Study G-300 July 31, 2020

Memorandum 2020-36

State and Local Agency Access to Customer Information from Communication Service Providers: Meaning of Interception

Memorandum 2020-20 reintroduced the Commission's study of government access to customer information from electronic communication service providers.[1] The memorandum provided an overview of the history of the study and a summary of the potential reforms that have not yet been addressed by the Commission. The staff is preparing a series of memoranda discussing those remaining issues in greater detail and presenting questions for Commission decision.

This memorandum discusses whether there need to be clarifying changes made to the meaning of "interception," as that term is used in California's wiretap statute.[2]

This is important because the Wiretap Act only applies to the "interception" of electronic communications. It is expressly inapplicable to "stored communications."[3]

That is a potential problem because federal courts have construed the term "interception" narrowly. Interception is limited to "acquisition contemporaneous with transmission." Any delay in acquisition will take it out of the definition of "interception," thereby exempting it from the stricter statutory protections that govern an interception.

That construction produces odd results, which may be inconsistent with the requirements of the Fourth Amendment of the United States Constitution. For example a court order authorizing law enforcement to read a target's text

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 Penal Code §§ 629.50-629.58.
3. See Penal Code § 629.51(b).

messages during their transmission would be an interception and the Wiretap Act's constitutionally-derived protections would apply.

If, instead, law enforcement were authorized to collect the target's text messages moments *after* they are delivered, that would not be an interception. Presumably, a regular search warrant would be required, rather than the more protective wiretap order.

The staff sees no good justification for that difference in treatment. This memorandum addresses that issue.

Unless otherwise indicated, all further statutory references in this memorandum are to the Penal Code.

SUPER-WARRANT REQUIREMENTS

In *Berger v. New York*,[4] the Court explained that an interception of communications is different from other types of searches, in ways that create special concerns with respect to the Fourth Amendment. Those special concerns require additional protections. For example:

- An authorized interception must not be indiscriminate. The warrant for an interception must describe with particularity the "things" (i.e., the conversations) to be seized. It is not sufficient to simply name the persons whose conversations will be intercepted. "[T]his does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized. As with general warrants this leaves too much to the discretion of the officer executing the order."[5]
- The period of authorized interception must not be overlong. Too long a period of authorization would be the "equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause. Prompt execution is also avoided. During such a long and continuous (24 hours a day) period the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation."[6]
- Because the success of real-time interception of communications depends on secrecy, there is no contemporaneous notice given to the target of the search, as there would be with a conventional

4. 388 U.S. 41 (1967).
5. *Id*. at 59.
6. *Id*.

search warrant. This lack of notice must be justified by some showing of exigent circumstances.[7]

Those concerns were directly addressed by Congress when it enacted a comprehensive wiretap statute.[8] That statute, which now applies to electronic communications as well as "wire" communications, requires the issuance of what is colloquially known as a "super-warrant" in order to authorize the interception of electronic and wire communications. The special requirements for issuing a super-warrant mitigate the constitutionally-based concerns described in *Berger*. For example:

- A federal wiretap order must include "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates."[9] In addition, "Every order and extension thereof shall contain a provision that the authorization to intercept … shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter…."[10] These minimization requirements help to safeguard against the indiscriminate interception of communications that are beyond the particular scope authorized by the warrant.
- The period of interception is limited. "Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable … and must terminate upon attainment of the authorized objective, or in any event in thirty days."[11] This also helps limit the indiscriminate collection of communications that are beyond the scope of authorization.
- The court must find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous…."[12] This exhaustion of alternatives helps to demonstrate exigent circumstances to justify the issuance of a warrant without contemporaneous notice to the subject of the warrant.
- Interception is only authorized in connection with a limited list of serious crimes.[13] This helps to mitigate all of the concerns discussed above, by limiting interception to unusually serious circumstances.

7. *Id*. at 60.
8. 18 U.S.C. § 2510 *et seq*.
9. 18 U.S.C. § 2518(4)(c).
10. 18 U.S.C. § 2518(5).
11. *Id*.
12. 18 U.S.C. § 2518(3)(c).
13. 18 U.S.C. § 2516(1)-(2).

California's wiretap statute imposes parallel requirements and limitations.[14]

"INTERCEPTION" AND MODERN ELECTRONIC COMMUNICATIONS

The concept of "interception" was fairly clear when *Berger* was decided. It necessarily involved contemporaneous access to communications *while they were in progress* (by either a wiretap or listening device).

That simplicity was lost with the advent of modern electronic communications. Electronic communication now typically involves the creation, delivery, and storage of *copies* of communication content, through a series of sequential steps. For example, when a person sends an email, the message content is sent from the sender's computer, to an email server, across the internet, to a destination server, and then to the recipient's computer. Copies are often retained, at least temporarily, at each step of that path.

When is accessing an electronic communication an interception? A number of federal courts have held that "interception," under the federal Wiretap Act, requires "acquisition contemporaneous with transmission."[15] Thus, access to electronic communications *after* transmission is not an interception. Instead, it is a search of stored communications.

How much delay between transmission and acquisition is enough to take the access out of the definition of "interception?" The courts have varied slightly on that point. Some have allowed a brief interval. For example, in *U.S. v. Szymuszkiewicz* the defendant had installed a forwarding rule on a supervisor's computer, so as to receive forwarded copies of all email sent to or by the supervisor. Despite the fact that there was a slight delay involved in forwarding these copies, the court held that this was an interception. The defendant "would have received each message with no more than an eyeblink in between. That's contemporaneous by any standard."[16] Under similar facts, a federal trial court in California held that email forwarding was not an interception.[17]

---

14. See Sections 629.50(a)(4) (particularity); 629.52(a) (limitation to specified crimes), (d) (exhaustion of alternatives); 629.58 (duration and minimization); 629.80 (minimization regarding privileged communications).
15. Konop v. Hawaii Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). See also Epstein v. Epstein, 843 F.3d 1147 (7th Cir. 2016); U.S. v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003), as amended (Jan. 20, 2004); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).
16. U.S. v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010).
17. Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148 (C.D. Cal. 2007).

In a First Circuit decision, the court briefly discussed, but did not decide, whether "transmission" of an electronic communication continues until a communication reaches its final destination (as compared to receipt and storage at various waypoints along the path to the ultimate destination). "[W]e need not and do not plunge into that morass."[18]

Another court has gone so far as to suggest that the contemporaneous acquisition requirement makes it virtually impossible to "intercept" email under the Wiretap Act:

> There is only a narrow window during which an E-Mail interception may occur — the seconds or milli-seconds before which a newly composed message is saved to any temporary location following a send command. … [I]nterception of E-mail within the prohibition of the Wiretap Act is virtually impossible.[19]

Finally, one court concluded that the existing understanding of "interception" is at odds with Congress' intention to extend Wiretap Act to electronic communications, but that "it is for Congress to cover the bases untouched."[20]

THE NATURE OF THE PROBLEM

In the staff's view, the prevailing federal interpretation of "interception" as used in the Wiretap Act is problematic. Under that interpretation, law enforcement could theoretically avoid super-warrant requirements for a de facto interception of electronic communications, simply by ordering a service provider to use message forwarding (after a brief delay) rather than immediate acquisition during transmission.

The staff does not see a good reason for conditioning the application of the Wiretap Act's constitutionally-derived protections on whether acquisition is immediate or slightly delayed.

While the staff is convinced that there is a significant logical problem in the prevailing federal understanding of "interception," it is not clear that this has caused actual problems in the area being examined in this study — government access to electronic communications from communication service providers. There are two reasons why such problems may not be occurring in practice.

---

18. United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005).
19. United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (quoting Jarrod J. White, *E–Mail @Work.com: Employer Monitoring of Employee E–Mail*, 48 Ala. L. Rev. 1079, 1083 (1997) (brackets omitted)).
20. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003).

Cases not Clearly Apposite

With one exception, the federal cases discussed in this memorandum involve *private* misconduct, rather than an authorized law enforcement search. Consequently, those cases do not directly discuss how the concept of interception should be understood in the law enforcement context.

The exception is *Steve Jackson Games, Inc. v. U.S. Secret Service*.[21] However, that case was decided in 1994, at the dawn of the modern Internet era. It involved a physical seizure of computer equipment, to search all of the messages that had been stored prior to the seizure, rather than a request for an ongoing "tap" on electronic communications for a period of time into the future. It is therefore not squarely on all fours with the issue discussed here.

It may be that a case involving the exact scenario discussed in this memorandum — law enforcement's use of a warrant, rather than a super-warrant, to conduct a de facto interception of electronic communications — might yield a better result.

Practical Constraints on Problem

There are practical reasons why the scenario discussed in this memorandum might not actually arise in practice.

For the problem to occur, a court would need to issue a regular search warrant for a search that authorizes the collection of future communications over a period of time. A court might well balk at doing so, because such a search would appear, on its face, to be an interception that is governed by the Wiretap Act.

Even if a court were willing to issue such a warrant, it might not provide a practicable way around the Wiretap Act. Recall that the effectiveness of an interception depends on secrecy. If a target knows that communications are being intercepted, the target will halt any compromising communication. That is why the Wiretap Act allows interception without contemporaneous notice to the target (with a showing of necessity).

A regular warrant for a search of stored electronic communications does not have an equivalent secrecy rule. Except in emergencies, contemporaneous notice to a target is required when a warrant authorizing a search of electronic records is issued.[22] That would largely close the theoretical "loophole" discussed in this

21. 36 F.3d 457 (5th Cir. 1994).
22. Section 1546.2.

memorandum. If law enforcement wishes to conduct a *surreptitious* interception of electronic communications, it would need a super-warrant under the Wiretap Act.

For all of those reasons, it may be that the problem identified in this memorandum does not occur in actual practice. It seems likely that law enforcement is routinely using the Wiretap Act when it wishes to conduct a surreptitious interception of electronic communications, even if the search involves delays between transmission and acquisition.

POSSIBLE REFORM

Prior Commission materials have proposed a possible alternative interpretation of "interception" that seems more compatible with the concerns outlined in *Berger v. New York*[23]

Rather than require that an interception be contemporaneous with transmission, California law could provide that an interception, for the purposes of the California Wiretap Act, is the acquisition of electronic communications that occur after the acquisition is authorized by the court.

In other words, if the court authorizes the collection of electronic communications prospectively, for a period of time into the future, that would be an interception. If instead the court authorizes the collection of electronic communications that already exist at the time that the warrant is issued, that would not be an interception; it would be a regular search of stored communications.

Consider how such a rule would map onto the concerns identified in *Berger*:

- **An authorized interception must not be indiscriminate.**[24]

  This is a concern when a warrant authorizes the prospective collection of communications that have not yet occurred. The exact scope of communications collected under such a search is not known at the time of authorization. The search may sweep in irrelevant communications. For that reason, it is important to precisely prescribe the kinds of communications to be collected and provide procedures for minimization of the collection of irrelevant communications. The super-warrant requirements would address that issue.

23. 388 U.S. 41 (1967).
24. *Id*. at 59.

This is not a concern when collecting communications that occurred before the search is authorized. Such records can be described with sufficient particularity at the time that the search is authorized, because they already exist. This is functionally the same as a search of existing physical records. Super-warrant requirements would not be needed.

- **The period of authorized interception must not be overlong.**[25]

  This is a concern when a warrant authorizes the prospective collection of communications that have not yet occurred. A time limit must be imposed on such a search, to avoid the "equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause."[26] Super-warrant requirements would address that issue.

  This is not a concern when collecting communications that occurred before the search is authorized. Because such a search would be a one-time search of specifically identified communications, the question of duration would be irrelevant. Super-warrant requirements would not be needed.

- **An interception without contemporaneous notice to the target must be justified by exigent circumstances.**[27]

  This is a concern when a warrant authorizes the prospective collection of communications that have not yet occurred. As with the tap of a phone line, the efficacy of such a search will depend on the target remaining unaware that the search is occurring. Thus, such a search may be authorized without contemporaneous notice to the target. As with a traditional wiretap, that should only be done on a sufficient showing of exigent circumstances. The super-warrant requirements would address this.

  This is not a concern when collecting communications that occurred before the search is authorized. There is no reason that notice cannot be given at the time of the search, so long as the records are secured against destruction before they can be accessed. Again, this is equivalent to a search of physical records. Super-warrant requirements would not be required.

As can be seen, the use of a prospective/retrospective distinction in construing the meaning of interception would be a good fit for the existing super-warrant protections, in a way that the federal contemporaneous acquisition rule is not.

25. *Id*.
26. *Id*.
27. *Id*. at 60.

When the reform described above was presented in Memorandum 2020-30, it prompted the following comment from ACLU-NC:

> 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.[28]

CONCLUSION

The staff sees a logical problem in the prevailing federal understanding of "interception," as that term is used in the Wiretap Act. It turns on a distinction — acquisition contemporaneous with transmission — that made sense in the era of wiretaps and listening devices. But with the advent of modern electronic communications, that concept now seems to have come uncoupled from the special concerns that were identified in *Berger v. New York*.

The concerns discussed in *Berger* all seem to depend on one essential characteristic that is inherent in the use of wiretaps and listening devices: Such surveillance will necessarily intercept communications that occur *after* the surveillance is authorized by a court and will continue for some span of time. This means that the authorizing court cannot know the exact nature of the communications that will be captured by the interception. This could lead to an unjustifiable invasion of privacy, with law enforcement capturing communications of innocent third parties that are unrelated to the purpose of the search. This is why the super-warrant provides special protections relating to specificity, minimization, duration, and necessity.

The staff does not believe that any of the special protections are needed when there is a search of records that already exist at the time that the search is authorized. In that situation, the court is dealing with a fixed universe of records, with known characteristics. The court can fashion its order to avoid overbreadth and protect privileged material. Contemporaneous notice can be given to the target.

That is why the staff originally proposed the reform discussed above. A definition of "interception" that only covers prospective searches of future communications would be a good fit for the Wiretap Act. The super-warrant

28. Memorandum 2020-30, Exhibit pp. 2-3.

requirements would be applied where they are needed to address the constitutional concerns identified in *Berger*, but would not be applied where they are not needed for that purpose.

However, the staff is becoming increasingly skeptical about whether the logical shortcomings of the prevailing definition of "interception" are causing any actual problems in the real world (at least with regard to law enforcement searches, the only application of the Wiretap Act that the Commission is authorized to study).

In addition, ACLU-NC does not favor the proposed reform. They believe it "would be in direct conflict with CalECPA's core principle of providing strong and consistent protections for all electronic information." The reform would solidify different treatment for different categories of searches, which ACLU-NC believes should be minimized.

In sum, while the proposed reform has logical appeal, it addresses a problem that is currently only theoretical (in the law enforcement context) and is seen by ACLU-NC as moving in the wrong direction with regard to the policies served by Cal-ECPA.

In light of all of that, the staff recommends that the Commission set the issue aside, without further work on the matter. If we later learn of actual problems involving the issues discussed here, the Commission could revisit the topic.

The staff also recommends against undertaking a study along the lines proposed by ACLU-NC, to apply super-warrant requirements to a search of stored electronic communications. As discussed above, the staff sees good reason for different treatment of a prospective interception and a retrospective search of already-existing records. The special concerns discussed in *Berger* apply to the former, but do not seem to apply to the latter.

Respectfully submitted,

Brian Hebert
Executive Director