Study G-300 October 15, 2020

Second Supplement to Memorandum 2020-54

State and Local Agency Access to Customer Information from Communication Service Providers: Minimization (Material Distributed at Meeting)

A letter from the American Civil Liberties Union of Northern California was distributed at the October 15, 2020, meeting of the California Law Revision Commission. It is attached as an Exhibit.

Respectfully submitted,

Brian Hebert
Executive Director

ACLU
AMERICAN CIVIL LIBERTIES UNION
Northern
California

California Law Revision Commission
c/o UC Davis School of Law
400 Mrak Hall Drive
Davis, CA 95616

October 14, 2020

Re: State and Local Agency Access to Customer Information from Communication Service Providers – Memoranda 2020-54, 2020-54a and 2020-55

Dear California Law Revision Commission:

We appreciate the Commission's ongoing efforts to review and modernize the laws governing electronic searches. We write today to recommend that the Commission continue its examination of minimization and notice. In particular, we urge the Commission to pursue solutions that ensure the privacy protections afforded to Californians are not determined by the mechanism employed by a government entity to access customer information held by service providers, but instead are consistent with the principles underlying CalECPA and the Fourth Amendment under all circumstances.

Below are our specific comments on the issues that the Commission has presented in its most recent memoranda:

1. Minimization and Privilege (Memoranda 2020-54 and 2020-54a)

Under the California Wiretap Act (as well as its federal counterpart), live interception of audio or video communications is subject to specific procedures requiring law enforcement to "sample" the communication (for up to 30 seconds) to determine whether the immediate communication is privileged, and to cease interception (for a minimum of 2 minutes) if so. As the Commission notes, this mechanism may not be applicable to asynchronous communications, particularly text-based communications such as SMS messages or email. Memorandum 2020-54 therefore considers alternative mechanisms for protecting privileged communications obtained via interception from "*any* access" by law enforcement, not merely from use as evidence at trial.

We encourage the Commission to continue its consideration of special masters as the best way to ensure consistent protection for all privileged communications, regardless of the time they were conducted or the mechanism used to obtain them from a service provider. As the Commission notes, current law, including CalECPA, provides for the appointment of a special master to screen electronic information or documentary evidence for privileged content when a search is conducted via search warrant. There is no reason that prospective collection of electronic communications should be afforded lesser safeguards.

Moreover, the use of the CalECPA approach is particularly appropriate since the "prospective" capture of text-based electronic communications can typically accomplished either via a wiretap "interception"

or via a combination of a retention order (requiring the target service to retain records) followed by a search warrant issued on the provider in the future.[1] Providing uniform protection for privileged information ensures that government officials cannot do not gain greater access to privileged information simply by obtaining a different form of court order to obtain the same result.

For that reason, we would encourage the Commission to continue to explore the use of special masters to safeguard privileged communications that might otherwise fall through the cracks of current protective procedures. Doing so would ensure consistent protection for all privileged communications, text or audiovisual, past or future.

2. Notice of Administrative Subpoena (Memorandum 2020-55)

The Commission has also raised the issue of notice to the consumer in the context of an administrative subpoena. We strongly encourage the Commission to continue this line of inquiry, both for the substantive reasons noted in the Memorandum and to ensure consistent privacy protections regardless of the government entity seeking the electronic communications.

As the Fourth Circuit noted and the Commission approvingly cited, one of the primary conceptual differences between a warrant and a subpoena is that the former allows no opportunity for the target to contest the search until after it happens, while the latter provides an opportunity to "challenge it in court before complying with its demands."[2] When a subpoena is issued on the target of an investigation, the target is in position to defend his own privacy via a motion to quash. However, a service provider that receives a subpoena seeking records about one of its customers is not required, and may choose not to, notify the customer. As the Commission points out, failing to do so renders compliance and disclosure not only inadequate as a privacy protection but constitutionally fraught.

In addition, providing notice to customers whose records are targeted by an administrative subpoena is consistent with the notice requirements for search warrants imposed by CalECPA.[3] Moreover, CalECPA's enforcement provisions are signed to allow any "individual whose information is targeted by .... legal process that is inconsistent with" its mandates to move to void or modify the warrant or order the destruction of any information so obtained. That right, however, depends on notice being given to the individual of the execution of legal process, which is not mandated under CalECPA for an administrative subpoena. We believe that it should be, and encourage the Commission to continue its research in that direction.

[1] This is generally true as well of "ephemeral" communications services, since by design such services lack access to unencrypted communications at any point and thus can neither retain nor facilitate the interception of such communications.

[2] Memorandum 2020-55 at 3 (quoting *In re Subpoena Duces Tecum*, 228 F.3d 341, 347-48 (4th. Cir. 2000)).

[3] *See* Penal Code § 1546.2(a)-(b).

We look forward to continuing the conversation about ways to ensure that California's electronic privacy laws continue to robustly safeguard the rights of Californians and keep pace with the ever-changing digital world.

Sincerely,

Chris Conley
Technology & Civil Liberties Attorney
ACLU of Northern California
415-621-2493 | cconley@aclunc.org