Study G-300 October 6, 2020

First Supplement to Memorandum 2020-54

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

The Commission[1] has received a letter from Mark J. Burnley, Assistant Head Deputy of the Los Angeles District Attorney's Office, Major Narcotics Division (hereafter "AHD Burnley"). The letter is attached as an Exhibit.

AHD Burnley writes to provide helpful background information and share his own opinion on the matters discussed in Memorandum 2020-54. *AHD Burnley is not writing on behalf of the Los Angeles District Attorney's office; he is speaking only for himself.*

The staff greatly appreciates the input. As acknowledged in Memorandum 2020-54, the staff is not sure that the issue discussed in the memorandum is enough of a problem in actual practice to justify further study. The memorandum specifically solicited "comment from law enforcement and civil liberties experts on whether the problem discussed here is merely theoretical, or is an actual problem in practice."[2]

AHD Burnley's letter is discussed briefly below.

General Issue

As a general matter, AHD Burnley agrees that Penal Code Section 629.80 is "inadequate to minimize electronic communications."[3] However, he disfavors the possible reforms discussed in the memorandum: "My fear is an unwieldy, impractical, and unnecessarily burdensome and unworkable statutory system is put in place to fix a problem that doesn't really exist."[4]

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. Memorandum 2020-54, p. 7.
3. See Exhibit p. 1.
4. *Id*. at 3.

General Minimization Requirements

Much of AHD Burnley's letter discusses the federal wiretap statute's general minimization provision:

> … Every order and extension thereof shall contain a provision that the [interception] shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter …[5]

California has a nearly identical provision generally requiring minimization.[6]

As AHD Burnley points out, the federal minimization statute has been judicially construed as requiring reasonableness, in light of the circumstances of each case:

> The United States Supreme Court has stressed that, because of the necessarily ad hoc nature of any determination of reasonableness, there can be no inflexible rule of law that will decide every case. (U.S. v. Scott, supra, 436 U.S. at 139.) Instead, the question whether the government complied with the statutory requirement to minimize surveillance by wiretap requires examination of the monitoring officers' conduct in light of the particular circumstances of the case. (Id. at p. 140.)[7]

California's general minimization statute has been similarly construed:

> The government is required to adopt reasonable measures to reduce the interception of conversations unrelated to the criminal activity under investigation to a practical minimum while permitting the government to pursue legitimate investigation. The standard for minimization is reasonableness. Reasonableness is determined from the facts of each case. (People v. Roberts (2010) 184 Cal.App.4th 1149, 1174.)[8]

However, those provisions are not directly analogous to the provision that is at the heart of this study, Penal Code Section 629.80. They impose a general minimization requirement, without prescribing any particular minimization method.

By contrast, Penal Code Section 629.80 has a narrower objective, minimizing the interception of *privileged* communications, and it *does* prescribe a specific minimization procedure — the time-based sampling method described in Memorandum 2020-54.

---

5. 18 U.S.C. § 2518(5).
6. Penal Code § 629.58.
7. See Exhibit pp. 1-2.
8. See Exhibit p. 1.

Despite that dissimilarity, there is an important point that can be drawn from examination of the general minimization statutes. They may provide an answer to a question that the staff asked in Memorandum 2020-54:

> If law enforcement is conducting an authorized interception of asynchronous communications, how is law enforcement access to privileged content minimized?

The answer may be that law enforcement falls back onto the general minimization statute's requirements, and "adopts reasonable measures" to minimize the interception of privileged content, tailored to the circumstances of the case. **If that is correct, it would be helpful to hear more detail about how this works in practice. What kinds of "reasonable measures" are used?**

Overbreadth

AHD Burnley is concerned that simply requiring law enforcement to screen the metadata for intercepted communications, in order to seal any communications between persons in a privileged relationship, would have overbroad results. "Basing the minimization simply on metadata overlooks the crime-fraud exception in Evidence Code Section 956. It goes well beyond the procedure set forth in PC 629.80."[9]

Memorandum 2020-54 makes the same point.[10]

Inconsistent Treatment

AHD Burnley objects to different treatment of different modes of communication:

> There should be no difference in how communications are treated based on how they are transmitted — emails or texts should not be given heightened protection over real-time aural communications.[11]

As a general matter, the staff agrees. That is largely the point of this study. Is it possible to give asynchronous communications approximately the same level of protection against the interception of privileged communications that is currently provided to streaming content? Under existing law, it appears that they receive very different levels of protection.

9. See Exhibit p. 1.
10. See Memorandum 2020-54, pp. 4-5.
11. See Exhibit p. 1.

Burdens

AHD Burnley asserts that any procedure that relies on a judicial hearing or the use of a special master to screen out privileged content would be unduly burdensome and slow:

> A court review or special master process would not only be expensive, but would take too long to administer. Time is frequently of the essence during wiretaps.[12]

The staff does not dispute that point, but sees a possible counter-argument. Existing Penal Code Section 1524(c) and (d) require the use of a special master to screen documents seized from the office of an attorney, physician, psychotherapist, or member of the clergy. This suggests that the Legislature has already balanced the cost and delay of special master screening against the value of protecting privileged communications and has decided that the latter is more important.

On the other hand, Section 1524 involves a regular search warrant rather than a wiretap. AHD Burnley may be correct that circumstances involving a wiretap typically involve a greater degree of urgency. If so, that could shift the policy balance that seems to have been struck in Section 1524.

Possible Alternative

Finally, AHD Burnley raises another possibility that is worth considering.[13] It might be workable to require that asynchronous communications between persons in a privileged relationship be reviewed by a law enforcement "monitor." That person would be allowed to review the entire content of the message to determine the extent to which it is privileged. Privileged content would be withheld and sealed. Unprivileged content would be returned to investigators for their use. The success of that approach would depend on a strict separation of functions. The monitor should not be permitted to divulge anything about the privileged content to investigators.

12. See Exhibit p. 1. AHD Burnley also points out another obstacle with use of a special master, wiretap communications are sealed pursuant to Penal Code Section 629.66. That issue could be addressed later, if the Commission decides to proceed with a reform of the type discussed in Memorandum 2020-54.
13. See Exhibit pp. 2-3.

Such an approach would likely be less costly and slow than seeking a judicial determination or referring documents to an outside special master for review.

Respectfully submitted,

Brian Hebert
Executive Director

EMAIL FROM MARK BURNLEY
(10/6/20)

Mr. Hebert,

I reviewed Memorandum 2020-54 and have some questions/concerns.

I agree the procedure set forth in Penal Code section 629.80 is inadequate to minimize electronic communications.

However, the suggested procedures are impractical. Basing the minimization simply on metadata overlooks the crime-fraud exception in Evidence Code section 956. It also goes well beyond the procedure set forth in PC 629.80. There should no difference in how communications are treated based on how they are transmitted – emails or texts should not be given heightened protection over real-time aural communications. Sophisticated criminals could disguise the metadata so it appears to be from a privilege holder when in reality it is not. This suggested procedure also makes a lot of assumptions about the software used by law enforcement to intercept wire and electronic communications.

A court review or special master process would not only be expensive, but would take too long to administer. Time is frequently of the essence during wiretaps. A special master is impractical, because wiretaps are sealed per PC 629.66 and intercepts cannot be disclosed except under certain enumerated circumstances.

The government is required to adopt reasonable measures to reduce the interception of conversations unrelated to the criminal activity under investigation to a practical minimum while permitting the government to pursue legitimate investigation. The standard for minimization is reasonableness. Reasonableness is determined from the facts of each case. (*People v. Roberts* (2010) 184 Cal.App.4th 1149, 1174.)

The Ninth Circuit recognized the electronic communication minimization issue in *U.S.* v. *McGuire* (9th Cir. 2002) 307 F.3d 1192. As part of an investigation into the "Montana Freemen," the FBI obtained federal wiretaps. (*Id.* at p. 1196.) The court addressed the issue of what minimization procedures are required for fax interceptions. Like Penal Code section 629.58, Title III requires that wiretapping or electronic surveillance "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." (18 U.S.C. § 2518(5); *Scott v. United States (1978)* 436 U.S. 128, 130.)

The Ninth Circuit noted the general requirements of the wiretap law, as explained by controlling precedent, are clear. Minimization requires that the government adopt reasonable measures to reduce to a practical minimum the interception of conversations unrelated to the criminal activity under investigation while permitting the government to pursue legitimate investigation. (*U.S.* v. *Torres (*9th Cir. 1990*)* 908 F.2d 1417, 1423; *United States v. Santora (*9th Cir. 1979*)*600 F.2d 1317, 1320.) The United States Supreme Court has stressed that, because of the necessarily ad hoc nature of any determination of reasonableness, there can be no inflexible rule of law that will decide every case. (*U.S.* v. *Scott, supra*, 436 U.S. at 139.) Instead, the

question whether the government complied with the statutory requirement to minimize surveillance by wiretap requires examination of the monitoring officers' conduct in light of the particular circumstances of the case. (*Id.* at p. 140.)

> The district court's wiretap order included the following minimization instructions:
>
> Each facsimile transmission will be printed on the machine used to intercept facsimile transmissions. The monitoring agent and [assistant United States attorney] will decide, based on the identities of the sender and recipient and the subject matter of the transmission, whether the facsimile appears to be pertinent to the criminal offenses listed in the court's order. If the facsimile does not appear to be pertinent, the intercepted transmission will be placed in an envelope and sealed. It will then be placed in a locked drawer until it is turned over to the court with the other intercepted transmissions after the interception order has expired. (*U.S.* v. *McGuire*, *supra*, 307 F.3d at p. 1200.)

The Ninth Circuit noted though it was unclear whether each fax was skimmed or read in its entirety before begin classified as pertinent or non-pertinent, the F.B.I. agents' conduct could not be "considered unreasonable on that ground alone." (*Ibid.*) The court also rejected the defense's argument that the agents should have looked at each fax transmission with a ruler in hand, reading line by line, and once it became apparent that language in a fax was not pertinent, the officials should have skipped about thirty lines and then continued reading, line by line, until they reached the end of the transmission. (*Id.* at p. 1202.)

The court quoted the Senate Judiciary Committee's legislative history of the Electronic Communications Privacy Act:

> It is impossible to "listen" to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. For instance, a page displayed on a screen during a computer transmission might have five paragraphs of which the second and third are relevant to the investigation and the others are not. The printing technology is such that the whole page including the irrelevant paragraphs, would have to be printed and read, before anything can be done about minimization.
>
> Thus, minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation. (*Ibid.*)

The court ultimately concluded the procedures used in *McGuire* to minimize the fax transmissions were reasonable. (*Ibid*.)

If any statutory changes are merited, I would urge the commission to determine whether this is in fact a serious issue. It would not be unreasonable for monitors to review all electronic communications and determine whether they are (1) pertinent and/or (2) privileged. Electronic

communications could be printed out and placed in a notebook that divides the messages into pertinent and non-pertinent categories. If an electronic communication is deemed non-pertinent, it should be designated as such and access shall be restricted. Privileged electronic communications could be handled in the same manner as privileged wire communications. Privileged communications would not be printed out but retained on the computer system. The wiretap monitors would be instructed not to pass privileged information to other monitors, law enforcement officers, or prosecutors.

My fear is an unwieldy, impractical, and unnecessarily burdensome and unworkable statutory system is put in place to fix a problem that doesn't really exist.

Mark J. Burnley, Assistant Head Deputy
Los Angeles County District Attorney's Office
Major Narcotics Division
211 W. Temple Street, 11th Floor
Los Angeles, CA 90012