Study G-300 April 6, 2015

First Supplement to Memorandum 2015-10

State and Local Agency Access to Customer Information from Communication Service Providers: Staff Draft Tentative Report

The Commission[1] has received a letter from the Electronic Frontier Foundation, Asian Americans Advancing Justice — Asian Law Caucus, the Center for Democracy & Technology, the Council on American-Islamic Relations, the First Amendment Coalition, and the Media Alliance (hereafter, for ease of reference, the "EFF letter"). The staff greatly appreciates the input. The letter is attached as an Exhibit.

The EFF letter is generally supportive of the Commission's work in this study, but expresses concern about one point made in Memorandum 2015-3, relating to the use of an investigative subpoena (i.e., an administrative or grand jury subpoena) to obtain documents.

The concern raised in the EFF letter primarily relates to how the Commission should approach drafting proposed legislation, a matter that has been temporarily set aside until the fate of SB 178 (Leno) is known. However, the issues raised in the EFF letter could also bear on the discussion of investigative subpoenas in the staff draft tentative report that is attached to Memorandum 2015-10. The remainder of this memorandum considers whether any of the points made in the EFF letter would warrant any changes to the draft report.

The memorandum first provides some general background on investigative subpoena use and revisits the discussion of that issue in the draft report. It then examines the main legal points made in the EFF letter and considers whether the Commission should revise the draft report in connection with those points. **The memorandum does not discuss the policy arguments made in the EFF letter, because the draft report does not make any policy recommendations. The**

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.

Commission should consider the policy arguments when it begins drafting proposed legislation.

BACKGROUND

The federal Stored Communications Act (hereafter "SCA") expressly permits the use of an administrative or grand jury subpoena to obtain stored communication *content*,[2] with one exception. Such a subpoena cannot be used to obtain the content of "electronic communication service" information that has been stored for 180 days or less.[3] For the most part, the SCA does *not* permit the use of such a subpoena to access stored *non-content* information (hereafter "metadata").[4] However, there is a narrow exception. Such a subpoena can be used to obtain a specified subset of metadata.[5]

The courts have generally held that the use of an administrative or grand jury subpoena to obtain records does not violate the Fourth Amendment of the United States Constitution or Article I, Section 13 of the California Constitution. This is true, notwithstanding the fact that such a subpoena need not be based on probable cause and is served without advance court authorization.

The use of investigative subpoenas is discussed at pages 17-18 of the staff draft tentative report:

> ***Investigative Subpoena***
>
> A warrant is not the only constitutionally sufficient authority to conduct a search that is governed by the Fourth Amendment and Article I, Section 13 of the California Constitution. In some circumstances, a search pursuant to an investigative subpoena *duces tecum*,[51] issued by a grand jury or an administrative agency, can also be constitutionally reasonable.
>
> > [T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists. [52]
>
> However, a grand jury subpoena must be reasonable. In *Hale v. Henkel*, the Court held that a grand jury's subpoena *duces tecum* was unreasonable under the Fourth Amendment because it was "too sweeping in its terms" and violated "the general principle of law

2. 18 U.S.C. § 2703(a) & (b)(1)(B)
3. 18 U.S.C. § 2703(a).
4. 18 U.S.C. § 2703(c)(1).
5. 18 U.S.C. § 2703(c)(2).

with regard to the particularity required in the description of documents necessary to a search warrant or subpoena." [53]

The same general principles apply to a subpoena *duces tecum* issued by an administrative agency that is investigating a possible violation of the laws that it enforces. The use of such a subpoena to compel the production of evidence (rather than a warrant) does not violate the Fourth Amendment, so long as the subpoena is authorized, sufficiently definite, and reasonable:

> Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant. [54]

---

[51]/ This report does not consider the use of a subpoena as an instrument of discovery in a pending adjudicative proceeding.

[52]/United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991).

[53]/201 U.S. 43, 76-77 (1906).

[54]/ Brovelli v. Superior Court, 56 Cal. 2d 524, 529 (1961) (citing United States v. Morton Salt Co., 338 U.S. 632, 651-54 (1950)); see also Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.").

The report goes on, at pages 18-20, to discuss an issue that has been raised more than once in this study — the possibility that the use of an investigative subpoena to obtain customer records from a communication service provider *without advance notice to the customer* would violate Article I, Section 13.

> Some courts have held that the constitutional reasonableness of a search pursuant to a subpoena *duces tecum* depends on the fact that the person whose records would be searched has notice and an opportunity for judicial review before any records are actually seized.
>
> > While the Fourth Amendment protects people "against unreasonable searches and seizures," it imposes a probable cause requirement only on the issuance of warrants. Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment (protecting the people against "unreasonable searches and seizures"), not by the probable cause requirement.
> >
> > A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued without prior notice and is executed, often by force,

> with an unannounced and unanticipated physical intrusion. Because this intrusion is both an immediate and substantial invasion of privacy, a warrant may be issued only by a judicial officer upon a demonstration of probable cause — the safeguard required by the Fourth Amendment.
>
> *A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.*
>
> In short, the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded. And while a challenge to a warrant questions the actual search or seizure under the probable cause standard, a challenge to a subpoena is conducted through the adversarial process, questioning the reasonableness of the subpoena's command. [55]

Advance notice and an opportunity for judicial review before records are searched are a routine feature of the procedure for issuance and execution of an investigative subpoena *duces tecum*, [56] when the subpoena is used to search records that are held by the person whose records are to be searched. But when a subpoena is instead served on a third party service provider, to search a customer's records, that customer may not receive any notice of the search or an opportunity for judicial review of the constitutionality of the search. In such a situation, only the service provider has an opportunity for judicial review of the subpoena. The service provider is not an adequate surrogate to protect the interests of the customer. The service provider may have no reason to object to the search, is usually shielded from liability for complying with the subpoena, and in some circumstances, may be legally prohibited from notifying the customer. [56]

The Commission has not found any case of the United States or California Supreme Courts expressly holding that the use of an investigative subpoena *duces tecum*, without notice to the person whose records are to be searched, would violate the Fourth Amendment or Article I, Section 13 of the California Constitution. However, that conclusion could perhaps be drawn from the cases that explain why the use of a subpoena is constitutionally permissible.

55/ *In re* Subpoena Duces Tecum, 228 F.3d 341, 347-48 (4th. Cir. 2000) (citations omitted) (emphasis added). See also People v. West

Coast Shows, Inc., 10 Cal. App. 3d 462, 470, (1970) ("the Government Code provides an opportunity for adjudication of all claimed constitutional and legal rights before one is required to obey the command of a subpoena duces tecum issued for investigative purposes").

56/ See People v. Blair, 25 Cal. 3d 640, 651 (1979) ("The issuance of a subpoena duces tecum [by a grand jury] pursuant to section 1326 of the Penal Code … is purely a ministerial act and does not constitute legal process in the sense that it entitles the person on whose behalf it is issued to obtain access to the records described therein until a judicial determination has been made that the person is legally entitled to receive them."); Gov't Code § 11188 (judicial hearing to review and enforce administrative subpoena).

57/ See, e.g., 18 U.S.C. § 2705(b).

The remainder of this memorandum considers whether the issues raised in the EFF letter warrant any change in the discussion set out above.

LEGAL ISSUES

The draft report does not make any policy recommendations. Instead, it describes the existing constitutional and federal statutory law that is relevant to state or local agency access to customer records of communication service providers. Consequently, the only reason to revise the draft report in response to the EFF letter would be if the letter exposes a deficiency in the report's description of existing law. Most significantly, if the EFF letter demonstrates that the use of an investigative subpoena is unconstitutional in a way that is not adequately described in the draft report, that could warrant revision of the draft report.

The EFF letter raises three legal issues that could affect the constitutionality of investigative subpoena use. They relate to (1) the standard of review of an investigative subpoena, (2) the issuance of an investigative subpoena without prior court approval, and (3) the adequacy of judicial review of a subpoena served on a third party record holder.

Those issues are discussed below.

Standard of Review

The EFF letter suggests that providing "differing legal protections" for different types of searches would violate the Fourth Amendment.[6] The

6. See Exhibit p. 1.

implication is that the use of an investigative subpoena *duces tecum* would violate the Fourth Amendment and Article I, Section 13 because the standard of review for a subpoena is different from the standard of review for a warrant (i.e., a subpoena need not be grounded on probable cause).

The staff has not found any case holding that the use of an administrative or grand jury subpoena is incompatible with constitutional search and seizure requirements because of the standard of review that governs the use of a subpoena. To the contrary, the case law is fairly clear in holding that the use of a subpoena can be compatible with the Fourth Amendment and Article I, Section 13, notwithstanding the fact that probable cause is not required when using a subpoena. If there is a constitutional problem with subpoena use, it does not appear to be the standard of review. **The staff does not believe that this point requires any adjustment to the staff draft tentative report.**

Issuance Without Prior Court Approval

The EFF letter notes that "administrative and grand jury subpoenas may issue with no judicial involvement at all."[7] The letter suggests that this is unconstitutional, citing *People v. Blair*.[8]

It is correct that *People v. Blair* held that the use of a subpoena *duces tecum* without judicial involvement violated Article I, Section 13. But that case does not hold that judicial review *prior to issuance* of the subpoena is constitutionally necessary. The defect in *Blair* was that law enforcement circumvented the *post-issuance* judicial review that is required by statute in California.[9]

In California, a criminal subpoena *duces tecum* can be served without prior court approval. But the documents must be delivered to the court, which then has an opportunity to consider the legality of disclosing the records to law enforcement.[10] In *Blair*, the documents requested in two subpoenas were not delivered to the court, as required by law. Instead, they were provided directly to law enforcement.[11]

---

7. See Exhibit p. 2.
8. 25 Cal. 3d 640 (1979).
9. See Penal Code § 1326 (grand jury subpoena); see also Gov't Code § 11188 (judicial review review of administrative subpoena).
10. Kling v. Superior Ct., 50 Cal. 4th 1068, 1071 (2010) ("Under Penal Code section 1326, subdivision (c), a person or entity responding to a third party subpoena duces tecum in a criminal case must deliver the subject materials to the clerk of court so that the court can hold a hearing to determine whether the requesting party is entitled to receive them.").
11. *Blair*, 25 Cal. 3d at 650-51 ("As we have seen, Diner's Club, after having been served with a subpoena returnable before the court at defendant's preliminary hearing …, instead provided

That circumvention of the requirement that the documents be delivered to the court precluded pre-production judicial review of the legality of the subpoena. That appears to be the constitutional infirmity at issue in *Blair*. The staff does not read *Blair* as requiring *pre-issuance* judicial approval. Nor has the staff seen any case in which the court held that the lack of judicial review before an investigative subpoena is served violates the Fourth Amendment or Article I, Section 13. **The staff does not believe that this point requires any adjustment to the staff draft tentative report.**

Adequacy of Judicial Review of Third Party Subpoena

The EFF letter notes that there are different constitutional issues presented when a subpoena is served on a third party record holder, rather than directly on the person whose records are being sought. The letter suggests that this distinction informed the decision in *Blair*.

The staff agrees that there is an important distinction to be drawn between a subpoena that is served on the person whose records are sought and a subpoena served on a third party service provider, for the production of a customer's records. That distinction is the crux of the concern expressed in the draft report, about the possible unconstitutionality of an investigative subpoena that is served on a third party service provider without notice to the customer. However, the staff does not believe that this precise issue was presented or decided in *Blair*.

As discussed above, the constitutional problem in *Blair* was the complete lack of an opportunity for judicial review before the documents were provided to law enforcement. That broad procedural failure was sufficient to decide the case. It was not necessary for the court to consider whether the subpoenas would have been constitutional had the documents been provided to the court as required by the statute (but without notice to the affected customer). Consequently, that specific issue was not addressed in *Blair*. Nor has the staff seen any United States or California Supreme Court decision in which that specific issue was decided.

That is why the draft report does not reach a firm conclusion on the issue. It acknowledges the possibility that the use of a third party subpoena without notice to the customer violates constitutional search and seizure requirements. But the report also notes the lack of a clear precedent on the issue. **The staff**

[the documents] to the prosecuting attorney…."); 654-55 ("The subpoena was made returnable before either the grand jury or an agent of the Federal Bureau of Investigation and the documents were delivered by the telephone company to the agent.").

believes that this is a fair statement of existing law and does not believe that the draft report requires any adjustment on this issue.

CONCLUSION

The EFF letter raises an important issue that the Commission should revisit before it prepares proposed legislation in this study — whether to permit the use of an investigative subpoena to obtain customer records from a third party service provider, without advance notice to the customer. However, the Commission need not decide that issue now. The staff draft tentative report does not include any recommendations for proposed legislation. Moreover, the issue may be resolved before the Commission begins drafting, if SB 178 is enacted into law.

As discussed above, the staff does not see any need to revise the staff draft tentative report. However, the purpose of approving and circulating a *tentative* report is to solicit comment from experts and other interested persons before a final report is approved. If any person or group believes that the discussion of investigative subpoenas (or any other issue) could be improved, we would welcome that input. The Commission will consider all public comment on the content of the tentative report before approving a final report.

Respectfully submitted,

Brian Hebert
Executive Director

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

March 31, 2015 **VIA U.S. MAIL & EMAIL**

Brian Hebert
Executive Director
California Law Revision Commission
UC Davis School of Law, Rm. 1128
Davis, CA 95616
feedback@clrc.ca.gov
bhebert@clrc.ca.gov

RE: CLRC Study G-300: State & Local Agency Access to Customer Information from Communication Service Providers

Dear Mr. Hebert,

This letter, submitted by the Electronic Frontier Foundation ("EFF"), Asian Americans Advancing Justice—Asian Law Caucus, the Center for Democracy & Technology ("CDT"), the Council on American-Islamic Relations ("CAIR"), the First Amendment Coalition and the Media Alliance, responds to the California Law Revision Commission's Memorandum 2015-3, part of Study G-300, concerning State and Local Agency Access to Customer Information from Communication Service Providers.

We appreciate the CLRC's thoughtful consideration of the important issues raised by the increasingly digital world, and applaud the Commission's overall recognition that the privacy protections in the California state constitution apply not only to the contents of electronic communication, but to non-content metadata as well. We completely agree that the California Constitution requires law enforcement to obtain a search warrant in order to access content and non-content metadata from a communications service provider.

But we are concerned about the CLRC's recommendation that the content of communications stored electronically for more than 180 days should be obtainable with an administrative or grand jury subpoena. In our view, the contents of *all* electronic communications should be protected by a warrant requirement regardless of how long they have been in electronic storage.

A. The State and Federal Constitutions Require a Search Warrant for Access to the Contents of All Electronic Communications Regardless of How Long They Have Been in Electronic Storage.

As the Commission has recognized, creating differing legal protections based on the time a message has been stored electronically violates the Fourth Amendment to the U.S. Constitution.[1] The California Supreme Court in *People v. Blair*, 25 Cal.3d 640 (1979), rejected the "third party doctrine" as a limitation on the privacy rights in Article I, Section 13 of the California

[1] *See* Memorandum 2015-3, p. 10 (citing *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)); *see also id.* at p. 12.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 x117 fax +1 415 436 9993 web www.eff.org email hanni@eff.org

Constitution.[2] Californians clearly have an expectation of privacy in the contents of *all* their electronic communications, no matter how long they have been stored.

We agree with the Commission that the process specified in 18 U.S.C. § 2703(d), which allows access to certain communications and records without a probable cause warrant, likely violates Article I, Section 13.[3] Part of the Commission's rationale for preserving the 180-day dividing line is to permit administrative agencies and grand juries to use subpoenas to access the contents of electronic communications at some point. But such subpoenas are governed by a relevance standard that is even more relaxed than the legal standard for judicial orders set forth in § 2703(d). And despite the inadequacy of § 2703(d), at least that section requires law enforcement go before a judge in order to obtain records. In contrast, administrative and grand jury subpoenas may issue with no judicial involvement at all. It was for that specific reason the California Supreme Court concluded in *People v. Blair* that both administrative and grand jury subpoenas were inadequate to obtain telephone records because they lack "a judicial determination that law enforcement officials were entitled" to the records.[4]

Thus, if § 2703(d), despite the involvement of a judge, fails the state constitutional standard, grand jury and administrative subpoenas—which have a lower standard of review and no judicial oversight before issuance —are even more problematic under the state constitution.

This is particularly true because preserving the 180-day dividing line to facilitate administrative and grand jury access to the contents of older communications would untenably give older emails less legal protection than metadata. We agree with the Commission that the California Constitution requires law enforcement to use a warrant to obtain both the contents of communications and electronic communication metadata (apart from customer account information).[5] But creating a specific carve-out for the contents of communications creates logical inconsistencies as to what a warrant requirement does and does not protect. While the California Supreme Court case cited by the Commission, *Broveli v. Superior Court*, found the use of an administrative subpoena rather than a warrant satisfied the Fourth Amendment, that case involved a subpoena issued directly to the target of an investigation rather than a third party service provider.[6] As the California Supreme Court's subsequent decision in *Blair* makes clear, there are different constitutional interests at play when a subpoena is issued to a third party service provider, which is why *Blair* concluded a subpoena to a third party service provider violated the California constitution.

[2] *Id*. at p. 20-21.
[3] *Id.* at p. 20.
[4] *People v. Blair*, 25 Cal.3d 640, 655 (1979).
[5] Memorandum 2015-3, p. 31-32.
[6] *Broveli v. Superior Court*, 56 Cal.2d 524, 526 (1961).

B. Keeping the 180-Day Dividing Line to Facilitate Grand Jury and Administrative Access to Electronic Communications Is Unnecessary.

Contrary to the Commission's view, there are compelling reasons to prohibit the use of administrative and grand jury subpoenas as a means of accessing the contents of communications.

First, a warrant requirement would not prohibit an administrative agency or grand jury from subpoenaing the record holder directly to obtain the contents of communications. This is the procedure that currently exists for private parties. The federal Stored Communications Act ("SCA")[7] prohibits a service provider from disclosing the contents of electronic communications to civil litigants.[8] Courts have indicated that the proper way for a civil litigant to obtain the contents of communications is to issue a subpoena for the communication records to the *individual directly*.[9] The California Court of Appeal reached that exact result in *O'Grady v. Superior Court*,[10] quashing a civil subpoena issued to an email provider seeking the contents of specific emails. Analyzing the issue under the SCA, *O'Grady* noted

> Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure storage, and who should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent. This does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted.[11]

It is this procedure—going to the user directly rather than a third party service provider—that is contemplated in the very case cited by the commission, *Craib v. Bulmash*, which involved an administrative subpoena issued by the Division of Labor Standards to a *specific employer itself* rather than a third party holding records on behalf of the employer.[12]

---

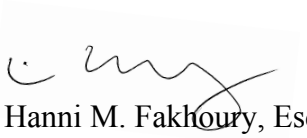
[7] 18 U.S.C. §§ 2701-2712.
[8] 18 U.S.C. § 2702(a); *see also Negro v. Superior Court*, 230 Cal.App.4th 879, 888 (2014).
[9] *See, e.g.*, *Mintz v. Mark Bartelstein & Assocs.*, 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Defendants may request documents reflecting the content of Plaintiff's relevant text messages, consistent with the SCA, by serving a request for production of documents on Plaintiff."); *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D.Mich. 2008) (ordering party to prepare discovery request to account holder rather than permitting issuance of a subpoena to communications service provider); *see also In re Subpoena Duces Tecum to AOL, LLC*, 550 F.Supp.2d 606 (E.D.Va. 2008) (AOL could not disclose emails via a civil subpoena); *FTC v. Sterling Precious Metals, LLC*, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013) (Consistent with the SCA, FTC could seek communications records information from user directly).
[10] 139 Cal.App.4th 1423 (2006).
[11] *O'Grady*, 139 Cal.App.4th at 1447.
[12] *Craib v. Bulmash*, 49 Cal.3d 475, 478-79 (1989).

Thus, given the Commission's finding that grand jury and administrative agency investigations are civil in nature,[13] the concern about maintaining their access to records "that the law requires to be kept, for regulatory purposes," can be addressed by following the same procedure civil litigants use: grand juries and administrative agencies may subpoena the *account holder* directly rather than the service provider to obtain the records.[14]

Additionally, there is simply no need to maintain the 180-day dividing line for grand juries specifically because they have an alternative means to gain access to the contents of communications. As the Commission has noted, while grand juries are not considered "peace officers" under California law, they can investigate crimes just as police do. In fact, the California Supreme Court in *Blair* specifically noted that "the prosecution 'is typically in complete control of the total process in the grand jury room' and that the grand jury is 'independent only in the sense that it is not formally attached to the prosecutor's office.'"[15] Because of this relationship and district attorneys' specific statutory permission to provide assistance to grand juries, there is simply no need to maintain the 180-day dividing line to facilitate grand jury access to the contents of communications.[16] Whenever a grand jury wants to review the contents of communications in connection with an active investigation, the District Attorney may apply for a search warrant on behalf of the grand jury and obtain communications contents from the service provider.

In sum, the 180-day dividing line should be completely eliminated and a search warrant should be required to access the contents of all communications, regardless of how long they have been in electronic storage, without any exception for grand jury or administrative subpoenas.

Sincerely,



Hanni M. Fakhoury, Esq.
Senior Staff Attorney
Electronic Frontier Foundation

[13] *See* Memorandum 2015-3, p. 22. On those occasions when an administrative enforcement officer acts as a "peace officer," he will be able to obtain a search warrant to access communications records from the service provider. *See id.* at p. 22 n. 75.
[14] Memorandum 2015-3, p. 24.
[15] *Blair*, 25 Cal.3d at 655 (quoting *Hawkins v. Superior Court*, 22 Cal.3d 584, 589 (1978)).
[16] Memorandum 2015-3, at p. 22, n. 76 (citing California Penal Code §§ 936, 939.1, 939.7).