Study G-300 July 16, 2021

Memorandum 2021-38

State and Local Agency Access to Customer Information from Communication Service Providers: Notice of Administrative Subpoena

At its June 2021 meeting, the Commission[1] directed the staff to prepare a draft of a proposed statute that would require notice be given to a customer when the government uses an administrative subpoena to obtain the customer's records from a communication service provider. The draft would implement the recommendations made in Memorandum 2021-32.[2] That draft is attached to this memorandum.

The staff was also directed to prepare a discussion of the possible use of a record preservation order in connection with such a subpoena. In particular, the discussion should address the application of such an order to a communication service that features routine deletion of communications, and a review of case law and other authority discussing a similar record preservation mechanism available under the federal Stored Communications Act.

This memorandum was prepared pursuant to those instructions.

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

DISCUSSION OF PROPOSED LEGISLATION

The proposed legislation is fairly straightforward. All of its provisions are borrowed from existing law, either the California Right to Financial Privacy Act or the federal Stored Communications Act (the specific sources are noted in the proposed Comments in the attached draft). A few specific aspects of the draft are discussed below.

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. See Minutes (June 2021), p. 4).

Location

The proposed law would govern a state agency's use of an administrative subpoena. The existing law that authorizes such subpoenas is Government Code Section 11181. That section is located in an article entitled "Investigations and Hearings," in a chapter entitled "State Departments and Agencies." It makes sense to locate the proposed law in the same place, near Section 11181.

Unfortunately, that location is crowded. There are no whole number gaps in section numbering. Although it is not ideal, the best choice seems to be placing the new provision next to Section 11181 (which it would directly supplement). That would require the use of a decimal in the section number. That is the approach used in the attached draft, with the proposed legislation drafted as a new Section 11181.5.

Definitions

The proposed law incorporates definitions from the California Electronic Communications Privacy Act ("Cal-ECPA"). The use of those definitions simplifies the drafting of the proposed law, improves its readability, and would create useful uniformity between this statute and Cal-ECPA.

Timing

Proposed Section 11181.5(b)(3) is borrowed from Section 7474(a)(3), which prohibits the disclosure of financial institution customer records until at least 10 days have passed without the customer giving notice to the financial institution of a motion to quash the subpoena.

Section 7474(a)(3) raises a few questions that should probably be answered when creating an analog in the proposed legislation:

- What is the event that triggers the 10-day period? Is it service of the subpoena on the financial institution or service of a copy on the customer?
- If the trigger is service on the financial institution, what is the result if service of a copy on the customer is delayed? Any delay would reduce the time available for the customer to move to quash the subpoena.
- If the trigger is service on the customer, how will the financial institution know the date of that event? There's nothing in the statute that requires a government agency to provide that information to the financial institution.

The staff sees two alternative ways that those issues might be addressed:

(1) Require that the copy be served on the customer *on the same day* as service of the subpoena on the financial institution. That way, the choice of triggering event would not matter, because both possibilities would yield the same timing result.

(2) Require that the government entity provide the financial institution with proof of service to the customer. The 10-day period would begin on the date of service on the customer.

The staff prefers the second approach. While it would add another procedural step (providing proof of service), it would provide timing flexibility that could be useful in some situations. Any delay between service of the subpoena on the service provider and service of a copy of that subpoena on the customer would not be prejudicial to the customer, because the customer would always have 10 days to move to quash the subpoena before it could operate.

The Commission needs to decide how to address this issue. The Commission's decision will be implemented in the next draft of proposed legislation.

It might be helpful to address the same issue in existing Section 7474. Unfortunately, the Commission does not have authority to study government access to financial records and the Commission's general authority to study "minor substantive defects"[3] probably could not be stretched that far. If the Commission ultimately recommends a change to address the timing issue for administrative subpoenas, the staff could informally raise the issue with the legislative committees that have jurisdiction over financial institutions and/or privacy. They could then decide whether to address the matter for financial institutions.

Record of Disclosure

Existing Section 7470(c) requires that a financial institution maintain records of the "examination or disclosure" of customer records by a government agency pursuant to that law. Among other things, the records must include "the identity of the person examining the financial records [and] the state or local agency or department thereof which he [sic] represents."

The requirement that the records name the agency representative who "examines" the records, in addition to naming the agency, seems to suggest that a government agent might visit a financial institution's office in person, in order to examine physical customer records.

3. Section 8298.

That possibility seems remote in the context of electronic records held by a communication service provider. It seems much more likely that the records held by a communication service provider would be delivered to the government in electronic form, for inspection on its own equipment.

For that reason, Section 11181.5(f) does not include references to "examination" of customer records or the "person who examined" customer records. Instead, it consistently refers to "disclosure." **The staff invites comment on whether that would cause any problems.**

Record Preservation

Proposed Section 11181.5(g) would establish a narrow record preservation requirement. It is discussed below.

EVIDENCE PRESERVATION UNDER THE STORED COMMUNICATIONS ACT

At the June meeting, the Commission directed the staff to prepare a discussion of the evidence preservation provision of the federal Stored Communications Act (18 U.S.C. § 2703(f)). Specifically, that discussion should address:

(1) The application of such an order to service providers who routinely delete customer records as a feature of the service that they provide.
(2) Practical considerations for how such a rule could be implemented (including an examination of law and commentary on a similar rule that exists in federal law).[4]

The staff reviewed federal court decisions, treatises, and law review articles. The results of that research are discussed below.

Record Preservation as Government Seizure

In 2016, Professor Orin Kerr, a frequent commentator on the intersection of the Fourth Amendment and the Internet, wrote an opinion piece for the Washington Post that questioned the constitutionality of record preservation requests made under Section 2703(f).[5] The argument rests on two premises. First,

4. See Minutes (June 2021), p. 4).
5. *The Fourth Amendment and Email Preservation Letters,* Wash. Post (Oct. 28, 2016) <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/28/the-fourth-amendment-and-email-preservation-letters/>.

because a request under Section 2703(f) is mandatory, a service provider who complies with the request is acting as an agent of the government (thereby bringing that action within the ambit of the Fourth Amendment). Second, the act of making a duplicate set of a customer's information constitutes a "seizure" that is governed by the Fourth Amendment.

The same general argument was also made by the American Civil Liberties Union in an amicus brief that it filed in *United States v. Basey*,[6] an unpublished decision of the Ninth Circuit of the U.S. Court of Appeals.[7] The court's decision in *Basey* did not address the merits of the ACLU's argument (the staff is not aware of any published appellate decision that has done so).[8]

The most difficult element of the argument seems to be the claim that making a duplicate of a customer's information is a seizure for purposes of the Fourth Amendment. The Supreme Court has held that a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[9] In the staff's view, the duplication of customer information causes only a very minor interference with the customer's possessory interest. Creation of a copy does not affect a customer's ability to access and use their own copy of the information. The only interference is the customer's inability to modify or delete the copy that might eventually be turned over to law enforcement pursuant to later lawful process (e.g., a warrant).

The staff did find one unpublished District Court opinion that considered and rejected the argument discussed above. Although not precedential, it does illustrate the possibility of judicial skepticism toward the claim that a service provider's duplication of information constitutes a seizure: "The preservation requests in this case did not interfere with the Defendant's use of his accounts and did not entitle the Government to obtain any information without further legal process."[10]

---

6. Brief of Amici Curiae American Civil Liberties Union & American Civil Liberties Union of Alaska Foundation in Support of Defendant-Appellant Kaleb Basey, 2019 WL 829338 <https://www.aclu.org/sites/default/files/field_document/basey_amicus.pdf>.
7. The same argument was later made in Tadoyon, *Preservation Requests and the Fourth Amendment*, 44 Seattle U. L. Rev. 105 (2020).
8. United States v. Basey (2019), 784 F. App'x 497, 498 (9th Cir.), *cert. denied,* 140 S. Ct. 616, 205 L. Ed. 2d 405 (2019).
9. United States v. Jacobsen (1984) 466 U.S. 109, 113.
10. United States v. Rosenow (S.D. Cal. 2018) 2018 WL 6064949, at *10.

Frequency of Use and Lack of Judicial Review

Both Professor Kerr and the ACLU expressed concern about the frequency with which preservation orders are used and the high likelihood that they will be used in a situation that never actually leads to the use of compulsory process to disclose the preserved information to the government.

This results in a very large aggregate effect on customers (even if the effect on each individual customer is relatively modest):

> Unsurprisingly, because section 2703(f) does not require probable cause or individualized suspicion and an independent judicial check — and because the government can issue demands under the statute quickly and simply — the volume of preservation demands is extremely high. Since at least July 2014, Google has annually received tens of thousands of 2703(f) letters requesting preservation of multiple user accounts — including 8,698 letters affecting 22,030 accounts in the first half of 2018 alone. … In recent years, these numbers have been rising. Comparing to the six-month period between July and December 2017 with the period between January and June 2018, Google and Facebook together experienced between 20% and 30% increases in section 2703(f) letters and affected accounts.
>
> In some of these instances, investigators eventually meet the constitutional and statutory standards required to search private account data by subsequently serving appropriate legal process on providers. But providers receive thousands more section 2703(f) letters than they do subsequent legal process to actually search the accounts. For example, in the most recent six-month reporting period, Facebook received a total of 57,000 section 2703(f) letters, but only received 23,801 search warrants, 9,369 subpoenas, and 942 section 2703(d) court orders. Even assuming — implausibly — that legal process is always tied to an account previously targeted by a section 2703(f) letter, investigators never demonstrated any basis for their demands to copy and preserve accounts on almost 23,000 occasions over six months. From this data, it appears that the government's actual use of section 2703(f) is not primarily about preservation of evidence in cases where investigators are actively seeking a warrant. Rather, section 2703(f) provides investigators with a powerful tool to routinely copy and preserve tens of thousands of accounts without any evidence, risk of spoliation, judicial oversight, or obligation to follow-up.[11]

These concerns about excessive and indiscriminate use of preservation orders under federal law could be avoided in the proposed law, by limiting record

11. *Supra* note 5, pp. 6-8 (footnotes and citations omitted).

preservation to a situation where a subpoena has actually been served. That is the approach taken in the proposed law:

> (g) When an administrative subpoena is served on a service provider pursuant to this section, the service provider shall promptly make a copy of any electronic communication information that is within the scope of the subpoena and within the possession of the service provider at the time that the subpoena was served. The copy shall only be preserved until it is disclosed pursuant to the subpoena or the subpoena is quashed.

This approach would ensure that record preservation requests would only occur in the context of an actual investigation that is concrete enough to justify the service of a subpoena. Such requests could not be used indiscriminately as a low-cost fishing tool.

A requirement that subpoenaed records be protected against modification or destruction seems compatible with existing policy against the misuse of the discovery process. For example, existing law permits the imposition of sanctions for spoliation of evidence in the civil discovery process.[12]

Auto-Delete Communication Services

One specific concern that the Commission raised at the June meeting is how a record preservation requirement would work when applied to a communication service that includes periodic deletion of content as a feature.

The apparent answer lies in the express language of Section 2703(f). By its terms, Section 2703(f) authorizes a preservation request to a service provider for evidence that is "in its possession." One treatise on electronic surveillance explains:

> The records covered by this provision are those already in existence; § 2703(f)(1) does not apply to records to be created from future activity. To require service providers to record future communications, law enforcement officials must comply with the statutes governing acquisition of communications in transit….[13]

The U.S. Department of Justice has the same understanding:

> Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information

12. Code Civ. Proc. § 2023.030.
13. J. Carr, P. Bellia, E. Creutz, *The Law of Electronic Surviellance* § 5:56 (Oct. 2018).

> about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4.[14]

The fact that an evidence preservation request only affects records in existence at the time of the request goes a long way toward avoiding operational problems for "auto-delete" communication service providers. Obviously, information that has already been deleted cannot be preserved. And, under the textual analysis of Section 2703(f) discussed above, a preservation order cannot require the retention of future communications. Thus, Section 2703(f) only requires a snapshot of the data available to the service provider at a single point in time. That shouldn't pose serious problems for service providers, even those that auto-delete on a fixed schedule.

Moreover, even though there are providers who advertise that they will delete content on a periodic basis, a cursory survey of the terms of service of such companies shows that they include an express exception for disclosure pursuant to lawful process. For example, Snapchat, which promises that messages will be deleted after being opened by all recipients (or held for no more than 30 days if they remain unopened), provides an express exception for Section 2703(f) requests:

> We honor formal requests from law enforcement to preserve information in accordance with 18 U.S.C. § 2703(f). Upon receiving a signed and dated preservation request on law enforcement department letterhead, we will attempt to preserve available Snapchat account records associated with any properly identified Snapchat user(s) in an offline file for up to 90 days, and will extend the preservation for one additional 90-day period with a formal extension request.[15]

This suggests that auto-delete providers have found ways to accommodate evidence preservation requests.

Conclusion

The Commission needs to decide whether to include a record preservation requirement in the proposed law. The staff believes it would be prudent to do so. Otherwise, those whose communication records are being sought by an administrative agency would have an opportunity to delete or modify their

14. U.S. Dep't of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* Ch. 3(G)(1) (3d ed. 2009).
15. <https://snap.com/en-US/safety/safety-enforcement>

records before turning them over, to obscure evidence of an administrative violation.

Some have argued that a broad and unconstrained power to require evidence preservation (like the power granted in 18 U.S.C. § 2703(f)) effects a seizure of property by a government agent, thereby bringing it within the scope of the Fourth Amendment. Therefore, the argument goes, a preservation order must be authorized by a warrant based on probable cause. It is not clear that courts will embrace that theory. The only interference in a customer's possessory interest that is caused by a preservation order is the customer's inability to destroy or modify records before they are turned over to government pursuant to some subsequent legal process (e.g., a warrant).

Some have also expressed concern that unrestrained use of evidence preservation orders has a problematic aggregate effect.

Those problems could perhaps be avoided by crafting a narrow record preservation requirement that is only applicable once an administrative subpoena has actually been served on a communication service provider (as in proposed subdivision (g) of the attached draft). That would be minimally disruptive, would prevent any overuse of the record preservation process, would require that every record request requirement be grounded in a concrete investigation, and would limit the use of record preservation to situations in which there is a ripe opportunity for judicial review (i.e., a motion to quash).

How would the Commission like to address this issue? Possibilities include:

(1) Include a broad record preservation rule similar to Section 2703(f)?
(2) Include a narrow rule like proposed subdivision (g)?
(3) Omit any provision requiring record preservation?

NEXT STEP

Once the Commission has decided the issues discussed in this memorandum, the staff will prepare a draft tentative recommendation for presentation at a future meeting.

Respectfully submitted,

Brian Hebert
Executive Director

PROPOSED LEGISLATION

Gov't Code § 11181.5 (added). Subpoena for customer's electronic communication information

SECTION 1. Section 11181.5 is added to the Government Code to read:

11181.5. (a) For the purposes of this section, the following terms have the following meanings:

(1) "Customer" means a person or entity that receives an electronic communication service from a service provider.

(2) "Electronic communication information" has the meaning provided in subdivision (d) of Section 1546 of the Penal Code.

(3) "Electronic communication service" has the meaning provided in subdivision (e) of Section 1546 of the Penal Code.

(4) "Service provider" has the meaning provided in subdivision (j) of Section 1546 of the Penal Code.

(b) In addition to any other requirements that govern the use of an administrative subpoena, an administrative subpoena can only be used to obtain a customer's electronic communication information from a service provider if all of the following conditions are satisfied:

(1) The department has served a copy of the administrative subpoena on the customer pursuant to Chapter 4 (commencing with Section 413.10) of Title 5 of Part 2 of the Code of Civil Procedure.

(2) The administrative subpoena includes the name of the department that issued it and the statutory purpose for which the information is to be obtained.

(3) Ten days have passed after service of the copy on the customer without the customer giving notice to the service provider that the customer has moved to quash the administrative subpoena.

(c) Nothing in this section shall require a service provider to inquire whether, or determine that, the department has complied with the requirements of this section, provided that the administrative subpoena served on the service provider shows compliance on its face.

(d) If a customer files a motion to quash an administrative subpoena issued pursuant to subdivision (b), the proceeding shall be afforded priority on the court calendar and the matter shall be heard within 10 days from the filing of the motion to quash.

(e) Nothing in this section shall preclude a service provider from notifying a customer of the receipt of an administrative subpoena pursuant to subdivision (b).

(f) The service provider shall maintain a record of any disclosure of its customers' electronic communication information pursuant to this section. That record shall be retained for a period of five years. The record shall include a copy of the administrative subpoena providing for examination of the electronic communication information. Upon request and the payment of the reasonable cost of reproduction and delivery, a customer shall be provided any part of the record that relates to the customer.

(g) When an administrative subpoena is served on a service provider pursuant to this section, the service provider shall promptly make a copy of any electronic communication information that is within the scope of the subpoena and within the possession of the service provider at the time that the subpoena was served. The copy shall only be preserved until it is disclosed pursuant to the subpoena or the subpoena is quashed.

Comment. Section 11181.5 imposes specified requirements when an administrative subpoena is used to obtain a customer's electronic communication information from a service provider. Similar requirements exist when a government agency uses an administrative subpoena to obtain customer information from a financial institution. See Section 7474.

Subdivision (b) is drawn from Section 7474(a).

Subdivision (c) is drawn from Section 7470(b).

Subdivision (d) is drawn from Section 7474(d).

Subdivision (e) is drawn from the first sentence of Section 7474(c).

Subdivision (f) is drawn from Section 7470(c).

Subdivision (g) is new. It requires the service provider to preserve requested information to prevent its deletion or modification by the affected customer. See also 18 U.S.C. § 2703(f).