Study G-300 September 25, 2020

Memorandum 2020-54

State and Local Agency Access to Customer Information from Communication Service Providers: Minimization

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 procedures used to minimize the interception of privileged communications when conducting an authorized interception of communications.

EXISTING MINIMIZATION REQUIREMENT

In California, there is a specific procedure that must be followed to minimize the collection of privileged communications when conducting an interception pursuant to a wiretap order. Penal Code Section 629.80 provides in relevant part:

> When a peace officer or federal law enforcement officer, while engaged in intercepting wire or electronic communications in the manner authorized by this chapter, intercepts wire or electronic communications that are of a privileged nature he or she shall immediately cease the interception for at least two minutes. After a period of at least two minutes, interception may be resumed for up to 30 seconds during which time the officer shall determine if the nature of the communication is still privileged. If still of a privileged nature, the officer shall again cease interception for at

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.

> least two minutes, after which the officer may again resume interception for up to 30 seconds to redetermine the nature of the communication. The officer shall continue to go online and offline in this manner until the time that the communication is no longer privileged or the communication ends. The recording device shall be metered so as to authenticate upon review that interruptions occurred as set forth in this chapter.

For example, if law enforcement is tapping a target's phone and hears that the target is talking to her attorney about matters within the scope of the attorney-client privilege, the officer would be required to suspend the wiretap for two minutes. The officer could then reactivate the wiretap and listen for up to 30 seconds to see if the two are still talking about privileged matters. If so, the wiretap would again be suspended for two minutes. This would continue until the target is no longer talking about matters within the scope of the privilege.

That sort of intermittent sampling, with specified intervals, should be practicable when intercepting a *streaming* communication, such as a telephone call or a videoconference. Law enforcement would simply dip in and out of the stream at the specified intervals. During the two-minute intervals when interception is suspended, the communication would not be captured at all, thereby minimizing government access to privileged content.

It should be emphasized that this procedure operates *at the time that communications are being seized*. It therefore operates to minimize the extent to which law enforcement has *any* access to privileged content. That effect of keeping privileged content away from the eyes of law enforcement could not be achieved by allowing unrestricted seizure of communications, followed by judicial review on the issue of privilege. While the latter would be helpful in preventing the improper introduction of privileged material as evidence in a trial, it would still allow law enforcement to learn the content of privileged communications at the time that they are seized.

The remainder of this memorandum considers how to approximate the effect of Section 629.80 when the communications being seized are asynchronous (i.e., they are communications that consist of a series of separate messages delivered at different times, rather than a continuous stream of content). For example, suppose that law enforcement is authorized by a wiretap order to intercept a person's email or text messages over a specified period of time. How can law enforcement access to privileged content in those messages be minimized at the time of interception?

IMPRACTICABILITY OF APPLYING TIME-BASED MINIMIZATION METHOD TO ASYNCHRONOUS COMMUNICATION

Although Section 629.80 expressly applies to the interception of "electronic communications," it is not at all clear how the minimization procedure required by that section would work when the content being intercepted is asynchronous (e.g., email or text messages).

For example, if law enforcement is authorized to intercept email messages that are sent or received by a particular person, what would happen if an officer reads an email message and finds that it contains privileged content? In that situation, the requirement that law enforcement "cease the interception for at least two minutes" makes no sense. Would the officer simply sit back and wait two minutes before continuing to read the email? Or would the rule preclude reading any email that was created within two minutes of the one that contained privileged content? Those possibilities seem nonsensical, in terms of the purpose of the minimization requirement.

It is not clear that a time-based screening method could be effectively applied to asynchronous communications.

POSSIBLE ALTERNATIVE MEANS OF ACHIEVING MINIMIZATION

Electronic communications have a feature that might provide a practicable way to screen out privileged content at the time of interception. Typically, asynchronous electronic communications include what is known as "metadata" (i.e., data about data). Metadata describes various attributes of a message *other than its content* (e.g., sender, recipient, subject, time sent, name of attached files, etc.).

In some cases, the metadata for a message could signal the likelihood that the message contains privileged material. For example, it is likely that an email sent by a person to the person's attorney will contain material that is covered by the attorney-client privilege. The law could prescribe special procedures for how law enforcement handles a message in that situation.

Such a statute would have two main elements:

(1) A standard to determine when a message requires special handling.
(2) A rule for how such messages are to be handled.

Standard for Special Handling

The staff believes that any standard used in such a law should be based on a bright-line rule. Law enforcement should not be required to make a qualitative judgment about the strength of any metadata evidence suggesting that a message might be privileged. That could be unduly burdensome, especially when processing a large volume of messages. It would also heighten the risk of error and uncertainty, which would increase the likelihood of litigation contesting individual decisions.

A fairly straightforward standard would turn on whether a message was sent to or received by persons known by law enforcement to be in a privileged relationship. That rule could be administered very simply, by searching the metadata for the name or address of such persons. For example, if law enforcement knows the email address of a suspect's attorney, it would be a simple matter to search for all messages that include that address in the sender or recipient metadata. Those messages could be easily segregated for special handling, without accessing their content.

The staff is drawn to the simplicity of this approach.

Special Handling Procedure

Once a set of messages has been identified for special handling, what treatment should they receive? Two possibilities are discussed below.

Embargo

The most straightforward approach would be a simple prohibition — law enforcement cannot access the content of the messages at issue. On determining that they meet the standard for special handling, they would be sealed and turned over to the court, unread.

This would be highly protective of privileged material. It would also be very simple to administer.

However, there is a downside to the "embargo" approach — it would be overbroad. Communications between two people in a privileged relationship are not necessarily privileged. For example, communication between an attorney and client is not privileged "if the services of the lawyer were sought or obtained to enable or aid anyone to commit or plan to commit a crime or a fraud."[2] Under the embargo approach, a message between attorney and client that falls into the

2. Penal Code § 629.68.

crime/fraud exception would be unavailable to law enforcement, even though there is no privilege to justify that result. This could deny law enforcement evidence to which they should properly have access.

One way to mitigate that overbreadth would be to authorize law enforcement to petition the court for a determination of the extent to which embargoed communications are privileged. Material that is not found by the court to be privileged could be returned to law enforcement for their use.

If the Commission decides to pursue this approach, the staff would need to do further research to consider how to structure a court review process in this context.

Special Master

Another alternative would be to require that messages that meet the standard for special handling be turned over to a special master, unread. The special master could then review the content of the messages and determine the extent to which they contain privileged content. Content that is privileged would be sealed and delivered to the court. Unprivileged content would be returned to law enforcement for their use.

This would avoid the overbreadth of the embargo approach. A neutral would make preliminary decisions on the privilege issue, which would allow unprivileged communications to be returned to law enforcement for their use.

The most significant downside to this approach would be its cost and delay.

There are precedents in existing law for the use of a special master to perform such a function:

- The California Electronic Communications Privacy Act (Cal-ECPA) allows for the appointment of a special master when electronic records are searched, in order to ensure that only information necessary to achieve the objective of the warrant or order is produced or accessed.[3] It may be that this authority could be used to achieve the kind of screening discussed above, on a case-by-case basis.
- Existing Penal Code Section 1524(c) requires the use of a special master when a search warrant is used to seize documentary evidence from the office of an attorney, physician, psychotherapist, or member of the clergy. If the person served with the warrant asserts that a particular document is privileged,

3. Penal Code § 1546.1(e)(1).

the special master seals it and delivers it to the court for a hearing on the privilege issue.

- A court has inherent power to appoint a special master to screen seized communications to determine the extent of any privilege.[4]

However, there is an important restriction on the functions that can be assigned to a special master.

> The California Constitution imposes limitations upon the power of nonjudicial officers to exercise judicial functions. "The judicial power of this State is vested in the Supreme Court, courts of appeal, superior courts, and municipal courts." (Cal. Const., art. VI, § 1.) To avoid an unconstitutional delegation of judicial authority, the Constitution requires the stipulation of the parties before a trial court may refer a cause to be tried by a referee. (*Id.*, § 21; *In re Edgar M.* (1975) 14 Cal.3d 727, 732, 122 Cal.Rptr. 574, 537 P.2d 406.) Such a referral of the entire case, with the consent of the parties, is known as a general reference and results in a binding determination by the referee.[5]

Because the proposed special master procedure would be based on statute, rather than a stipulation of all parties, it could not be structured as a general reference in which the special master makes final adjudicative decisions. Instead, the special master could make provisional decisions, which would be subject to judicial review before having binding effect. "Masters and referees perform subordinate judicial duties only if their findings and recommendations are advisory and not binding until adopted by the court."[6]

Again, if the Commission is interested in pursuing this option, the staff would need to do more research as to the proper form of judicial proceeding to be used in this context.

CONCLUSION

It seems likely that the minimization procedure used during a wiretap pursuant to Section 629.80 would not be workable when conducting an interception of asynchronous electronic communications. The notion of timed interruptions has no practical application in that context.

This memorandum discusses whether it might be possible to craft a different approach to achieve the same general effect, minimization of law enforcement

4. People v. Superior Court (Laff), 25 Cal. 4th 703, 732 (2001).
5. *Id*. at 721.
6. *Id*.

access to privileged communications during the conduct of a search. The goal would not be simply keeping privileged communications from being used as evidence at trial. The goal would be to minimize law enforcement access to the content of privileged communications.

The memorandum proposes that metadata be used by law enforcement to identify electronic communications that are likely to contain privileged material, without accessing the content of those communications.

Those communications could then be either (1) embargoed, subject to judicial review, or (2) turned over to a special master for preliminary screening, subject to judicial review.

The staff is open to other suggestions on how minimization of law enforcement access to privileged material could be achieved, when intercepting asynchronous communications.

The Commission needs to decide whether it is interested in doing further work on this topic. Before making that decision, it would be helpful to have comment from law enforcement and civil liberties experts on whether the problem discussed here is merely theoretical, or is an actual problem in practice.

In particular, the staff is interested in hearing how this issue is handled now. If law enforcement is conducting an authorized interception of asynchronous communications, how is law enforcement access to privileged content minimized? Is there some general rule of which the staff is unaware? Do individual judges impose tailored minimization requirements as a condition of the issuance of a warrant, on a case-by-case basis?

Until the Commission has such feedback, it might be prudent to pause work on this specific topic.

Respectfully submitted,

Brian Hebert
Executive Director