Study G-300 June 29, 2020

Memorandum 2020-31

State and Local Agency Access to Customer Information from Communication Service Providers (Discussion of Issues)

Memorandum 2020-20 reintroduced the Commission's study of government access to customer information from electronic communication service providers. The memorandum provided an overview of the history of the study and a summary of most of the potential reforms that have not yet been addressed by the Commission.

The Commission[1] received a letter commenting on that memorandum, from Chris Conley, representing the American Civil Liberties Union of Northern California ("ACLU-NC"). A copy of that letter is attached as an Exhibit.

The Commission considered Memorandum 2020-20 at its May meeting, but only briefly. It did not closely examine the issues described in the memorandum or the letter from ACLU-NC. Nor did it make any decisions, other than to continue the study at a future meeting.

This memorandum reiterates and expands on the discussion of the first two issues discussed in Memorandum 2020-20. Future memoranda will explore the other issues that remain to be addressed.

Except as otherwise provided, all statutory references in this memorandum are to the Penal Code.

SERVICE PROVIDER LIABILITY

The California Electronic Communications Privacy Act ("Cal-ECPA")[2] expressly limits the liability of a California or foreign corporation that acts in compliance with an order issued pursuant to Cal-ECPA:

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

2. Sections 1546-1546.4.

> A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action 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 this chapter.[3]

It is not clear why that immunity is only provided to a corporation. While most service providers are likely to be incorporated, some could be organized as another form of business entity (e.g., a limited liability company). It is also possible that Cal-ECPA could be used to compel the production of information from a government entity that acts as a communication service provider (e.g., a state university providing Internet service to its students, alumni, and staff).

Cal-ECPA does not define the term "corporation." Nor is there a general definition that would apply to Cal-ECPA.

Argument in Favor of Reform

As a matter of policy, the immunity provision in Cal-ECPA should probably apply to all service providers, regardless of their form. A service provider who follows a lawful order that compels the disclosure of customer information should not be liable for complying with that order. If that principle applies to corporations, the staff sees no reason why it should not also apply to LLCs, partnerships, public entities, or any other form of legal entity.

Support for that argument can be found in Section 1524.3(d), a similar immunity provision that governs a warrant for the disclosure of electronic communication customer information. That subdivision provides:

> No cause of action shall be brought against any provider, its officers, employees, or agents for providing information, facilities, or assistance in good faith compliance with a search warrant.

That provision applies to any *provider*, without regard to whether the provider is a corporation. That approach is consistent with the reasoning discussed above — the immunity should extend to any entity that is legally compelled to disclose customer information, regardless of the entity's form.

If that were not the case, non-corporate providers could face liability for action taken pursuant to a search warrant or other compulsory legal process. The staff sees no good argument for that result.

3. Section 1546.4(d).

However, there is another provision that muddies the waters a bit. Section 1524.2 provides rules on the obligations of corporations when served with a warrant that requires the disclosure of customers' electronic communication information. The main focus of that provision is the differing obligations of California corporations and foreign corporations, when served with a warrant by a court of this state or of another state. That section includes an immunity provision that is very similar to the one used in Cal-ECPA, in that it is limited to corporations:

> (d) A cause of action shall not lie against any foreign or California corporation subject to this section, its officers, employees, agents, or other specified persons for providing records, information, facilities, or assistance in accordance with the terms of a warrant issued pursuant to this chapter.[4]

Does the existence of that provision support the idea that Cal-ECPA's immunity provision should also be limited to corporations?

Arguably not. Section 1524.2 only regulates corporations. It therefore makes sense to limit its immunity provision to corporations; the immunity should be coextensive with the legal mandates that could cause liability.

By contrast, Cal-ECPA applies to any "person or entity offering an electronic communication service."[5] The rules are not limited to corporate entities. This means that the obligations imposed by Cal-ECPA apply to some persons and entities that are not within the scope of the immunity provision's protections. The staff sees no good policy reason for that result.

Comment from ACLU-NC

ACLU-NC generally supports the idea of broadening the application of the liability provision to all providers:

> We agree with the commission that immunity for liability should not be limited to entities with a specific form of incorporation. Instead, it should extend not only to other business organizations but also to nonbusiness entities such as private individuals that qualify as service providers under CalECPA. The present immunity language arguably already encompasses any legally recognized business, but it is less likely to extend to unorganized entities.[6]

4. Section 1524.2(d).
5. Section 1546(j) ("service provider" defined).
6. See Exhibit p. 1.

In addition, ACLU-NC suggests that it might be helpful to add a disclaimer, making clear that the immunity from liability for compliance with a requirement of Cal-ECPA has no effect on liability that may exist for other actions by the service provider:

> We further urge the commission to ensure that immunity under CalECPA for compliance with valid legal process or emergency requests does not also immunize service providers from the illegal collection or retention of that information in the first place. In particular, a service provider that collects or retains consumer information in violation of the California Consumer Privacy Act should not be immunized from liability under that Act if the information is later disclosed in response to an otherwise-valid search warrant.[7]

While the staff does not see great scope for confusion on that point, it might be helpful to add a carefully worded disclaimer.

Recommendations

The staff recommends that Cal-ECPA's immunity provision be revised to apply to any "service provider," which would not be limited to corporations.[8] Thus:

> 1546.4. …
> (d) A ~~California or foreign corporation~~ service provider, and its officers, employees, and agents, are not subject to any cause of action 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 this chapter.[9]
>
> **Comment**. Subdivision (d) of Section 1546.4 is amended to make clear that it applies to any service provider and not just one that is formed as a corporation.

The Commission should also consider adding a disclaimer along these lines, either as part of subdivision (d) or in the Commission's Comment:

> Nothing in this subdivision affects any liability of a service provider for an act that is not compelled by the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.

---

7. *Id*.
8. Section 1546(j) ("Service provider" means a person or entity offering an electronic communication service.").
9. Section 1546.4(d).

Should one or both of the provisions discussed above be included in a tentative recommendation?

SPECIAL MASTER

Under Cal-ECPA, when a court issues a warrant or other order for access to electronic information, the court has *discretion* to appoint a special master.[10] The special master is "charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed."[11] Cal-ECPA does not specify how a special master is to perform that function. Presumably, the special master will screen the information obtained and decide which information to pass along to law enforcement, while sealing the rest.

A provision outside Cal-ECPA — Section 1524(c) — also involves the screening of seized evidence by a special master. It applies when a warrant is issued for a search of "documentary evidence" that is "in the possession or under the control" of a lawyer, doctor, psychotherapist, or member of the clergy "who is not reasonably suspected of engaging or having engaged in criminal activity related to the documentary evidence for which a warrant is requested." In that case, the appointment of a special master is *mandatory*, and a specific procedure must be followed.[12]

The mandatory special master rule makes sense, given the heightened likelihood that records in possession of a lawyer, doctor, psychotherapist, or member of the clergy are subject to an evidentiary privilege.

Cal-ECPA expressly provides that a warrant for electronic information must satisfy all other state and federal law that governs warrants. That should include the special master rule in Section 1524(c).

However, notwithstanding that broad incorporation of other law, it is possible that Section 1524(c) might, *by its own terms*, be inapplicable to a warrant for electronic information. The staff does not believe that this is the case, but certain language in Section 1524(c) could create uncertainty on that point. Specifically, it may not be sufficiently clear how the concepts of "documentary evidence" and "in the possession or under control" apply to electronic records held by a service provider on behalf of a customer. The staff has not found any court opinion discussing that issue. The question is discussed further below.

10. Section 1546.1(e)(1).
11. *Id.*
12. Section 1524(c)(1)-(3).

Documentary Evidence

As noted, Section 1524(c) only applies to "documentary evidence." That term is defined broadly for the purposes of Section 1524(c):

> As used in this section, "documentary evidence" includes, but is not limited to, writings, documents, blueprints, drawings, photographs, computer printouts, microfilms, X-rays, files, diagrams, ledgers, books, tapes, audio and video recordings, films, and papers of any type or description.[13]

That definition does not expressly refer to electronic communications. However, the definition is framed as a nonexclusive list of examples, so it should be read as expressing a concept that is embodied in the defined term itself, as illustrated by the list of examples. Viewed that way, the staff believes it is reasonable to construe "documentary evidence" very broadly, as including any type of stored information, include electronically stored information.

Moreover, given the close connection of Section 1524(c) to the rules that govern evidentiary privileges, it seems reasonable to construe the meaning of "writings" used in Section 1524(f) in accord with Evidence Code Section 250, which defines "writing" to mean:

> handwriting, typewriting, printing, photostating, photographing, photocopying, *transmitting by electronic mail* or facsimile, *and every other means of recording upon any tangible thing, any form of communication or representation*, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, *regardless of the manner in which the record has been stored*.[14]

In addition, ACLU-NC does not see a need for a clarifying amendment:

> Electronic communication information satisfies the definition of "documentary evidence" (which, as the Commission notes, "includes but is not limited to" documents, images, and other analogs of electronic communication information under CalECPA) …. As such, we do not believe that [a change is] necessary.[15]

While the staff did not find any court opinions that specifically addressed whether the definition of "documentary evidence" in Section 1524(f) includes electronic records, there are a few unpublished opinions in which a search conducted by a special master pursuant to Section 1524(c) resulted in the seizure

13. Section 1524(f).
14. Emphasis added.
15. See Exhibit p. 2.

of a computer or computer storage media. That fact was treated as unremarkable in the opinions, suggesting a general acceptance that documentary evidence includes computer files.

Based on all of the above, there doesn't seem to be a compelling need for clarification of the definition of "documentary evidence" in Section 1524. **The staff is inclined to leave the matter alone.**

Possession or Control

There is a second potential point of uncertainty about the application of the mandatory special master rule to a Cal-ECPA warrant. Section 1524 only applies to documentary evidence that is "in the possession or under the control" of an attorney, doctor, psychotherapist, or member of the clergy.

Is it sufficiently clear that electronic records held on behalf of a customer by a communication service provider (e.g., email on mail server, files in cloud storage) are in the possession or under the control of the customer?

It might be argued that such records are not in the "possession" of the customer, especially if the records reside exclusively on the service provider's equipment (e.g., a Google doc).

It might also be argued that records on a service provider's equipment are not wholly within the customer's "control." If the customer has the ability to add, change, or delete content in the records, then there is a good argument that the customer has control of the records. But what if the service provider maintains archival copies of the records that cannot be changed by the customer (as is the case with the cloud storage service that is used by the staff, which maintains a comprehensive "version history" of every file in storage). Are those back-up records within the customer's control?

The staff first raised this issue after finding a case that addressed the application of Section 1524(c) to a report prepared for a law firm by a consultant. In *PSC Geothermal Services Co. v. Superior Court*,[16] the court held that the mandatory special master rule did not apply to a copy of report prepared by a consultant for an attorney, when that copy was seized at the consultant's office. Under those facts, the court held that the record was neither in the attorney's possession, nor under the attorney's control.

16. 25 Cal. App. 4th 1697 (1994). The staff has not found any published opinion that addresses the application of Section 1524(c) to electronic records held by a communication service provider on behalf of a customer who is a lawyer, doctor, psychotherapist or member of the clergy.

ACLU-NC does not believe there is a problem with the "possession or control" language, because "the owner or user of an account controls the information at stake."[17]

That is probably the best understanding of the concept of control. It might be helpful to codify that understanding. **How would the Commission like to proceed?**

Respectfully submitted,

Brian Hebert
Executive Director

17. See Exhibit p. 2.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Northern California

California Law Revision Commission
c/o UC Davis School of Law
400 Mrak Hall Drive
Davis, CA 95616

May 18, 2020

Re: State and Local Agency Access to Customer Information from Communication Service Providers - Study G-300

Dear California Law Revision Commission:

The ACLU of Northern California appreciates the Commission's longstanding efforts to review and propose reforms to California's laws. As the Commission noted, the California Electronic Communications Privacy Act (CalECPA) substantially updated the landscape of electronic privacy law in California. CalECPA provides robust protections for all electronic information, including enhanced warrant requirements, mandatory notice, and a suppression remedy for all violations. We encourage the Commission to ensure that any continued work in this area is consistent with CalECPA's principles and supports its objective of robustly protecting the privacy and free speech rights of Californians in the digital age.

Below are our specific comments on the various issues that the CLRC proposes to investigate:

1. Service Provider Liability

CalECPA immunizes "California or foreign corporations" from liability (under California law) for providing information pursuant to court orders or emergency certification. The CLRC has posed the question of whether this immunity extends or should be extended to other entities, including non-incorporated business entities (e.g. a limited liability partnership) and non-business entities.

We agree with the commission that immunity for liability should not be limited to entities with a specific form of incorporation. Instead, it should extend not only to other business organizations but also to non-business entities such as private individuals that quality as service providers under CalECPA. The present immunity language arguably already encompasses any legally recognized business, but it is less likely to extend to unorganized entities.

We further urge the commission to ensure that immunity under CalECPA for compliance with valid legal process or emergency requests does not also immunize service providers from the illegal collection or retention of that information in the first place. In particular, a service provider that collects or retains consumer information in violation of the California Consumer Privacy Act should not be immunized from liability under that Act if the information is later disclosed in response to an otherwise-valid search warrant.

2. Special Master

CalECPA provides that the court issuing a warrant or other order has the discretion to appoint a special master charged with "ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed." Separately, Penal Code 1524(c) mandates the appointment of a special master for demands for records held by an attorney, doctor, psychotherapist or clergy member. The Commission has raised the question of whether the law should be revised to require the appointment of a special master for any search warrant issued under CalECPA seeking information held by a service provider on behalf of an attorney, doctor, psychotherapist or clergy member.

We believe that there is no need for such provision since the requirements of Penal Code 1524(c) already apply. Electronic communication information satisfies the definition of "documentary evidence" (which, as the Commission notes, "includes *but is not limited to*" documents, images, and other analogs of electronic communication information under CalECPA) and the owner or user of an account controls the information at stake. As such, we do not believe that changes are necessary.

If the Commission choose to pursue this line of inquiry, it should ensure that any proposed protections for specific categories of privileged information do not implicitly or explicitly erode safeguards for other information. In particular, any proposal should explicitly state that the appointment of a special master under CalECPA is not limited to circumstances where the target of the warrant potentially possesses privileged information but is available in all circumstances if the issuing magistrate deems it necessary or appropriate.

3. Meaning of "Interception" under Wiretap Act

Current law requires a wiretap order, or "super-warrant," to "intercept" communications. However, as the Commission rightly notes, courts have interpreted interception narrowly in the electronic space. As such, the Commission raises the question of whether California law should treat any prospective capture of electronic communication information as an interception requiring a wiretap order.

We believe that creating a separate regime for prospective capture of electronic information, while well-intentioned, would be in direct conflict with CalECPA's core principle of providing strong and consistent protections for all electronic information. As such, we urge the Commission to instead consider whether the protections of the Wiretap Act should be applied to all demands for electronic communications information.

The narrow interpretation of "intercept[ion]" is but one of many examples of situations where court interpretations of existing law has failed to reflect our digital reality with repercussions for the privacy and free speech rights of Californians. Like many of these deficits, the root cause of this problem is the decision to treat a particular form of information, here information "in transit," as meriting greater privacy protections than other forms of information. That distinction may have been justified in the context of the telephone calls of the time, where conversations were inherently ephemeral and recordings of prior communications were rare exceptions, but it fails to reflect the modern reality where many digital conversations are recorded verbatim and stored indefinitely. As such, we agree with the Commission that the current understanding of interception limits the effectiveness of the Wiretap Act.

However, we believe that the approach embodied by CalECPA is a preferable solution to that proposed by the Commission. CalECPA was enacted to eliminate, not merely update, antiquated distinctions

between different categories of information embedded in federal privacy law. It provides the same level of robust protection to metadata as it does to content, and to historical as to real-time information. And it brings many (though not all) of the protections of the Wiretap Act, notably enhanced specificity and mandatory notice, to all collection of electronic information, retrospective as well as prospective. Given the pervasive retention of communication information, we believe that the distinction between those two categories is not one that merits heightened protections for only prospective information. Instead, any additional safeguards should encompass both prospective and retrospective information.

As such, rather than applying heightened protections to a specific subset of information, we encourage the Commission to look more broadly at what protections from the Wiretap Act or elsewhere should be applied to all electronic communication information, whenever it is created. We believe that this would serve Californians better than an attempt to identify one specific type of information for enhanced safeguards.

4. Remaining Issues

The Commission raises two final issues for possible consideration: whether the law should be amended to require that a government entity provide notice to a customer when issuing an administrative subpoena for electronic communication information, and whether there is a practical mechanism to achieve minimization of interception of privileged electronic communications analogous to the suspension of an aural wiretap when a privileged conversation is identified? Of those, we believe that the first merits the Commission's continued attention.

We believe that it is useful to further consider the proposal to require notice to the target of an administrative subpoena. CalECPA currently requires notice to the target of a warrant, and many service providers either provide notice to the target of an investigation when permitted to do so or simply require the government entity to subpoena the target directly. Nonetheless, explicitly requiring that the target of a subpoena is directly notified by the government agency prior to the execution of the subpoena gives the target an opportunity to quash the subpoena before information is inappropriately disclosed. Direct notice of administrative subpoenas also furthers the goal of transparency of public demands, analogous to the notice and reporting requirements in CalECPA. *See* Penal Code 1546.2.

We look forward to continuing the conversation about ways to ensure that California's electronic privacy laws continue to robustly safeguard the rights of Californians and keep pace with the ever-changing digital world.

Sincerely,

Chris Conley
Technology & Civil Liberties Attorney
ACLU of Northern California
415-621-2493 | cconley@aclunc.org