IP addresses.

biometrics. As mentioned, CalECPA subjects all the information included in this category, and the next, to the same tailored warrant requirement.

The second type of information CalECPA protects, electronic device information, includes information that a person has stored on their device as well as information that is generated through use of that device.[103] Presumably, much of what will be stored on a person's electronic device will be electronic communication information, but "electronic device information" may include more than electronic communication information. Individual photos, videos, and other information that may not be associated with a particular electronic communication would still be considered to be electronic device information when stored on a person's device. Similarly, information that a cell phone generates about its location does not have to be associated with a particular communication to be protected electronic device information.[104] Device identification numbers should also be included in this category.[105]

3. What Is Not Protected?

CalECPA explicitly excludes "subscriber information" from the definition of electronic communication information; government entities do not need a CalECPA warrant to compel the disclosure of subscriber information from service providers.[106] CalECPA defines subscriber information as:

> [T]he name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.[107]

CalECPA explicitly preserves government entities' existing authority to use administrative, grand jury, trial, or civil discovery subpoenas to obtain subscriber information.[108]

103. CAL. PENAL CODE § 1546(g) (West 2017).

104. *See also* Liebeskind, *supra* note 4 (suggesting that electronic device information includes information obtained from an IMSI catcher, or a cell site simulator device like a StingRay).

105. CAL. PENAL CODE § 1546(g) (West 2017) (including in "electronic device information" any information "stored on . . . an electronic device").

106. *Id.* § 1546(d).

107. *Id.* § 1546(*l*). *See infra* Section III.C.3 (comparing the information that may be obtained with a subpoena under CalECPA with that which may be obtained with a subpoena under ECPA).

108. CAL. PENAL CODE § 1546.1(i)(3) (West 2017).

CalECPA's exclusion of subscriber information from its warrant requirement reflects the understanding that such information does not change over time as do other types of electronic communication information. Because subscriber information is "static information," its acquisition by the government requires less judicial oversight than the acquisition of information that reveals someone's activities over a period of time.[109] Compared to the latter, static information is less likely to implicate intimate activities, or activities that reflect First Amendment values of speech and association. Further, as a practical matter, law enforcement agents need to have some investigative building blocks that they can obtain without having to establish probable cause. Subscriber information constitutes that type of building block that can establish probable cause for a warrant for access to more revealing and protected information.

B. WHO MUST COMPLY?

CalECPA casts a large net by imposing a warrant requirement on the acquisition of information by "government entit[ies]," which includes both state agencies and individuals within those agencies.[110] By its terms, CalECPA regulates not just police, but everyone involved in the criminal justice system—from prosecutors to sheriffs to probation officers.[111] Its language also covers searches by public school and hospital officials and other government agency employees who use one of CalECPA's covered methods.

CalECPA's purposeful limitation significantly reduces the statute's reach, however. Notably, CalECPA does not impose its warrant requirement when a government entity compels the disclosure of electronic information for purposes other than "investigating or prosecuting a criminal offense."[112] In other words, outside of criminal investigations, when it comes to compelled disclosures, CalECPA permits the use of subpoenas to the extent permitted by

109. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 163 (discussing static information).

110. CAL. PENAL CODE § 1546(i) (West 2017) (defining "[g]overnment entity" as "a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof").

111. *Id.*

112. *Id.* § 1546.1(b)(4) ("A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device . . . [p]ursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense.").

other law.[113] That means that a host of administrative inquiries and investigations will continue to proceed under subpoena regulations not specified in CalECPA.[114] Though this limit is based on the purpose of the investigation and not on who conducts it, in practice it will reduce the type and number of government entities subject to CalECPA's warrant requirement.[115]

CalECPA's broad coverage led to numerous calls for exclusions. As passed, CalECPA contained only one categorical exclusion: it explicitly permitted prison officials to access electronic device information directly from devices seized in prisons, where it is illegal for inmates to have devices.[116] The Governor signed into law a bill including some amendments to CalECPA in September of 2016.[117] That bill made minor adjustments to the law and added additional carve-outs from coverage pertaining to probationers and parolees, and to the location information associated with "911" emergency calls.[118]

C. HOW TO COMPLY?

The following Subsections lay out the different investigative methods subject to CalECPA's warrant requirement and describe the circumscribed warrants CalECPA requires. The discussion then elaborates on those investigative methods that do not require a CalECPA warrant, either because they are explicitly excluded or because they involve voluntary disclosures, consent, or emergencies. Finally, the last Subsection describes CalECPA's comprehensive notice requirements.

1. Warrant-Regulated Methods

CalECPA effectively regulates by investigative method, rather than by the type of information acquired in an investigation.[119] CalECPA subjects three different methods of accessing electronic information to the warrant

113. Use of the subpoena must not be prohibited by other federal or state law, and CalECPA disclaims any intent to expand any subpoena authority under state law. *Id.*

114. *See, e.g.*, CAL. GOV'T CODE §§ 11180, 11181(e) (West 2004).

115. Because CalECPA has incorporated subpoena access into its terms as a method of obtaining electronic information, however, such access will still be subject to CalECPA's remedies if done improperly. *See infra* Section III.D.

116. CAL. PENAL CODE § 1546.1(c)(8) (West 2017) (requiring that the device seized is not known or believed to be in "the possession of an authorized visitor" and that the seizure not otherwise be "prohibited by state or federal law").

117. S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016).

118. CAL. PENAL CODE § 1546.1(c)(9)–(11) (West 2017).

119. This follows the approach suggested by Professors David Gray and Danielle Citron. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013) ("Rather than asking *how much* information is gathered in a particular case, we argue here that Fourth Amendment interests . . . demand that we focus on *how* information is gathered.").

requirement; two involve compelled disclosure from third parties and the third involves direct interaction with an electronic device.

The first type of compelled disclosure that CalECPA subjects to its warrant requirement involves the compelled "production of or access to electronic communication information from a service provider."[120] As mentioned above, government entities have increased their demands for information about customers' electronic communications from service providers such as email providers and cell phone service providers. CalECPA imposes a warrant requirement on such demands and imposes a notice requirement as well.[121]

The second type of compelled disclosure occurs when a government entity compels the "production of or access to electronic device information from any person or entity other than the authorized possessor of the device."[122] Electronic device information includes information that a person has stored on their device as well as information that is generated through use of their device.[123] For example, CalECPA requires a California government entity to obtain a warrant before it may compel a device manufacturer that is not acting as a service provider (such as Apple), to divulge a device's unique device ID (not electronic communication information) to facilitate cracking the device's encryption.[124]

The third investigative method that CalECPA imposes a warrant requirement upon is the direct interaction with an electronic device to gather electronic device information.[125] The warrant requirement applies when the government entity interacts with the device physically, such as by typing commands into a smart phone or computer to obtain information from that device. It also applies when the government entity uses electronic communications to obtain information from an electronic device, for example

120. CAL. PENAL CODE § 1546.1(a)(1) (West 2017).

121. *See infra* Section IV.C.6 (discussing notice provisions).

122. CAL. PENAL CODE § 1546.1(a)(2) (West 2017). *See also infra* notes 142–145 and accompanying text (discussing the justification for the authorized possessor carve out).

123. *See supra* Section III.A.2.

124. *Cf.* Katie Benner & Eric Litchtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html [https://perma.cc/7JK8-UQE5] (describing the standoff resulting from the FBI's demand that Apple help unlock an encrypted iPhone); *In re* Search of an Apple iPhone Seized During the Execution of Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD20, No. ED 15-0451M, 2016 WL 618401, at *1–2 (C.D. Cal. Feb. 16, 2016) (ordering Apple to assist the FBI).

125. CAL. PENAL CODE § 1546.1(a)(3) (West 2017).

by using a StingRay to obtain information from a cell phone or by using a hacking-type method to obtain information from a computer.[126]

2. Warrant Requirements

CalECPA generally prohibits the three investigative methods described in the immediately preceding Subsection, and then specifies the only way those methods may lawfully proceed. In the ordinary course, the investigative method will proceed by way of a CalECPA-specified warrant, to be described. But CalECPA also permits, when applicable, government entities to investigate pursuant to orders under California's Wiretap Act or Reader Privacy Act, both of which provide comparable protections to CalECPA.[127] After amendment in 2016, the law clearly permits access to electronic information by a Pen Register and Trap and Trace Order as well.[128] For simplicity, the rest of this Article will refer to CalECPA as requiring the warrant it specifies even though it also permits use of court orders under these three statutes instead.

When courts issue warrants under CalECPA, they follow CalECPA's additional requirements as well as the standard procedures for warrant applications set forth in California law.[129] The standard procedures require, among other things, that a search warrant be issued only upon a finding of probable cause, supported by an affidavit.[130] CalECPA specifically requires that the warrants it authorizes comply with all other provisions of California and federal law that impose additional requirements on the use of search warrants.[131]

CalECPA further limits the scope of information gathered pursuant to its authority to reduce the risk of unjustified information collection. While

126. *See generally* Pell & Soghoian, *supra* note 51; *see also* Letter from Richard Salgado, Google Inc., to the Judicial Conference Advisory Comm. on Criminal Rules 2 (Feb. 13, 2015), https://assets.documentcloud.org/documents/1670588/13feb2015-google-inc-comments-on-the-proposed.pdf [https://perma.cc/E8KN-NBHH] (describing various ways government entities have proposed obtaining "remote access" to devices).

127. CAL. PENAL CODE §§ 1546.1(b)(1)–(3), (c)(1)–(2) (West 2017); *see also* Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

128. CAL. PENAL CODE §§ 1546.1(b)(5), (c)(12) (West 2017) (permitting government entities to obtain electronic information from service providers and from electronic devices pursuant to pen register or trap and trace orders under California Penal Code section 638.50). The new provisions pertaining to pen register and trap and trace orders repeat several of the provisions in CalECPA, such as the requirements of sealing, notice, and the extensive remedies. *See id.* §§ 638.52, 638.54, 638.55.

129. *Id.* §§ 1546.1(b)(1), (c)(1) (describing the warrant as being "issued pursuant to Chapter 3" of the California Penal Code).

130. *Id.* § 1525.

131. *Id.* § 1546.1(d)(3).

background California law requires that the warrant particularly describe what is to be searched,[132] CalECPA further requires that the warrant specify "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."[133] By specifying additional parameters for its warrants, CalECPA endeavors to cut down on the "all accounts, for all time" orders that have become commonplace with digital searches.[134] Such searches 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.[135]

In a significant innovation, CalECPA further mandates that any information obtained that is "unrelated to the objective of the warrant" be sealed and unavailable without a further court order.[136] A court shall issue such an order only when federal or state law requires it, or when the court finds probable cause to believe the information is relevant to an active investigation.[137] This provision of CalECPA implements the data protection privacy principle that data collectors should specify the purposes for data collection, and precludes uses that are inconsistent with those purposes. It also maintains data quality by limiting the use of irrelevant data.[138] Data protection principles have, historically, found much more traction in Europe than in the United States.[139] CalECPA's introduction of such principles into its law enforcement collection rules moves decidedly away from the notion that all digital information is available for law enforcement use.

---

132. *Id.* § 1525.

133. *Id.* § 1546.1(d)(1). This language was changed slightly in the 2016 amendment. See S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016).

134. *See, e.g.*, Brief of Erwin Chemerinsky et al. as Amici Curiae in Support of the Petition for a Writ of Certiorari at *2, Rindfleisch v. Wisconsin, 136 S. Ct. 128 (2015) (No. 14–1481), 2015 WL 4481305 (citing Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971 (2012)).

135. *See, e.g.*, *In re* Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 6 (D.D.C. 2013) (rejecting the government's overbroad request and issuing more limited search warrant to avoid granting a "general warrant" in violation of the Fourth Amendment's particularity requirement).

136. CAL. PENAL CODE § 1546.1(d)(2) (West 2017).

137. *Id.*

138. *See* ORG. FOR ECON. COOPERATION & DEV., THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES at 21–22 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf [https://perma.cc/8ZFJ-5Q89].

139. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 122 (2017).

Besides requiring more specific warrant descriptions, CalECPA gives judges who issue warrants under it discretion to take other steps to reduce over collection. For example, CalECPA permits such judges to appoint a special master to ensure that only the information needed to achieve the warrant's objective is produced or accessed.[140] After the electronic information has been collected, a judge may, in response to a petition or on her own initiative, require the entity that has obtained the information to destroy any information "unrelated to the objective of the warrant."[141]

3. Exclusions from the Warrant Requirement

CalECPA specifically excludes several methods of obtaining electronic information from its warrant requirement. First, CalECPA does not apply when government entities "compel the production of or access to electronic device information" from the device's "authorized possessor"[142]—either the device's owner or someone the owner has authorized to possess the device.[143] That means agents may use a subpoena or another method to compel a person to disclose information stored on her own smart phone or computer, just as they may similarly compel the disclosure of that person's private papers, diaries, photo albums, and the like.[144] Compulsion directed to a device's authorized possessor falls outside CalECPA's concern because such an order is served directly on the target; having notice, the target can exercise her right to contest the compelled disclosure on constitutional or other grounds.[145] In contrast, CalECPA regulates investigative techniques that may not—without its provisions—require notice to the person whose information is sought, and where the basis for challenge requires the clarification CalECPA provides.[146]

140. CAL. PENAL CODE § 1546.1(e)(1) (West 2017); *see* Liebeskind, *supra* note 4 (noting that law enforcement sometimes refers to the special master as part of a "taint team"). The judge may decide to appoint a special master on her own or she may do so in response to a petition brought by the target or recipient of the order. CAL. PENAL CODE § 1546.1(e) (West 2017). Special masters are already provided for in § 1524(d), to which CalECPA refers.

141. CAL. PENAL CODE § 1546.1(e)(2) (West 2017). To avoid the destruction of exculpatory information, the destruction obligation does not kick in until the government entity has terminated the current investigation and related investigations. *See id.*

142. *Id.* § 1546.1(a)(2).

143. *Id.* § 1546(b).

144. *See, e.g.*, Mintz v. Mark Bartelstein & Assocs., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012).

145. Targets may raise constitutional (First Amendment, Fourth Amendment, Fifth Amendment, state Constitution) and any statutory claim in motions to quash. *See, e.g.*, Bellia & Freiwald, *supra* note 109, at 142 (describing two-step process); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005).

146. For example, the Fourth Amendment protection for location data is uncertain and is not yet established for other forms of metadata. Moreover, CalECPA establishes a

CalECPA requires notice and additional restrictions to protect the targets of investigations who are not as able to protect themselves as those who are directly served with orders for compelled disclosure.[147]

Second, CalECPA permits government entities to use a variety of subpoenas to compel senders and recipients of communications to disclose their electronic communications.[148] The same logic applies to possessors of targeted electronic communications as applies to authorized possessors of targeted devices. Notice will be served directly on the person whose communications are sought and that person—particularly if she is the target of the investigation—can raise claims in response to the demand for disclosure.

Under CalECPA, the party who communicated with the investigation's target and whose communications with the target are disclosed by that target, has no privacy right violated by that disclosure. Presumably, that is based on application of the doctrine that the Fourth Amendment does not prevent a party to the communication from disclosing it to the government.[149] Patricia Bellia and I have argued that the law should distinguish between one's communication partner voluntarily disclosing one's communication, which is a risk one takes, and the government compelling the disclosure of that communication, which is a risk one should not be seen to assume merely by communicating.[150] By excluding from the warrant requirement electronic communication information that the government *compels* a person's communication partner to disclose, CalECPA accepts a broader application of the third-party doctrine than we recommended.[151] CalECPA's provision opens the door not only to a target being compelled to disclose his communications partners' communications, but also to a target's communication partners being

comprehensive statutory suppression remedy for victims of unlawful seizure. *See infra* Section III.D.

147. Although the law of direct digital searches also lacks clarity, it is beyond CalECPA's scope. *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Lily R. Robinton, *Courting Chaos: Conflicting Guidance from the Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311 (2010).

148. CAL. PENAL CODE § 1546.1(i)(1) (West 2017) (permitting subpoenas to "[r]equire an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication").

149. United States v. Charbonneau, 979 F. Supp. 1177, 1184–85 (1997); Hoffa v. United States, 385 U.S. 293, 302 (1966).

150. Bellia & Freiwald, *supra* note 109, at 154.

151. CalECPA's approach does have support in the cases, however. *See id.* at 157; *see also* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 590 (2009) (arguing that agents may compel disclosure from third parties because witnesses can be compelled to testify about anything without Fourth Amendment oversight).

compelled to disclose the target's communications, without the protections of CalECPA or an opportunity for the target himself to raise claims.[152]

In a related application of the third-party doctrine, CalECPA permits government entities to use a subpoena, rather than a warrant, to obtain electronic communication information from some employers. In particular, when an employer uses a company-provided email service, the company can be made to disclose, pursuant to a subpoena, information to which it has access.[153] Existing Fourth Amendment case law supports the idea that an employee has no right to privacy on her employer's server,[154] but a more privacy-protective approach would have recognized that employees should not have to forfeit their privacy just because they use a company email service, particularly as to their private messages.

4. Voluntary Disclosures and Consent

CalECPA entirely excludes from its coverage voluntary disclosures of electronic communication information by recipients of electronic communications.[155] To illustrate, if the subject of an investigation, Alice, sends an email to her friend Bob reporting on her intent to rob a bank, nothing prevents Bob from choosing to disclose to a government entity the contents of Alice's email or any other information about Alice's email that CalECPA would consider to be electronic communication information (including the time or date Bob received the email, Alice's IP address, etc.). The animating principle is that Alice, by communicating with Bob, has assumed the risk that Bob will disclose her communication and information about it to the government.[156]

Service providers can also voluntarily disclose (1) electronic communication information, obviating the need for a warrant, and (2) subscriber information, obviating the need for whatever state law requires for

152. Notice to the target in situations where her communication partners are compelled to provide electronic communication information would have helped with this problem. Early drafts of CalECPA had broader notice provisions.

153. CAL. PENAL CODE § 1546.1(i)(2) (West 2017) (permitting a government entity to "[r]equire an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity").

154. *See, e.g.*, United States v. Simons, 206 F.3d 392, 401–02 (4th Cir. 2000); Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011).

155. CAL. PENAL CODE § 1546.1(a)(3) (West 2017).

156. *See supra* notes 149–152 and accompanying text.

compelled disclosure—presumably a subpoena.[157] CalECPA places two significant limits on these voluntary disclosures. First, they must not otherwise be prohibited by state or federal law.[158] Because ECPA constrains when service providers (as it defines them) may disclose some electronic communication information, CalECPA incorporates those limits.[159] For example, ECPA permits service providers to disclose such information to government entities only with the user's consent, as necessary to render service or to protect the provider's rights or property, and in emergencies.[160]

Second, the government must destroy, within ninety days, any electronic communication information it receives pursuant to voluntary disclosure unless it first (1) obtains the consent of the sender or recipient, (2) obtains a court order, or (3) reasonably believes the information relates to child pornography.[161] These limits on retention of voluntarily-disclosed information significantly constrain the government's ability to exploit voluntary disclosures as end runs around CalECPA's warrant requirements.

Government entities can attain direct access to an electronic device without obtaining a warrant when they get the specific consent of the authorized possessor of the device.[162] The authorized possessor's "specific consent" must be "provided directly to the government entity seeking information," which should rule out government entities' reliance on terms of service—to which the government entity is not a party—to establish consent to search.[163] Specific consent does not require knowledge that one is giving consent to a government entity, so it can be given unwittingly to an

157. CAL. PENAL CODE § 1546.1(f) (West 2017).

158. *Id.*

159. *See* 18 U.S.C. § 2702 (2012). Federal preemption would require that CalECPA not permit disclosure of information when federal law would prohibit it, since ECPA sets a floor on electronic communications privacy protection that the states may not go below. *See supra* note 64 and accompanying text.

160. 18 U.S.C. §§ 2702(b)(3), (c)(2) (2012). A service provider may also disclose contents information to a law enforcement agency if they obtain it inadvertently and it appears to relate to the commission of a crime. *Id.* § 2702(b)(7).

161. CAL. PENAL CODE § 1546.1(g) (West 2017). Before granting an order, the court must ensure either that "the conditions justifying the initial voluntary disclosure persist . . . or there is probable cause to believe that the information constitutes evidence that a crime has been committed." *Id.*

162. *Id.* § 1546.1(c)(3). When the government entity believes in good faith that a device is lost, stolen or abandoned, CalECPA permits that entity to access electronic device information on the device solely to "attempt to identify, verify, or contact the owner or authorized possessor of the device." *Id.* § 1546.1(c)(6). The owner of a device can also give specific consent to search it when the device has been reported lost or stolen. *Id.* § 1546.1(c)(4).

163. *Id.* § 1546(k).

unidentified undercover agent.[164] In addition, one specifically consents to the receipt of an electronic communication by members of the intended audience of that communication, which includes members of a listserv or chat room.[165] This provision facilitates undercover operations such as when an unidentified agent receives evidence of a crime as part of a larger audience.

5. Emergency Provisions

CalECPA does not specifically provide for compelled disclosure orders in emergencies, but service providers can use their good-faith belief that an emergency exists to justify their voluntary disclosure of electronic communication information under federal ECPA.[166] As described above, CalECPA explicitly incorporates ECPA's voluntary disclosure provisions so that such disclosures are not subject to CalECPA's warrant requirement.

CalECPA does contain its own emergency provision for direct access to electronic devices. This provision permits such access without a warrant or other order when a "government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person" requires electronic device information access.[167] CalECPA limits recourse to this provision by using language associated with serious emergencies.[168] Further, within three days of obtaining the information, the government entity must establish before a court sufficient factual support for the claimed emergency.[169] Alternatively, the government entity can file an application for a warrant under CalECPA.[170] If the court does not grant a warrant or approve the emergency disclosures, then the court must order the immediate destruction of all information obtained and provide, if it has not done so already, immediate notice to the target of the disclosure.[171]

6. Notice Requirements

Under CalECPA, the government entity who obtains information via a warrant or an emergency order must furnish notice to the identified targets.[172] Notice must be furnished contemporaneously with the warrant's execution,

164. *Id.*
165. *See id.*
166. 18 U.S.C. § 2702(b)(8) (2012).
167. CAL. PENAL CODE § 1546.1(c)(6) (West 2017) (tracking ECPA's emergency provision language).
168. *Id.* § 1546.1(h).
169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.* § 1546.2(a). Notice may be served by first class mail, email, or other reasonably effective means.

or, in the case of an emergency, within three days of receiving the information.[173] CalECPA requires that the notice include a copy of the warrant and the nature of the compelled or requested information.[174]

Government entities may request from the court a time extension for providing notice and an order prohibiting any party providing information from notifying the target that information has been sought.[175] The court may grant such orders when it finds reason to believe that notifying the target may have an adverse result; however, the order only lasts as long as the adverse result would exist, or up to ninety days, when the order becomes renewable.[176] When the government entity eventually does give notice, CalECPA requires it to furnish to the target a statement of the grounds for the court's determination to grant the delay, along with the information ordinarily required for notice.[177] Additionally, with delayed notice, the government entity must later provide to the target either a copy of all of the electronic information obtained or a summary of that information, including the number and type of records disclosed and the time period covered by such records.[178] These additional requirements serve as a burden on the request to delay notice.

As an interesting innovation, CalECPA requires the same information (basic notice information and additional information in cases of delayed notice) to be provided to the California Department of Justice (CaDOJ) in cases when the target may not be identified.[179] The CaDOJ must publish reports it derives from such information on its website within ninety days of receiving the information.[180] This mechanism provides transparency in investigations such as cell tower dumps and others that involve the collection

173. *Id.*

174. Notice must also state the government investigation under which the information is sought with reasonable specificity. *Id.* For emergency disclosures not involving warrants, the government entity must include a written statement that describes the facts that gave rise to the emergency. *Id.*

175. *Id.* § 1546.2(b)(1). While CalECPA does permit the government entity to request gag orders, it provides no other limitation on any party's ability to disclose information about requests for information. *Id.* § 1546.2(d).

176. *Id.* §§ 1546.2(b)(1)–(2), 1546(a) (defining an "adverse result" to match 18 U.S.C. § 2705(a)(2)). *See* Smith, *supra* note 60 (discussing the problem with indefinite gag orders and delays of notice in the federal system).

177. *Id.* § 1546.2(b)(3).

178. *Id.*

179. *Id.* § 1546.2(c).

180. *Electronic Search Warrant Notifications*, CAL. DEP'T OF JUSTICE, https://openjustice.doj.ca.gov/data [https://perma.cc/5GRU-XVHH] (last visited Mar. 27, 2018). It may redact names, presumably of investigators, and other personal identifying information from the reports.

of information from unidentified targets.[181] That should facilitate the ability of interested parties to monitor the CaDOJ's website for problematic patterns and practices.[182]

D. SANCTIONS AND REMEDIES

CalECPA also provides a statutory suppression remedy. Under its terms, "any 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 [CalECPA]."[183] The new law incorporates procedures already in place under California law for handling suppression motions.[184] California courts have interpreted these provisions not to apply when law enforcement agents violate the pertinent statutes in merely technical ways.[185] But the 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.[186] The real risk that evidence collected will be excluded at trial furnishes government entities with significant incentives to comply with CalECPA's rules on obtaining and retaining information, as the suppression provision explicitly refers to both.

In addition to suppressing unlawfully obtained information, CalECPA permits individuals, service providers, and others involved in investigations to petition the issuing courts to "order the destruction of any information obtained in violation of [CalECPA], or the California Constitution, or the

181. *See, e.g.*, *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 674–77 (S.D. Tex. 2015) (granting an order that compelled seven cell phone service provider to disclose data from cell towers serving a crime scene during the ten minute period that the crime transpired); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013) (arguing that cell tower dumps implicate reasonable expectations of privacy and are not covered by the Stored Communications Act).

182. Unfortunately, reporting provisions present in the early versions of CalECPA that would have furnished even greater transparency had to be dropped during the legislative process because of the expense of compliance. *See supra* notes 85–87 and accompanying text. The New York and New Mexico bills cited above, *supra* note 5, both would require extensive annual reporting of the kind that CalECPA had to drop.

183. CAL. PENAL CODE § 1546.4(a) (West 2016).

184. *Id.* (referring to the procedures in California Penal Code section 1538.5(b)–(q)).

185. *See, e.g.*, People v. Hoag, 83 Cal. App. 4th 1198 (Cal. Ct. App. 2000).

186. *See, e.g.*, United States v. Leon, 466 U.S. 897, 922 (1985). *See generally* TRACEY MACLIN, THE SUPREME COURT AND THE FOURTH AMENDMENT'S EXCLUSIONARY RULE (2013) (describing the origin and gradual erosion of the exclusionary rule).

United States Constitution."[187] Petitioners may also ask the court to void or modify a warrant, order, or other legal process that violates CalECPA.[188]

CalECPA authorizes the Attorney General to bring a civil action to compel any government entity to comply with its terms.[189] The statute does not provide for fines or other damage awards for victims of unlawful investigations. Its terms do not authorize private actions against entities who improperly furnish information to investigators or otherwise assist them. In fact, CalECPA immunizes corporations and their agents from any cause of action for complying with any process issued pursuant to the chapter.[190] Affording such immunity certainly removes one way of deterring noncompliance with CalECPA, but it may have been essential to obtaining the enthusiastic participation of private companies in the CalECPA coalition.[191]

IV. WHAT SETS CALECPA APART FROM FEDERAL LAW

Compared to ECPA, CalECPA requires warrants for more investigations; its warrants impose more restrictive requirements; it provides more notice to targets; and it furnishes more significant remedies. Congress has shown significant support for, but has not yet passed, ECPA reform bills that would move ECPA closer to CalECPA by expanding its warrant requirement to cover the compelled disclosure of all electronic communications content acquired from service providers (as ECPA defines them).[192] But those bills do not close any of the other significant gaps between ECPA and CalECPA nor do they adopt any of CalECPA's other innovative features. Regardless of the proposed reforms, CalECPA still stands head and shoulders above federal law in protecting the privacy of modern communications.

The following provides more detail on the differences between ECPA and CalECPA. The discussion will briefly cover differences between California's Wiretap and Pen Register Acts and their federal analogs before focusing on the differences between CalECPA and the federal Stored Communications Act ("SCA"), which is the second of ECPA's three titles.[193]

187. CAL. PENAL CODE § 1546.4(c) (West 2016).

188. *Id.*

189. *Id.* § 1546.4(b).

190. *Id.* § 1546.4(d).

191. *See infra* Section V.A (discussing the uncertainty about whether companies are truly immune from liability).

192. *See* Email Privacy Act of 2017, H.R. 387, 115th Cong. (2017); Email Privacy Act of 2015, H.R. 699, 114th Cong. (2015).

193. Stored Wire and Electronic Communications and Transactional Records Access, Pub. L. No. 99–508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 USC §§ 2701–09,

A. CALECPA VERSUS FEDERAL WIRETAP AND PEN REGISTER LAW

1. Wiretap Law Differences

The California Wiretap Act is modeled after federal law.[194] A significant difference is that CalECPA makes suppression and other remedies available to victims of improper interceptions of electronic communications, while the federal provisions specifically deny suppression as a remedy for improper investigations of electronic communications.[195]

2. Pen Register Law Differences

Pen registers obtain metadata, such as telephone numbers dialed and addressing information, in real time.[196] Prior to CalECPA, California lacked a specific Pen Register Act.[197] After passage of CalECPA and an amendment to it to reconcile a pen register law that was passed the same year,[198] pen register orders are generally subject to all of CalECPA's requirements and protections, described above, with a few minor modifications.[199] ECPA, by contrast, requires only a rubber-stamp court order based on relevance for investigations that obtain dialing, routing, addressing, and signaling (DRAS) information in

2711–12). ECPA's provisions covering interceptions, or wiretaps, make up its first title and its pen register provisions are located in its third title.

194. CLRC MEMORANDUM 2014-50, *supra* note 36, at 8–17. Note that outside the law enforcement context, California requires two parties to consent for wiretapping to be valid, while federal law requires only one party to consent. *Id.* at 4 (describing other exceptions available under federal law that California law does not recognize).

195. *See* 18 U.S.C. § 2515 (2012) (providing a statutory suppression remedy only for improper interceptions of wire and oral communications). Note that California's Wiretap Act has its own more limited suppression remedy as well as a provision for civil damages subject to good faith reliance. CLRC MEMORANDUM 2014-50, *supra* note 36, at 15–17.

196. *See* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1295 (2005); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949, 982–89 (1996).

197. CLRC MEMORANDUM 2014-50, *supra* note 36, at 19 (noting that pursuant to an opinion of the Attorney General, California law enforcement could use search warrants to authorize pen register and trap and trace investigations).

198. A.B. 929, covering pen registers and trap and trace devices, passed just before CalECPA, which created confusion as to which governed. Assemb. B. 929, 2014–2015 Leg., Reg. Sess. (Cal. 2015). S.B. 1121 and A.B. 1924 passed the next year and reconciled the two laws. *See* S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016). The new provisions require that the magistrate find "the information likely to be obtained . . . is relevant to an ongoing investigation and that there is probable cause to believe that the pen register or trap and trace device will lead to" certain types of evidence. CAL. PENAL CODE § 638.52(b) (West 2016).

199. For example, the pen register provisions permit investigations to last for sixty days, with extensions, and for information to be periodically furnished to the supervising officer. CAL. PENAL CODE §§ 638.52(e), (f), (j) (West 2016). Standard search warrants a void after ten days under California Penal Code § 1534(a).

real-time.[200] ECPA's pen register provisions do not provide for notice to targets but rather provide for automatic sealing of orders and gag orders on providers who install pen registers.[201] ECPA provides no remedies for improper pen register installations, which means no statutory suppression remedy nor even a right to recourse through civil actions exists.[202]

B. CALECPA COMPARED TO THE STORED COMMUNICATIONS ACT (SCA)

1. Who Is Protected?

Like CalECPA, the SCA protects the privacy of those whose electronic communication information is stored with third-party service providers. Unlike CalECPA, however, the SCA does not protect information stored on electronic devices.[203] That leaves law enforcement access to device-stored data—where not regulated by state laws like CalECPA—covered only by the Supreme Court's decision in *Riley v. California*.[204] As discussed in Section II.B, *Riley* applies in the limited context of searches incident-to-arrest; in that context, its exception for exigent circumstances may leave many cell phones and other devices vulnerable to warrantless searches.[205] Outside of the search-incident-to-arrest context, searches conducted solely pursuant to Fourth Amendment law face much uncertainty as to when notice is required, how to particularize the warrant, what remedy is available, and other questions to which CalECPA provides much clearer guidance.

2. What Is Protected and How to Comply

The greatest difference between the SCA and CalECPA lies in their scope. The SCA imposes a warrant requirement on access to only a subset of

200. 18 U.S.C. §§ 3121, 3123 (2012). JAMES CARR & PATRICIA BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE 4:84 (2014) (explaining that the Pen Register Act does not contemplate independent judicial review of orders).

201. 18 U.S.C. § 3123(d) (2012).

202. In theory, the knowingly improper installation or use of a pen register could incur criminal liability. *See* 18 U.S.C. § 3121(d) (2012). It also violates the SCA for a government entity to willfully disclose pen register obtained information outside of official duties. *See id.* § 2707(g). *See* CLRC MEMORANDUM 2014-33, *supra* note 64, at 35.

203. 18 U.S.C. § 2702 (2012).

204. 134 S. Ct. 2473 (2014).

205. *See supra* notes 49–51 and accompanying text (discussing the differences between *Riley* and CalECPA). Note also that while *Riley* would permit access for exigent circumstances, the comparable CalECPA emergency provision would excuse the need for a warrant only when there is a good faith belief that danger of death or serious physical injury require access. CAL. PENAL CODE § 1546.1(c)(5) (West 2017).

electronic communications contents,[206] and does not require a warrant for law enforcement access to some contents or to any metadata, including location data.[207] In particular, the SCA requires a warrant only to compel the disclosure of the contents of electronic communications that have been in electronic storage for 180 days or less on an electronic communications service.[208] Counter-intuitively, because they are likely to be more important to the user, electronic communications contents, like emails, stored more than 180 days are subject to a procedural hurdle that is easier to satisfy than probable cause.[209]

In contrast, CalECPA's uniform warrant requirement is surely its most privacy-protective feature. CalECPA applies its warrant requirement to the broad category of electronic information, which includes contents, metadata, location data, and electronic device data. Also unlike the SCA, CalECPA uses a broader definition of service providers, to include those who act as mere intermediaries in the transfer of electronic communications as well as those who merely store them.[210] CalECPA's broad definition of service provider should yield many more covered entities than the comparable federal language and much more covered information.

The SCA defines its service providers, which must be either an "electronic communications service"[211] (ECS) or a "remote computing service"[212] (RCS) in ways that further limit the scope of the SCA's warrant protection.[213] For example, based on those statutory definitions and the definition of "electronic

206. *See* 18 U.S.C. § 2510(8) (2012) (defining "contents" as "any information concerning the substance, purport, or meaning of that communication").

207. *Id.* §§ 2703(a), (b)(1)(A).

208. *Id.* § 2703(a).

209. The SCA defines electronic communications similarly to CalECPA. The SCA treats electronic communications and wire communications the same, but lists them separately. 18 U.S.C. §§ 2510(1), (12) (2012). In contrast, CalECPA includes communications sent by wire in its definition of electronic communications, thereby treating wire communications as a subset of electronic communications. CAL. PENAL CODE §1546(c) (West 2017).

210. The SCA also limits RCS's to those who provide services to the public. 18 U.S.C. § 2711(2) (2012).

211. *Id.* § 2510(15) ("'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.").

212. *Id.* § 2711(2) (defining "remote computing service" to mean "the provision to the public of computer storage or processing services by means of an electronic communications system").

213. CLRC MEMORANDUM 2014-33, *supra* note 64. The SCA covers communications contents held by RCS's as opposed to ECS's only when those communications are held or maintained "on behalf of, and received by means of electronic transmission from . . . a subscriber or customer of such remote computing service" and held or maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer," with the RCS not being able to access the contents of the communication for any other purpose. 18 U.S.C. § 2703(b)(2) (2012).

storage,"[214] the federal Department of Justice (DOJ) has taken the position that emails that have been opened, accessed, or downloaded are not protected by SCA's warrant requirement. The DOJ has opined that such emails stored by providers that do not offer service to the public, like universities, the government, and corporations, fall entirely outside the protections of the SCA.[215] Since 2013, DOJ policy has been to require a warrant for access to the content of all emails, despite the terms of the statute, but that practice could change outside of the Sixth Circuit, where the *Warshak* case governs.[216]

As another example, a California district court found the social networking site LinkedIn to qualify as neither an ECS nor an RCS with respect to its customers' web browsing information that it shared with third parties. The court therefore denied plaintiffs' claims arising under the SCA.[217] CalECPA's broad definition of service provider would surely have covered LinkedIn and the browsing information that it shared.[218]

Even when the SCA does require a warrant requirement for law enforcement access, the federal statute does not require that the warrants issued under it be as tailored as CalECPA's warrant are in order to avoid excessive information collection. Service providers responding to SCA warrants may be compelled to disclose everything they have about a target. In *Warshak*, for example, the service provider disclosed thousands of emails from Warshak's account, spanning the nine years that he held his account with that provider.[219] The SCA also lacks any mechanisms for the segregation or deletion of irrelevant data.

The SCA, unlike CalECPA, provides a graduated and complex set of hurdles to obtaining different types of communications depending on their characteristics. Regarding communication contents, if they are held in

214. 18 U.S.C. § 2510(17) (defining "electronic storage" to include "temporary, intermediate storage . . . incidental to the electronic transmission" and storage "for purposes of backup protection" of the communication by an electronic communication service.").

215. U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123–26, 138 (3d ed. 2009), www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [https://perma.cc/LX89-BKDA] [hereinafter DOJ Manual]. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215–18 (2004).

216. H.R. REP. NO. 114–528, at 9 (2014). The Ninth Circuit has also used a broader definition of electronic storage that does not support the DOJ's former interpretation. Theofel v. Farey-Jones, 359 F.3d 1066, 1076–77 (9th Cir. 2004).

217. Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1022–24 (N.D. Cal. 2012).

218. *See* ACLU OF N. CAL., *supra* note 12 (describing various types of information covered by CalECPA, including social network content and web browsing data).

219. *See* Bellia & Freiwald, *supra* note 109, at 130 (discussing the federal case against Warshak).

electronic storage by an RCS or held for more than 180 days by an ECS, government entities may acquire them with a subpoena if they give notice, or they may obtain a court order ("D order")[220] after meeting a procedural hurdle between the mere relevance standard and probable cause.[221] The D order is available only when the information sought is "relevant and material to an ongoing criminal investigation."[222]

Under the SCA, information that is not the contents of a communication falls into one of two categories: it is either a "record or other information pertaining to a subscriber to or customer of" an ECS or an RCS, or it is outside the SCA's scope.[223] Thus, electronic device data that is stored on personal devices rather than by an SCA service provider would be protected by CalECPA's warrant requirement but not protected by the SCA.

Whether the SCA even includes location data within its scope is unclear, which is not that surprising considering that the SCA was drafted in 1986, well before cell phones were in popular use. Most judicial opinions on the topic have assumed that the SCA's records provision includes data collected by cell phone service providers that indicate which cell towers cell phones use when they make and receive calls.[224] But some judicial opinions have found location data to be generated by a "tracking device"—a cell phone—and therefore excluded from SCA coverage.[225] If the SCA's records category includes location data, then agents may compel covered providers to disclose the data when they get a D order. It is unclear what rule applies if location data falls outside of the SCA's coverage.[226] The Fourth Amendment's treatment of

220. It is called a D order because it is obtained under procedures detailed in 18 U.S.C. § 2703(d).

221. 18 U.S.C. § 2703(b) (2012). A D order requires "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). Reformers have pressed for legislation to mandate a uniform warrant standard for access to all communications content. *See supra* note 192 and accompanying text.

222. § 2703(d). The limit on D orders indicates that the SCA, like CalECPA, is intended to regulate law enforcement investigations, although, like CalECPA, its terms refer generally to government entities. *See supra* notes 112–114 and accompanying text (describing how CalECPA leaves California law as it found it regarding investigations that do not have a law enforcement purpose).

223. 18 U.S.C. § 2703(c) (2012); *see also infra* Section V.A (elaborating on how the SCA defines service provider).

224. *See, e.g.*, United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016) (en banc).

225. *See* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislatures in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L REV. 875, 883–86 (2014) (describing courts' analyses and explaining that ECPA's definition of electronic communications excludes information generated by a tracking device.)

226. *Id.*

location data remains uncertain; many, but not all, cases have found no warrant required for access to historical location data.[227]

CalECPA imposes its warrant requirement on location data, broadly defined, stored with a service provider because it includes the "location of the sender or recipients at any point during the communication" in the definition of electronic communication information.[228] By bringing location data, however collected, so clearly within the scope of the warrant requirement, CalECPA brings helpful clarity to what has been a particularly muddled area of the law. It also protects information about people's movements, which several scholars and courts have agreed should receive the judicial oversight that a warrant procedure entails.[229]

The SCA does not treat all "records" as subject to the D order; some of them are available pursuant to a subpoena—mirroring much of the information that CalECPA permits access to with a subpoena in its "subscriber information" category.[230] The SCA permits access to much more information with a subpoena than CalECPA does, however. In particular, the SCA permits government entities to obtain call data records and subscriber numbers or identities with a subpoena, while CalECPA requires the greater protection of a warrant for access to that information, as well as IP addresses.[231]

3. Notice

Unlike CalECPA's comprehensive notice scheme, the SCA explicitly requires notice to the target only in one context: when a government entity uses a subpoena or a D order to compel the disclosure of the contents of a communication held in electronic storage more than 180 days by an ECS or an RCS.[232] For all other methods that the SCA regulates—including whenever a warrant is used to obtain contents and whenever non-contents information

227. *See supra* notes 52–56 and accompanying text.

228. CAL. PENAL CODE § 1546(d) (West 2017).

229. *See, e.g.*, Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); State v. Earls, 214 N.J. 564 (2013) (finding seizure of location data requires the protections of a warrant based on the New Jersey Constitution).

230. 18 U.S.C. § 2703(c)(2) (2012); CAL. PENAL CODE § 1546(d) (West 2017).

231. 18 U.S.C. § 2703(c)(2) (2012); CAL. PENAL CODE § 1546(d) (West 2017); *see also* Liebeskind, *supra* note 4 (noting that the SCA permits subpoena access to payment information, call detail records and IP address information, while CalECPA requires a warrant for that same information).

232. 18 U.S.C. § 2703(b)(1)(B) (2012). Note that notice can be delayed under the SCA for similar reasons as under CalECPA. *Id.* § 2705.

is obtained—the statute either explicitly dispenses with notice, or cases have interpreted the statute to dispense with the need for notice.[233]

Notice is essential to keeping law enforcement officers within the parameters set by a legislative scheme. Without it, targets of investigations may never come to understand that their electronic communication information has been acquired, particularly if the service provider is served with a gag order, which often happens under the federal law.[234] With the exception of defendants in criminal trials in which prosecutors disclose electronic communications data as part of discovery practice, targets cannot challenge improper government access to their digital data without adequate notice of that access. As the next Subsection details, under the federal statute, there are few reasons to bring such challenges, even for good cases.

4. Sanctions and Remedies

The SCA provides few remedies. Most notably, it furnishes no statutory suppression remedy to victims of investigations that violate its terms.[235] Respected commentators have viewed the SCA's lack of a suppression remedy as its most significant failing, largely because without the possibility of having evidence against them excluded, criminal defendants lack an incentive to challenge law enforcement practices.[236] Without such challenges, the law fails to develop,[237] not to mention that government practices in violation of the statute likely go unaddressed.[238] The SCA does permit victims of unlawful acquisition to bring a damages claim against a service provider that discloses their communications data in violation of the Act, so long as the provider did not act in good faith.[239]

---

233. The DOJ contends that notice is not required when a warrant is used, which seems odd given that notice is constitutionally required under the Fourth Amendment. *See* DOJ Manual, *supra* note 215, at 133.

234. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 324–25 (2012).

235. 18 U.S.C. § 2708 (2012). Unlike CalECPA, it also fails to provide for an Attorney General action or for motions to modify orders granted pursuant to it or to destroy information obtained under it.

236. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1285 (2004); Orin S. Kerr, *Lifting the 'Fog' of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824–26 (2003).

237. *Cf.* Orin Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on* Camreta v. Greene *and* Davis v. United States, 2010–2011 CATO SUP. CT. REV. 237, 239, 248–61 (discussing how a narrowed constitutional exclusionary rule removes the incentive to bring cases and stunts the development of Fourth Amendment law).

238. Freiwald, *supra* note 48, at 361–79; *see also* 18 U.S.C. § 2707 (2012) (providing for the possibility of administrative discipline).

239. 18 U.S.C. § 2707 (2012) (providing for damages).

By comparison, while CalECPA lacks a private cause of action, its suppression remedy and other remedies are sure to make it a more potent deterrent against law enforcement abuse than the SCA. Since CalECPA's passage, law enforcement agencies and other government entities around the state have been scrambling to ensure that their practices are consistent with the statutory mandates.[240] In addition, considerable effort was put into amending CalECPA to achieve compromises between the demands of the statute and the actual practices of law enforcement personnel.[241] There is no question that CalECPA has teeth.

V. CONSIDERATIONS GOING FORWARD—FOR CALECPA AND SIMILAR LAWS

CalECPA clearly provides expansive privacy protection to a wide array of modern electronic communications. Even before practical issues of implementation are considered, however, CalECPA's own terms present questions about how to delineate the statute's coverage. They also challenge seemingly entrenched notions in federal statutory and constitutional law.

A. OPEN ISSUES

What is an electronic communication? ECPA and CalECPA use the same language for this central concept, but that language, though exceptionally broad, is not clear. CalECPA defines an electronic communication as "the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."[242] ECPA uses the same language and then adds a few exclusions.[243] But when does a file, whether it is a music file, a photo, or a spreadsheet, become an electronic communication? Are all electronic files stored in the cloud "electronic communications" because they have been sent over the Internet—attached to communications? What if they are created and transferred without human involvement? What, if anything, does not count as an electronic communication? And if something is not an electronic communication, then what is it and how is it treated?[244]

240. This is based on conversations the author has had with various law enforcement officials in California.

241. *See supra* notes 117–118.

242. CAL. PENAL CODE § 1546(c) (West 2017).

243. 18 U.S.C. § 2510(15) (2012) (excluding, for example, wire and oral communications and communications from a tracking device from the definition of "electronic communication").

244. CalECPA's sponsor stated that the new law was designed to institute "clear probable cause warrant requirements for government access to electronic information, including data

CalECPA recognizes that some information stored on or generated by an electronic device does not count as electronic communication information and explicitly protects that information nonetheless.[245] But the borderline of an electronic communication—separating what counts from what does not—is still important because CalECPA's service provider definition, and therefore its scope, relies on its definition of an electronic communication.

Recall that CalECPA service providers furnish their "subscribers or users the ability to send or receive electronic communications," and include "any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information."[246] To comply with CalECPA, government entities need to know whether they are seeking electronic communication information and whether they are compelling disclosures from a covered service provider. With such a broad definition, the scope of "service provider" under CalECPA will depend largely what counts as an electronic communication.[247] With the definition of an electronic communication unclear, the scope of "service provider" also remains in question, though clearly it is an expansive term.

Over time, court decisions may clarify the definition of electronic communication. They may also elucidate the dividing line between service providers and non-service providers under CalECPA. Until then, it seems that whenever California government entities seek digitally stored information from companies, they must do so using a CalECPA warrant.

Another area of uncertainty concerns the dividing line between subscriber information and electronic communication information. CalECPA's definition of electronic communication information explicitly includes "an IP address" when it is "information pertaining to any individual or device participating in

from electronic devices, emails, cloud storage, digital documents, text messages, metadata, and location information." CAL. ASSEMB. COMM. ON PRIVACY & CONSUMER PROT., BILL ANALYSIS, S.B. 1121, 2015–2016 Leg., Reg. Sess., at 6 (2016), www.leginfo.ca.gov/pub/15-16/bill/sen/sb_1101-1150/sb_1121_cfa_20160620_130429_asm_comm.html [https://perma.cc/7VTJ-XR3B]. That certainly indicates broad coverage, but it does not help with borderline cases.

245. CAL. PENAL CODE § 1546(d) (West 2017) (electronic information is electronic communication information or electronic device information).

246. *Id.* § 1546(j). As discussed, that definition is much broader than the comparable definitions in federal law. *See supra* notes 97, 211–213.

247. ECPA further limits the scope of its service providers by using defined terms like remote computing service, 18 U.S.C. § 2711(2) (2012), and electronic communications service providers. 18 U.S.C. § 2510(15) (2012).

the communication . . . ."[248] But there may be times when an IP address acts like "a subscriber or account number or identifier," such as when it is a fixed IP address that is attached to a person's device and does not vary with that person's communications.[249] Will such fixed IP addresses be considered to be "subscriber information," not subject to CalECPA's warrant requirement?[250] Because of the difference between static information and communications information,[251] the legal status of IP addresses and related information may depend on their function.

CalECPA clearly applies when California government entities conduct their investigations in California, which, for jurisdictional reasons, will be most of the time. But will there be other contexts in which courts will impose CalECPA's procedures? What about cases involving California-based witnesses? California-based service providers?[252] At the same time, if CalECPA affects interstate commerce unduly, it may fall afoul of the Dormant Commerce Clause.[253]

Finally, the status of immunity for providers under CalECPA could be clarified. Recall that CalECPA precludes "any cause of action" against a private company or its agents "for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to [CalECPA]."[254] CalECPA's immunity language directly matches the SCA's, but

248. CAL. PENAL CODE § 1546(d) (West 2017) (defining electronic communication information to also include "any information about an electronic communication or the use of an electronic communication service").

249. *See, e.g.*, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 120 (E.D. Va. 2011) ("Some networks assign one predefined address to each attached device ('static' addressing), whereas others assign addresses from a pool of available addresses ('dynamic' addressing)").

250. CAL. PENAL CODE § 1546(l) (West 2017). Recall that the SCA explicitly permits "any temporarily assigned network address" to be acquired with a subpoena. 18 U.S.C. § 2703(c)(2)(E) (2012).

251. *See* Bellia & Freiwald, *supra* note 109.

252. *See* Kearney v. Salomon Smith Barney Inc., 39 Cal. 4th 95 (2006) (applying California wiretapping law in a case arising out a Georgia firm's communications with California clients). I am indebted to Michael Sussmann of Perkins Coie for raising the issue of domestication as it relates to CalECPA.

253. DETERMANN, *supra* note 23, § 1-2:2.3.

254. CAL. PENAL CODE § 1546.4(d) (West 2016). The California Law Review Commission has suggested that "service provider" would be better than "corporation" in the statutory text. It is not a good idea to make immunity hinge on obtaining the statutory designation of service provider, however. Courts will likely view "corporation" as broad enough to encompass anyone targeted by a lawsuit subject to this provision. *See* Memorandum from the Cal. L. Revision Comm'n, State and Local Agency Access to Customer Information

CalECPA lacks the SCA's good faith reliance defense,[255] likely because the California law provides no civil cause of action to which that defense seemed necessary.

At least one commentator has suggested that immunity is unavailable to providers who are subject to CalECPA but who do not strictly comply with its terms.[256] Because CalECPA places no affirmative obligation on private companies, it is not easy to identify ways that they could run afoul of the law. As opposed to California government entities, who must comply with CalECPA's warrant, notice, and data destruction provisions, nothing in CalECPA explicitly obligates private companies to do anything other than comply with their obligations arising under other law.[257] Nonetheless it remains possible that a plaintiff, or group of plaintiffs, could bring a claim under California law if a service provider fails to ensure that the government entity to whom it disclosed information or rendered assistance complied with CalECPA.[258] For example, New York has proposed language in a bill modeled on CalECPA that would provide immunity for providing information in accordance with the statutory provisions but then states that "[t]his does not preclude a cause of action for providing records, information, facilities, or other forms of assistance in a manner that is inconsistent with" those provisions.[259] The possibility of private lawsuits was not likely on the minds of the many companies that strongly supported CalECPA's passage, though the threat of liability could certainly boost compliance.

---

from Communication Service Providers (2015 Legislation and Next Steps) at 15 (Nov. 25, 2015), http://www.clrc.ca.gov/pub/2015/MM15-51.pdf [https://perma.cc/2BG8-VCN6].

255. 18 U.S.C. § 2707(e)(3) (2012) (establishing good faith reliance on court orders, warrants, requests, etc. to be "a complete defense to any civil or criminal action brought under this chapter or any other law").

256. Liebeskind, *supra* note 4 ("Service providers should note that the CalECPA immunity requires strict compliance while the federal ECPA allows for good faith immunity.").

257. Service providers may voluntarily disclose electronic communication information if otherwise lawful. CAL. PENAL CODE § 1546.1(f) (West 2017).

258. *See* DETERMANN, *supra* note 23, § 6-2:1.2 (discussing unfair business practice claims in California). California's unfair business practice doctrine is more expansive than under federal law, which has itself recently expanded in the privacy context. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY (2016) (discussing unfair competition enforcement by the FTC).

259. Assemb. B. No. 1895, 2017 Gen. Assemb., 1st Reg. Sess. § 695.20(4) (N.Y. 2017).

B. IMPACT ON BROADER LEGAL QUESTIONS

CalECPA's uniform, highly protective approach has distinct advantages that cast the deficiencies of other statutory models in a poor light.[260] By applying its warrant requirement to metadata, location data, electronic communication content, and electronic device data, CalECPA obviates the need to determine where a piece of information resides, how long it has resided there, and the nature of the provider that stores it. That not only provides the greater privacy protection that users want and need, but it creates a statutory structure that is less amenable to indefensible arbitrariness.

As an example, CalECPA does not distinguish on the basis of historical as opposed to forward-looking, or real-time data, which precludes end runs around stricter laws based on that distinction. As an example of the latter, agents in one case seemed to go out of their way to make sure that the cell phone location data was collected as stored records rather than in real-time, presumably because real-time acquisition was subject to a warrant requirement and they viewed access to historical data as available with an easier-to-obtain D order.[261] The application requested that the cell phone service provider momentarily store the location data, as it was produced in real-time, and then deliver the newly created "stored records," on an ongoing basis, to the requesting agents, subject to the rules of stored, but not real-time data.[262] One judge described the same behavior as based on the "instantaneous storage" theory and denied the government's application under the Stored Communication Act.[263] Because CalECPA treats access to stored (historical) and real-time data the same, it removes the incentive for such maneuvering and properly reflects that historical data can be just as intrusive and revealing as data collected in real time.[264]

---

260. *Cf.* Susan Freiwald & Sylvain Metille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261 (2013) (comparing the uniform and broadly protective Swiss statute to more the uneven and less protective ECPA).

261. Freiwald, *supra* note 225, at 894–97. The Fifth Circuit ultimately agreed with the agents that they could obtain the stored records with a D order rather than a warrant. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

262. Freiwald, *supra* note 225, at 894–97.

263. *In re* Application of the U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 893 (S.D. Tex. 2014) (denying the government's attempts to have its application approved on the basis of a D order rather than probable cause).

264. *Id.*; *see also* Freiwald, *supra* note 225, at 896–97 (describing views of judges and academics that historical data can be just as intrusive as prospective data). *But see supra* note 52 (describing the *Carpenter* case, pending at the time of publication).

CalECPA's passage also weakens the force of the arguments in favor of the third-party doctrine.[265] The large number of technology companies who vigorously backed CalECPA strongly supports the view that people do not forfeit their privacy interests by using new electronic devices or by storing their digital communications in the cloud. The California law enforcement community's willingness to withhold opposition or even support CalECPA suggests that any disagreement with that view is not too firmly held.[266] That support also belies the idea that requiring a warrant for metadata and location data will fundamentally inhibit law enforcement investigations.[267]

VI. CONCLUSION

CalECPA is on its way to demonstrating that the police and other government entities can do their jobs while respecting the enhanced sensitivity of the data users store with their service providers and on their electronic communications devices. As a much more uniform and highly protective law than those at the federal level and in other states, CalECPA stands out as a model for others interested in reform. Understanding how the new law works—in terms of the strides it has made and the few issues it leaves open—is the first step in getting the word out.

265. CalECPA's passage adds to the chorus of other states who have rejected the third-party doctrine when interpreting their state constitutions. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 393–412 (2006) (describing a fifty-state survey of state constitutional application of the third-party doctrine).

266. *See, e.g.*, Barcelona, *supra* note 81.

267. The San Diego Police Officer Association lauded CalECPA (S.B. 178) because it would "strengthen[] community relationships and increase[] transparency without impeding on law enforcement's ability to serve the needs of their communities." Letter from Brian R. Marvel, President, San Diego Police Officers Ass'n, to Mark Leno, Senator, Cal. State Senate (Sept. 1, 2015), https://www.eff.org/document/sdpoa-support-letter-sb-178-calecpa [https://perma.cc/5NS3-YZTV].