IN THE SUPREME COURT OF CALIFORNIA

FACEBOOK, INC.,
Petitioner,
v.
THE SUPERIOR COURT OF SAN DIEGO COUNTY,
Respondent;
LANCE TOUCHSTONE,
Real Party in Interest;
SUMMER STEPHAN,
as District Attorney, etc.,
Intervener.

S245203

Fourth Appellate District, Division One
D072171

San Diego County Superior Court
SCD268262

August 13, 2020 (reposting corrected version)

Chief Justice Cantil-Sakauye authored the opinion of the Court, in which Justices Chin, Corrigan, Liu, Cuéllar, Kruger and Groban concurred.

Chief Justice Cantil-Sakauye filed a concurring opinion.

Justice Cuéllar filed a concurring opinion.

FACEBOOK, INC. v. SUPERIOR COURT

S245203

Opinion of the Court by Cantil-Sakauye, C. J.

We granted review to address the propriety of a criminal defense subpoena served on Facebook, seeking restricted posts and private messages of one of its users who is also a victim and critical witness in the underlying attempted murder prosecution.

In addition to discussing the Fifth and Sixth Amendment issues presented in this and recent related litigation (*Facebook v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245 (*Facebook (Hunter)*), the parties raised four related preliminary legal issues, all potentially dispositive, in the course of their briefing.

In the meantime, our review of the record — including a key declaration and exhibits that had been presented to the trial court ex parte and sealed (and hence kept from Facebook, as well as from the prosecuting authority below, intervener San Diego County District Attorney (hereafter the district attorney)) — raised questions regarding whether this case presents an appropriate vehicle to resolve any of the earlier briefed legal issues. Specifically, our review raised the question whether the underlying subpoena was supported by good cause and, if not, whether the trial court's denial of Facebook's motion to quash the subpoena should be vacated and the matter remanded to the trial court for further proceedings regarding that motion.

Accordingly, after giving the parties notice and an opportunity to comment, we unsealed the declaration and

related exhibits, took judicial notice of the preliminary hearing transcript and related exhibits, and solicited supplemental briefing from all three parties concerning the adequacy of the justifications for the subpoena. In response, real party in interest Lance Touchstone, defendant in the prosecution below (hereafter defendant) filed a supplemental brief maintaining that the subpoena is supported by good cause, and that the trial court properly denied Facebook's motion to quash. By contrast, the supplemental briefs filed by Facebook and the district attorney contend that defendant failed to state sufficient justification for acquiring the sought communications, and that the subpoena is not supported by good cause. When it came time to file reply briefs in the latest round of briefing, Facebook and the district attorney did so, responding to defendant's arguments. Defendant did not file a reply.

The most recent briefing has not alleviated our initial questions concerning the viability of the underlying subpoena. As explained in greater detail below, the trial court erred by conducting an incomplete assessment of the relevant factors and interests when it found that defendant established good cause to acquire the sought communications from Facebook and denied Facebook's motion to quash. The trial court's misstep was understandable, given that (1) the trial court did not have the benefit of full adversarial engagement, (2) there is surprisingly little guidance in the case law and secondary literature with regard to the appropriate inquiry, and (3) this court has not previously articulated a clear roadmap or set of factors to be applied by trial courts in this context.

In this case, we will provide direction to the trial court and parties, both for the benefit of this litigation and other similar cases. In doing so we will highlight seven factors that a trial

court should explicitly consider and balance in ruling on a motion to quash a subpoena duces tecum directed to a third party. In the process we will reiterate our prior caution to trial courts against readily allowing a defendant seeking to enforce such a subpoena to proceed, as was done here, ex parte and under seal.

With regard to the other issues potentially presented by this case, we are generally reluctant to address significant substantive legal issues when, due to underlying factual and related problems, it may prove unnecessary to do so. Here, as we will explain, we are especially disinclined to resolve the important constitutional, statutory, and related issues addressed in the briefs when the underlying subpoena may not be enforceable for other reasons.

Ultimately, we will direct the Court of Appeal to remand this matter to the trial court with directions that the trial court vacate its order denying the motion to quash and conduct further proceedings consistent with the guidelines set forth in this opinion.

I. BACKGROUND AND UNDERLYING PROCEDURE

In *Facebook (Hunter), supra,* 4 Cal.5th 1245, we addressed issues concerning the propriety of criminal defense subpoenas served on social media entities, including Facebook, seeking restricted posts and private messages of two of their users. We held, in part, that to the extent such a subpoena seeks a communication that had been configured as and remained public, Facebook could not assert the federal Stored Communications Act (18 U.S.C. § 2701 et seq.; hereafter SCA or

Act) as a shield to block enforcement of the subpoena. (*Id*., at pp. 1250, 1262–1274.)

At the time when the proceeding in *Facebook (Hunter)*, *supra,* 4 Cal.5th 1245 was pending in this court, we granted review in this seemingly similar pretrial criminal discovery matter. In the present case, defendant is charged with shooting and attempting to murder Jeffrey Renteria. Defendant seeks all of Renteria's Facebook communications (including restricted posts and private messages) before and after the shooting.

Defendant argues that he needs all electronic communications by Renteria in order to prepare his defense in two respects: Primarily, he contends, he has a viable claim of *self-defense* against Renteria, and requires the communications to investigate and present that affirmative defense. Secondarily, or alternatively, he seeks to prepare to *impeach the character* of the anticipated main prosecution witness against him — the victim, Renteria — if, as expected, Renteria is called by the prosecution at trial.

Defendant asserts that to the extent the SCA allows Facebook to block his subpoena, the Act must be found to violate his federal Fifth Amendment due process rights, along with his Sixth Amendment rights of confrontation, cross-examination, and counsel — and hence the SCA is unconstitutional as applied to him. Defendant recognizes that in *People v. Hammon* (1997) 15 Cal.4th 1117, 1128, we declined to recognize such constitutional rights to pretrial discovery of statutorily privileged psychotherapy information. Yet, defendant contends, we should now limit or overrule this aspect of *Hammon*. These are essentially the same constitutional claims and arguments

that were presented, but not reached, in *Facebook (Hunter), supra,* 4 Cal.5th 1245.

The Court of Appeal below, observing that *Facebook (Hunter), supra,* 4 Cal.5th 1245 was then pending before us, rejected defendant's claims (*Facebook, Inc. v. Superior Court (Touchstone)* (2017) 15 Cal.App.5th 729, 739–745) and denied him pretrial discovery (*id.*, at pp. 745–748 [exploring optional means by which defendant might obtain the sought information]). In our subsequent order granting review we directed the parties to address additional issues arising from the briefing and the Court of Appeal's opinion (*id.*, at pp. 746–748) — specifically, whether the trial court might compel Facebook's compliance with the underlying subpoena (or alternatively compel Renteria to consent to disclosure by Facebook), and whether the trial court might compel the prosecution to issue a search warrant on behalf of the underlying defendant.

In May 2018 we permitted the district attorney, the prosecuting authority in the underlying criminal action, to intervene in this proceeding. We later allowed the district attorney to file briefs, and also permitted all parties and amici curiae to file supplemental briefs addressing the effect, if any, of our decision in *Facebook* (*Hunter*), *supra*, 4 Cal.5th 1245. That briefing in turn spawned two additional potentially dispositive issues: whether Facebook users expansively consent to disclosure of all communications; and whether Facebook's business model removes it from coverage under the SCA.

II. FACTS ALLEGED IN THE PETITION FOR REVIEW — CONTRASTED WITH THE PRELIMINARY HEARING TESTIMONY AND RELATED EXHIBITS

Defense counsel's recitation of the facts in the petition for review, which is substantially identical to what defense counsel previously told the trial court and the Court of Appeal, advanced three key representations, as follows:

(1) "In August 2016, [defendant] drove to San Diego . . . to visit his sister Rebecca . . . . When he arrived, he discovered that Rebecca's boyfriend, Jeffrey Renteria, had moved into her home. Over the next several days, [defendant] observed odd behavior by Renteria . . . [and] grew concerned for their safety on August 8, 2016, *when he [and Rebecca] noticed that Rebecca's personal firearms were missing from the home*, [and] . . . Renteria himself . . . appeared to have moved out [of the house]. [(2)] When [defendant] and Rebecca attempted to contact Renteria over the phone about the missing firearms, Renteria made threatening statements that he was coming to harm [defendant] and Rebecca. [(3)] Hours later, while [defendant] and Rebecca were home alone, *Renteria burst through the front door and lunged at them*. [Defendant], armed with his personal handgun, immediately fired, hitting Renteria three times." (Pet. for rev., italics added.)[1]

---

[1] The petition continued: "None of the wounds were fatal. [¶] [Defendant] set aside his weapon, called 911, and was ultimately arrested for assault. He was compliant and cooperative with responding officers, giving a detailed explanation of the day's events and efforts to defend himself and his sister against Renteria. He was ultimately charged . . . with . . . attempted murder, with allegations of personal use of a

We obtained the underlying preliminary hearing transcript and exhibits from the superior court, and without objection we took judicial notice of those items. These materials paint a picture different from the facts set forth by defendant in his petition for review and related prior (and subsequent) briefs.

With regard to defendant's first representation — that defendant and his sister feared Renteria had taken his sister's guns from their home — testimony at the preliminary hearing suggests that on the morning of the shooting Renteria had placed Rebecca's firearms, and some of defendant's ammunition, into a secure container in Rebecca's attic. On cross-examination of Renteria at the preliminary hearing, and on redirect examination, Renteria repeatedly confirmed that he had hidden the weapons in the attic. A police officer who responded to the shooting further testified at the preliminary hearing that during a search immediately following the shooting, those same guns were found in Rebecca's room: a rifle was in a locked bag that was apparently in plain sight; a Glock handgun was in a dresser; and two loaded magazines for the handgun were outside the dresser. Defense counsel declined to cross-examine the officer.

This testimony appears to suggest that defendant and Rebecca had *themselves* found the firearms and magazines, placed them in her room, and hence would have had no reason to believe at the time of the shooting that any of those items were in Renteria's possession. Thus, defendant's characterization of the facts in his presentation to the lower

---

firearm and inflicting great bodily injury[,] . . . expos[ing] him to a maximum sentence of twenty-two years in State Prison."

courts and this court appears inconsistent with the evidence submitted at the preliminary hearing.

With regard to defendant's second factual recitation — that Renteria had threatened that he was coming to harm defendant and his sister — the preliminary hearing transcript reveals Renteria testified that, after receiving increasingly aggressive messages from Rebecca, he had responded to Rebecca and her brother, telling them that "if you try anything, you're going to jail for a long time." On cross-examination, Renteria confirmed that he had told Rebecca and defendant that if they were "setting [him] up for something," then they "would be arrested."

With regard to defendant's third factual recitation — that Renteria "burst through" Rebecca's front door and "lunged at" defendant and Rebecca — Renteria testified at the preliminary hearing that, soon after sundown, he told Rebecca by phone that he would return to the house to speak with her. Renteria testified that after unlocking and entering the home's front door, and immediately before he was shot, he was holding (only) a smartphone, which he used to take two photographs of defendant while defendant, sitting on a couch with Rebecca, raised his gun and prepared to shoot Renteria. Those two photos, and other related photos taken by police officers, all introduced as exhibits at the preliminary hearing, show a person identified as defendant, sitting back and cross-legged on a sofa, apparently in the early and then later process of raising his gun, while seated next to Rebecca. Defendant and Rebecca appear to be approximately six to eight feet from the front door where Renteria stood and took the pictures in the lighted room. This evidence is in tension with the narrative that defense counsel represented to all three levels of courts until very

recently — that Renteria "burst though" the door, and that he "lunged at" (and inferentially posed a deadly threat to) defendant or his sister. Again, on cross-examination, Renteria confirmed his testimony, emphasizing that he had his phone in his right hand when, intending to make a video, he instead "only hit the camera button," and took the two pictures. Defense counsel thereafter declined the court's invitation to offer "[a]ny affirmative evidence of the defense."

In sum, the testimony and exhibits introduced at the preliminary hearing call into question (1) defendant's asserted self-defense justification for obtaining access to Renteria's restricted posts and private messages and (2) defendant's contention that his need for access to such communications is particularly weighty and overcomes any competing privacy interests of victim and social media user Renteria. Although this is, to be sure, merely preliminary hearing evidence, it nevertheless constitutes relevant material that could properly be considered by a trial court that, having been presented with an assertedly viable claim of self-defense, is required to rule on a motion to quash a subpoena seeking restricted and private social media communications.

III. SUBSEQUENT PROCEDURE: THE PRESERVATION ORDER; THE SEALED DECLARATIONS AND EXHIBITS OPPOSING THE MOTION TO QUASH; UNSEALING OF THE DECLARATIONS AND EXHIBITS; AND REQUEST FOR SUPPLEMENTAL BRIEFING

Five months after the preliminary hearing described above, defendant sought, before a different judge, the underlying subpoena at issue in this litigation. He supported his demand for all of Renteria's Facebook communications

(including restricted posts and private messages), and a related request that Facebook preserve all such communications, by offering a *sealed* declaration describing and quoting certain public Facebook posts made by Renteria after the shooting that, defendant asserted, revealed Renteria's violent general musings.[2] The trial judge ordered Facebook to comply with the subpoena or appear in court to address any objection to it and to preserve the account and related stored communications.

Facebook preserved Renteria's account as directed, and then moved to quash the subpoena. Defendant's publicly-filed brief opposing the motion to quash recited the familiar trilogy noted earlier: (1) on the day of the shootings defendant "noticed that Rebecca's personal guns and ammunition were missing from the apartment"; (2) upon contacting Renteria about this, he "made threatening statements to harm [defendant] and Rebecca," causing them to be "concerned, alarmed, and afraid"; and (3) immediately before the shootings, "Renteria burst through the front door and charged at them."

---

[2] The sealed declaration added: "It is unknown whether additional relevant posts have been made to . . . Renteria's [Facebook] page that are not visible to the public, or whether additional relevant messages have been sent through the Facebook messaging system that have not been disclosed to defense counsel. . . . Through this subpoena, defense counsel seeks to preserve and obtain the stored contents of . . . Renteria's personal Facebook page; these records are relevant, material, exculpatory, and reflect upon the character and propensity for violence of the prosecution's key witness." This initial sealed declaration did not attach the described public posts or any document supporting the declaration's other statements.

Defendant argued in his brief opposing the motion to quash that he had established the requisite "plausible justification" (see, e.g., *City of Alhambra v. Superior Court* (1988) 205 Cal.App.3d 1118, 1134 (*Alhambra*)) for acquiring any restricted posts and private messages, and that the motion to quash should be denied. In support, defendant invited the trial judge to "review . . . the specific plausible justifications establishing [defendant's] right to compel the disclosure of documents" set out in a *second* and *also sealed* declaration in opposition to the motion to quash filed that date, April 21, 2017, simultaneously with the opposition brief.[3]

A *redacted* version of the key April 21 declaration, along with supporting *redacted* exhibits, was made available to the other interested parties (and was subsequently included in Facebook's Appendix supporting its writ petition), employing blackout to mask all descriptions of, and quotes from, the public posts and other documents referred to in counsel's declaration opposing the motion to quash. Defense counsel asserted: "Based on the foregoing recitation of facts and beliefs, the sought content from [the] account is relevant because (1) it may contain additional information that is inconsistent with the information previously provided by . . . Renteria to law enforcement and the prosecution as it related to this case, (2) it may contain

---

[3] Trial court documents reflect that, at defense counsel's request, the trial judge permitted that declaration to be filed under seal. In so requesting, counsel asserted that the declaration was "privileged" within the meaning of the federal Constitution, constituted protectable "work product, and [was] confidential [with respect] to a percipient witness (Jeffery Renteria)" — and that "[t]he redacted declarations [had been] narrowly tailored in order to protect . . . [these] rights, and permit interested parties" to respond substantively.

additional information that demonstrates a motivation or character for dishonesty in this matter, (3) it may contain additional information that demonstrates a character for violence that is relevant to the self-defense that will be asserted by defense counsel at trial, and [(4)] it may contain additional information that provides exonerating, exculpatory evidence for [defendant]." And this, counsel asserted, established a plausible justification for disclosure via the underlying subpoena.

The *unredacted* version of the April 21 sealed declaration and related exhibits was made available to the trial court. Those documents also were subsequently called up by the Court of Appeal, and thereafter we obtained them from the appellate court. After reviewing those documents and considering that material in conjunction with the earlier-described preliminary hearing transcript and exhibits, we advised the parties under California Rules of Court, rule 8.46(f)(3), that we contemplated unsealing the declaration and related exhibits. We gave the parties an opportunity to comment and, receiving no objection, we unsealed the documents.[4]

---

[4] Our order specified that "[a]s to the parties," we unsealed "the entirety of the April 21, 2017 declaration and all related exhibits, which in turn quote from and present copies of public social media posts and conditionally confidential probation reports. (Cal. Rules of Court, rule 8.46(f)(3).)" We also specified: "As to all others, the passages of the declaration and related exhibits that quote from and present copies of the public social media posts are unsealed; but the passages of the declaration and related exhibit that quote from and present copies of the probation reports are and remain sealed."

IV. RELEVANT LAW CONCERNING A MOTION TO QUASH A CRIMINAL SUBPOENA DUCES TECUM

At this point it is useful to describe the relevant statutes and case law relating to criminal subpoenas. Under Penal Code section 1326, subdivision (a), various officials or persons — including defense counsel, and any judge of the superior court — may issue a criminal subpoena duces tecum, and, unlike civil subpoenas, there is no statutory requirement of a " 'good cause' " affidavit before such a subpoena may be issued. (*Pitchess v. Superior Court* (1974) 11 Cal.3d 531, 535 (*Pitchess*); *City of Woodlake v. Tulare County Grand Jury* (2011) 197 Cal.App.4th 1293, 1301 [no requirement of a "good cause affidavit" "[i]n criminal matters"].) It is important to note, however, that such a criminal subpoena does not command, or even allow, the recipient to provide materials directly to the requesting party. Instead, under subdivision (c) of section 1326, the sought materials must be given *to the superior court* for its in camera review so that it may "determine whether or not the [requesting party] is entitled to receive the documents." (Pen. Code, § 1326, subd. (c); see also *People v. Blair* (1979) 25 Cal.3d 640, 651 [such materials cannot legally be given directly to the requesting party].)

Although no substantial showing is required to *issue* a criminal subpoena duces tecum, as explained below, in order to *defend* such a subpoena against a motion to quash, the subpoenaing party must at that point establish good cause to acquire the subpoenaed records. In other words, as we have observed, at the motion to quash stage the defendant must show "some cause for discovery other than 'a mere desire for the

benefit of all information.' " (*Pitchess, supra,* 11 Cal.3d at p. 537.)

How should a trial court assess good cause to enforce a subpoena duces tecum in the face of a motion to quash? A helpful decision by Justice Croskey, filed more than three decades ago, lists seven factors that "[t]he trial court . . . must consider and balance" when "deciding whether the defendant shall be permitted to obtain *discovery* of the requested material." (*Alhambra, supra,* 205 Cal.App.3d 1118, 1134, italics added.)[5] In turn, those seven factors are helpfully set forth, along with citations to some of the cases concerning discussion of the issue we face in this case — that is, *the enforcement of a criminal subpoena duces tecum issued to a third party* — in a leading criminal discovery treatise, Hoffstadt, California Criminal Discovery (5th ed. 2015) § 13.03, pages 390–391 (Hoffstadt on Criminal Discovery). Most recently, the appellate court in *Facebook v. Superior Court (Hunter)* (2020) 46 Cal.App.5th 109,

---

[5] In *Alhambra*, the defendant, who was charged with capital murder, sought (1) by *judicial subpoena*, police reports relating to other ostensibly similar homicides; and subsequently, (2) pretrial *discovery* from the prosecution, again concerning similar police reports relating to other ostensibly similar homicides. The Court of Appeal determined that the judicial subpoena had been improperly issued (by a pretrial judicial officer instead of the trial judge) and hence should have been quashed; accordingly, the appellate court vacated the order denying the motion to quash. (205 Cal.App.3d at pp. 1127–1129, 1136–1137.) Regarding the related discovery request, the court rejected the prosecution's objections to compliance and affirmed the propriety of that requested discovery. (*Id.*, at pp. 1129–1136, 1137.) In the course of resolving the defendant's *discovery* request, the Court of Appeal proceeded to review and apply seven "well established . . . principles" (*id.*, at p. 1132), which it eventually summarized on page 1134.

119–121 (review granted June 10, 2020, S260846; *Facebook (Hunter) II*) applied these factors in the context of evaluating the same criminal defense subpoena that we addressed in *Facebook (Hunter), supra*, 4 Cal.4th 1245.

A. The *Alhambra* factors

We list the seven factors that should be considered by a trial court in considering whether good cause has been shown to enforce a subpoena that has been challenged by a motion to quash. In the process, we include additional relevant case citations to those set forth in *Alhambra* and Hoffstadt on Criminal Discovery:

(1) Has the defendant carried his burden of showing a " 'plausible justification' " for acquiring documents from a third party (*Kling v. Superior Court of Ventura County* (2010) 50 Cal.4th 1068, 1075 (*Kling*); *Hill v. Superior Court* (1974) 10 Cal.3d 812, 817–818 (*Hill*) [discovery context]; *Joe Z. v. Superior Court* (1970) 3 Cal.3d 797, 804 (*Joe Z.*) [discovery context]; *Ballard v. Superior Court* (1966) 64 Cal.2d 159, 167 (*Ballard*) [discovery context]; see also, e.g., *Facebook (Hunter) II, supra,* 46 Cal.App.5th at p. 119, rev. granted; *Alhambra, supra,* 205 Cal.App.3d at pp. 1124, 1128, 1131–1136 [discovery context]; *Lemelle v. Superior Court* (1978) 77 Cal.App.3d 148, 162–164 (*Lemelle*) [discovery context]; *Pacific Lighting Leasing Co. v. Superior Court* (1976) 60 Cal.App.3d 552, 566–567 (*Pacific Lighting)*; *In re Valerie E.* (1975) 50 Cal.App.3d 213, 218 [discovery context]) by presenting specific facts demonstrating that the subpoenaed documents are admissible or might lead to admissible evidence that will reasonably " 'assist [the defendant] in preparing his defense' "? (*People v. Superior Court (Barrett)* (2000) 80 Cal.App.4th 1305,

1318 (*Barrett*); *Alhambra, supra*, 205 Cal.App.3d 1118, 1133–1134 [discovery context].) Or does the subpoena amount to an impermissible " 'fishing expedition' "? (*Pitchess, supra,* 11 Cal.3d at p. 538; *Barrett, supra,* 80 Cal.App.4th at p. 1320, fn. 7.)[6]

(2) Is the sought material adequately described and not overly broad? (*People v. Serrata* (1976) 62 Cal.App.3d 9, 15 (*Serrata*); *Alhambra, supra,* 205 Cal.App.3d at p. 1134 &

---

[6] The decision in *Alhambra, supra,* 205 Cal.App.3d at page 1134, lists plausible justification as the last of its seven factors — but we agree with Justice Hoffstadt's treatise that this consideration should be given prominence and listed first.

We also note that although most decisions phrase this factor as "plausible justification," in *Kling, supra,* 50 Cal.4th at page 1075, we referred to " 'a plausible justification or a good cause showing of need,' " quoting the lead opinion in *Alford v. Superior Court* (2003) 29 Cal.4th 1033, 1045 (*Alford*), which used that phrasing. *Alford* in turn cited to *Barrett, supra,* 80 Cal.App.4th at pages 1320–1321, which, in footnote 7, employed the disjunctive phrasing. Earlier, the appellate court's decision in *Hinojosa v. Superior Court* (1976) 55 Cal.App.3d 692, 695, also employed the disjunctive phrasing, while citing to our own decision in *Hill*, *supra*, 10 Cal.3d at page 817, which, like our earlier decisions in *Ballard, supra,* 64 Cal.2d at page 167, and *Joe Z., supra,* 3 Cal.3d at page 804, spoke only of "plausible justification."

On reflection, we believe that Justice Hoffstadt's phrasing, reflecting that of most other cases (see, e.g., those cited in the text immediately above), is correct. The plausible justification consideration is but one (albeit the most significant) of multiple factors that, together, reflect a global inquiry into whether there is good cause for a criminal subpoena. It is included within the overall good-cause inquiry and is not an alternative to that inquiry. Accordingly, we decline to employ the disjunctive phrasing used in *Kling, Alford*, *Barrett*, and *Hinojosa*.

fn. 16 [discovery context]; see also *Lemelle, supra,* 77 Cal.App.3d 148, 165, and cases cited [discovery context].)

(3) Is the material "reasonably available to the . . . entity from which it is sought (and *not* readily available to the defendant from other sources)"? (*Alhambra, supra,* 205 Cal.App.3d at p. 1134, italics added [discovery context]; see also *Facebook (Hunter), supra*, 4 Cal.5th at p. 1290 [noting prospect that "the proponents can obtain the same information by other means"] and *id.*, at p. 1291 [suggesting that the trial court on remand consider alternative mechanisms]; *Hill, supra,* 10 Cal.3d 812, 817 [posing whether the defendant "cannot readily obtain the [discovery] information through his own efforts"]; *Facebook (Hunter) II, supra,* 46 Cal.App.5th at pp. 120–121, rev. granted [considering various alternative sources for the subpoenaed information]; *People v. Von Villas* (1992) 10 Cal.App.4th 201, 228–236 (*Von Villas*) [concluding, in light of factors set out in *Delaney v. Superior Court* (1990) 50 Cal.3d 785, that the trial court properly granted a freelance newsperson's motion to quash a subpoena duces tecum on the ground that there existed an alternative source for the requested information[7]].)

---

[7] In *Delaney, supra,* 50 Cal.3d 785, we held that when a criminal defendant who seeks "unpublished information" protected by the newsperson's shield law (Cal. Const., art. I, § 2, subd. (b); Evid. Code, § 1070) subpoenas a reporter and establishes "a reasonable possibility the [sought] information will materially assist his defense" (50 Cal.3d at p. 809, italics omitted), the court must consider and balance various factors, including whether there is an "alternative source" for the information sought. Moreover, in considering whether to impose a "universal and inflexible" alternative source

(4) Would production of the requested materials violate a third party's "confidentiality or privacy rights" or intrude upon "any protected governmental interest"? (*Alhambra, supra,* 205 Cal.App.3d at p. 1134 [discovery context]; *Facebook (Hunter) II, supra,* 46 Cal.App.5th at p. 121, rev. granted [noting a social media user's " 'privacy interests' " in subpoenaed material]; *Barrett, supra*, 80 Cal.App.4th at p. 1316 [noting governmental interest in preventing disclosure of " 'official information' " as to which there is a necessity of preserving confidentiality]; *Millaud v. Superior Court* (1986) 182 Cal.App.3d 471, 475 [subpoena must not constitute "an unreasonable search and seizure as to the third party"]; *Pacific Lighting, supra,* 60 Cal.App.3d 552, 567 ["protection of the witness's constitutional rights requires that the ' "plausible justification" for inspection' [citation] be so substantiated as to make the seizure constitutionally reasonable"]; see also *Kling, supra,* 50 Cal.4th at p. 1078 [noting that the People have an interest in ensuring that evidentiary privileges are not sacrificed merely because a subpoena recipient lacks interest to object] & p. 1080 [noting crime victims' rights under Marsy's Law, Cal. Const., art. I, § 28, subd. (b)(4), to prevent disclosure of confidential information to a defendant]; *Alford, supra,* 29 Cal.4th 1033, 1038–1039 [describing law enforcement officers' privileges and procedures relating to third-party discovery concerning officer records]; *Hammon*, *supra*, 15 Cal.4th 1117, 1127 [noting a patient's statutory privilege and constitutional right of privacy]; *Delaney, supra,* 50 Cal.3d 785,

---

requirement in that setting, the trial court must consider "the type of information being sought . . . , the quality of the alternative source, and the practicality of obtaining the information from the alternative source." (*Id.*, at pp. 812–813.)

798–816 [construing scope of the state constitutional and statutory newsperson's shield law in the context of a criminal defense subpoena].)

(5) Is defendant's request timely? (*Hill, supra,* 10 Cal.3d 812, 821 [discovery context]; *People v. Cooper* (1960) 53 Cal.2d 755, 771 [discovery context]; *Alhambra, supra,* 205 Cal.App.3d 1118, 1134 [discovery context].) Or, alternatively, is the request premature? (See *People v. Lopez* (1963) 60 Cal.2d 223, 247 ["[u]nder certain circumstances, delayed disclosure [via discovery] may well be appropriate"].)

(6) Would the "time required to produce the requested information . . . necessitate an unreasonable delay of defendant's trial"? (*Alhambra, supra,* 205 Cal.App.3d at p. 1134 & fn. 17 [discovery context]; see also *Kling, supra,* 50 Cal.4th at p. 1087 [noting the People's right to a speedy trial].)

(7) Would "production of the records containing the requested information . . . place an unreasonable burden on the [third party]"? (*Alhambra, supra,* 205 Cal.App.3d at p. 1134 [discovery context]; see also *Facebook (Hunter), supra*, 4 Cal.5th at pp. 1289–1290 [regarding asserted burdens on a social media provider]; *Serrata, supra,* 62 Cal.App.3d 9, 15; cf. *People v. Kaurish* (1990) 52 Cal.3d 648, 686 [criminal discovery may be denied if "the burdens placed on government and on third parties *substantially* outweigh the demonstrated need"].)

For convenience, we will refer to these seven considerations as the "*Alhambra* factors."

B. Applying the *Alhambra* Factors — With Emphasis on the Plausible Justification and Confidentiality/Constitutional Rights Considerations

We will review selected prior decisions cited above in order to illustrate key underlying principles, with emphasis on the plausible justification and confidentiality/constitutional rights considerations, which are especially pertinent to the present litigation.

1. The plausible justification factor

a. Ballard

We first articulated the plausible justification consideration in *Ballard, supra,* 64 Cal.2d 159. There the defendant, a doctor, stood charged with drugging and raping his patient. The prosecution, with the cooperation of the victim, made recordings of telephone conversations in which the defendant incriminated himself. The defendant was granted discovery, and the prosecution also agreed to provide defense counsel with the names and addresses and the statements of witnesses that would be called at trial. But, in addition, the defendant sought to discover the names and addresses of *all* persons interviewed by the police regarding the charge. (*Id.*, at p. 166.)

We found the trial court properly denied the blanket request for information beyond that already provided to the defendant. We explained that " '[a]lthough the defendant does not have to show, and indeed may be unable to show, that the evidence which he seeks to have produced would be admissible at the trial [citations], *he does have to show some better cause for inspection than a mere desire for the benefit of all information*

which has been obtained by the People in their investigation of the crime.' " (*Ballard, supra,* 64 Cal.2d at p. 167, italics added.)

We elaborated: "A defendant's motion for discovery must . . . describe the requested information with at least some degree of specificity and must be sustained by *plausible justification*." (*Ballard, supra,* 64 Cal.2d at p. 167, italics added.) We immediately followed on that same page by quoting a passage from a then-recent law review article by Chief Justice Traynor, which, although not employing the italicized phrase, states: " 'A showing [. . .] that the defendant cannot readily obtain the information through his own efforts will ordinarily entitle him to pretrial knowledge of any unprivileged evidence, or information that might lead to the discovery of evidence, *if it appears reasonable that such knowledge will assist him in preparing his defense*. . . .' (Traynor, *Ground Lost and Found in Criminal Discovery* (1964) 39 N.Y.U. L.Rev. 228, 244; italics added.)" (*Ballard* at p. 167.)

We then proceeded to apply and give meaning to the "plausible justification" standard, while determining that "[i]n the instant case petitioner has not met these requirements." (*Ballard, supra,* 64 Cal.2d at p. 167.) We first observed that the defendant had failed to carry his burden of explaining to the trial court his reasons for procuring the names and addresses of those persons whom the prosecution does not intend to call as witnesses. (*Id*., at pp. 167–168.) In reaching this conclusion, we addressed the defendant's "recently advanced ground for such discovery." (*Id.*, at p. 168.) We noted that the defendant claimed "he needs the names of these persons in order to determine 'whether or not the accusatory stage had been reached' " when " 'the complained-of tape recordings were made.' " (*Ibid.*) "According to [the defendant], if that stage had been reached,

the failure of the police to advise him of his rights to counsel and to remain silent renders any evidence of his recorded statements inadmissible" under case law construing those constitutional rights. (*Ibid.)* But we rejected "such justification for discovery" because, we explained, the defendant "was not in custody at the time he gave such statements" and hence "the accusatory stage could not have been reached." (*Ibid*.) After undertaking an extended analysis of the defendant's right-to-counsel and right-to-remain silent claims underlying his asserted "plausible justification" for acquiring the sought information (*id*., at pp. 167–170), we concluded that because the defendant "was clearly not in custody at the time he uttered the incriminating statements to the victim, he cannot successfully challenge the admissibility of those statements on the basis of [the cited case law authority]." (*Id*., at p. 170.) Consequently, we held, the defendant's invocation of possible issues concerning his rights to counsel and to remain silent did not plausibly "justify discovery in the instant case." (*Ibid*.)

As this recitation shows, in our first decision articulating the plausible justification standard we measured the defendant's stated justification for acquiring the sought information against the legal claims (in that case, asserted violations of the rights to counsel and to remain silent) pursuant to which the defendant urged the information would be relevant. In resolving that plausible justification inquiry we considered the facts as then known, determined the underlying legal claims to be inapplicable on those facts, and hence found no plausible justification for acquiring the sought information to support such a legal claim. An analogous inquiry in the present case concerning defendant's stated *primary* ground for acquiring and inspecting the sought information — that is, to support an

assertion of self-defense — calls for an examination of the facts as alleged in the briefs and also as reflected in the preliminary hearing transcript described earlier, in order to assess whether a claim of self-defense is sufficiently viable to warrant the intrusion that would occur if the sought communications were required to be disclosed.

b. Hill

As noted earlier, defendant in the present case asserts two bases for acquiring the sought information. In addition to his primary justification (to help establish a claim of self-defense against Renteria), he also advances a *secondary* (or, if the primary basis fails, an *alternative*) justification — to impeach the prosecution's anticipated witness, Renteria, by highlighting his character for untruthfulness and violence. In this regard, *Hill, supra,* 10 Cal.3d 812, which we decided eight years after *Ballard*, is enlightening. As explained below, in *Hill* we found that the defendant had indeed shown plausible justification to acquire such impeachment evidence — but that he had not established justification under other theories.

The defendant in *Hill*, charged with attempted burglary, sought to discover (1) any public records of *felony convictions* that might exist regarding the prosecution's prospective key witness against him — in order to impeach that witness; and (2) any general *arrest and detention records* that might exist regarding the prosecution's prospective key witness against him — in order to argue that the prosecution witness, who had reported the alleged crime to the police, in fact committed that

underlying crime.[8] The trial court denied both aspects of discovery on the ground that the defendant had not shown that any such records existed concerning the witness. (*Id.*, at p. 816.)

We first addressed the request for records of felony convictions, in order to impeach. We observed that " '[i]n criminal cases, the trial court retains wide discretion to protect against the disclosure of information which might unduly hamper the prosecution or violate some other legitimate governmental interest.' " (*Hill, supra,* 10 Cal.3d at p. 817.) Then we highlighted the plausible justification factor, as first articulated in *Ballard,* and we quoted again from the same passage in Chief Justice Traynor's article in the course of explaining that trial courts have "discretion to deny discovery *in the absence of a showing which* specifies the material sought and *furnishes a 'plausible justification'* for inspection." (*Ibid.*, italics added.)

We found that the defendant had adequately described the sought felony conviction records, and we acknowledged that the evidence code allows for such felony records to impeach a witness's credibility. (*Hill, supra,* 10 Cal.3d at p. 817.) We determined that the defendant could not " ' "readily obtain the information through his own efforts" ' " (*ibid.*; see also *id.*, at pp. 817–819), and then we turned to the justification for

---

[8] The motion for discovery asserted that such records, if they exist, "may show that [the witness] has a bias or motive to lie in the current action." Moreover, the defendant asserted, "[The witness] may have prior arrests . . . for burglary. These incidents may be similar to the current offense" and could demonstrate that the witness "may be the actual perpetrator of the offense for which [the defendant] is now charged, thus giving him a motive to lie." (*Hill, supra,* 10 Cal.3d at p. 815.)

acquiring and inspecting any such felony conviction records. We noted that the subject of the records request "was an eyewitness to the felony charged," he was evidently "the only eyewitness other than the persons he claimed perpetrated it," and "the corroboration of his report was not strong." (*Id.*, at p. 819, italics omitted.) Echoing Chief Justice Traynor's phrasing first quoted in *Ballard*, we observed: " ' "[I]t appears reasonable that such information will assist [the defendant] in preparing his defense." ' " (*Id.*, at p. 817.) We concluded, "[m]anifestly it would be of help in preparing the defense to obtain information regarding any prior felony convictions of [the key prosecution witness], whose credibility was likely to be critical to the outcome of the trial." (*Id.*, at p. 819.) Considering and balancing these factors, we determined that the defendant had established good cause for the proposed acquisition and inspection concerning impeachment of the prospective prosecution witness. (*Id.*, at p. 819.)[9]

We then turned to the defendant's additional request for access to and inspection of any "arrest and detention" records, which as noted earlier the defendant sought in order to probe whether the prospective witness, and not the defendant, committed the charged attempted burglary. (*Hill, supra,* 10 Cal.3d at p. 822.) We acknowledged that the prospective

---

[9] We were careful to stress, however, that our conclusion was based on a consideration of *all* of the relevant factors — and we pointedly cautioned that a finding of good cause should not flow automatically "in every case in which a defendant charged with a felony seeks discovery of any felony convictions in any 'rap sheet' of prosecution witnesses." (*Hill, supra,* 10 Cal.3d at p. 819.) Instead, we clarified, discretion remains with the trial judge to determine, based on all the relevant factors, whether to grant such discovery. (*Id.*, at p. 820.)

witness's " 'rap sheet,' if it exists, might contain information regarding arrests or detentions for prior burglaries or attempted burglaries, and such information conceivably might lead to the discovery of evidence of prior offenses by [the prospective witness] having a distinctive modus operandi common to both the prior offenses and the offense with which [the defendant] is charged." (*Ibid.*) But, we held, "[e]ven if it be assumed that such evidence would be admissible as tending to show that [the prospective witness] committed the instant offense, a matter that might affect his credibility by showing he had a motive to lie, it does not follow that [the trial court] erred in denying discovery of the arrest and detention records, if any." (*Ibid.*) We explained: "*In view of the minimal showing of the worth of the information sought* and the fact that requiring discovery on the basis of such a showing could deter eyewitnesses from reporting crimes, we are satisfied that [the trial court] did not abuse its discretion in denying discovery of those records, if they exist." (*Ibid.,* italics added.)[10]

---

[10] We elaborated: "Before ruling, [the trial court] inquired whether there were any facts in [defense counsel's] declaration indicating that [the prospective witness] 'may have been involved' other than his claiming to have been an eyewitness, and [defense counsel] replied, 'No . . . .' [Defense counsel] also advised the court that [the prospective witness] was the one who 'initially called the police' apparently regarding the crime charged against [the defendant]. Even if [the prospective witness] committed prior offenses having a distinctive modus operandi common to both the prior offenses and the offense charged, that fact, together with his calling the police and claiming to have been an eyewitness to the offense charged would not, without more, warrant a reasonable belief that [the prospective witness] committed that offense and therefore had an interest in the case which might affect his credibility. Those

As this recitation from *Hill* again shows, each legal claim that a defendant advances to justify acquiring and inspecting sought information must be scrutinized and assessed regarding its validity and strength. In *Hill*, the defendant's request to acquire and inspect any existing public records of felony convictions in order to facilitate proposed impeachment of the prospective witness was, under the circumstances, supported by plausible justification because: it was adequately described; the prospective (and sole) witness's credibility was likely to be critical to the outcome, that person was particularly subject to impeachment, and the information sought was relevant to that impeachment; and it reasonably appeared that such information would assist in preparation of the defense. But the defendant did not meet the same plausible justification test concerning his effort to acquire and inspect any existing, and even more sensitive, records concerning mere arrests or detentions, which he sought in order to attempt to shift blame from himself to the prospective prosecution witness. As noted, we found only a "minimal showing of the worth of" that information, and expressed concern that requiring discovery of such sensitive information (contrasted with disclosure of public records of

---

facts at best would raise only a suspicion that [the prospective witness] might have committed the instant offense. And in the words of [the trial] court, 'it seems . . . that what [[defense counsel] is] suggesting [i.e., allowing discovery of [the witness's] arrest and detention records, if any] would have an awesome effect on people reporting crime.' " (*Hill, supra,* 10 Cal.3d at pp. 822–823.) At the same time, and of potential significance to the present case, we suggested that such discovery might be proper if it related to a valid claim of self-defense, and if a jury could reasonably determine from the sought information, along with any other proffered evidence, that the defendant had been acting in self-defense. (*Id.*, at p. 823.)

actual felony convictions) based on such an insubstantial showing could have the undesirable effect of "deter[ring] eyewitnesses from reporting crimes." (*Hill, supra,* 10 Cal.3d at p. 822.)

Consistent with the approach undertaken in *Ballard* and *Hill*, in assessing the present defendant's *primary* basis for plausible justification to acquire and inspect the sought restricted posts and private messages (to support a claim of self-defense), an appropriate inquiry would focus on the facts as alleged in the briefs and also as reflected in the preliminary hearing transcript in order to assess whether a claim of self-defense is sufficiently viable to warrant that significant intrusion.

Likewise, in assessing the present defendant's *secondary* (and, if the self-defense-claim justification fails, *alternative*) basis for plausible justification in the present case — to impeach prospective witness Renteria — an appropriate inquiry would consider whether such a significant intrusion is warranted and necessary to facilitate the contemplated impeachment. The analysis should be informed by the circumstance that defendant has already acquired, not only Renteria's public posts (which, defendant asserts, contain substantial relevant information) but also, and perhaps most importantly, Renteria's probation reports (see *ante*, fn. 5), which in turn detail his prior convictions and contain other substantial related impeachment information. Moreover, as explained below, when as here a subpoena seeks restricted social media posts and private messages, in the absence of an apparent relationship between the underlying crime and such communications, a trial court should examine even more closely the proffered showing of plausible justification in support of such a privacy intrusion.

2. A third party's confidentiality or constitutional rights and "protected governmental interests"

As the Court of Appeal stressed in *Pacific Lighting, supra,* 60 Cal.App.3d 552, when considering the enforceability of a criminal defense subpoena duces tecum, "[t]he protection of [the subject of a subpoena's] right to be free from unreasonable search and seizure constitutes a 'legitimate governmental interest.' Thus, though 'ordinarily' a criminal defendant may be entitled to pretrial knowledge where 'it appears reasonable that such knowledge will assist him in preparing his defense,' [citation] the protection of the witness's constitutional rights requires that the ' "plausible justification" for inspection' [citation] be so substantiated as to make the seizure constitutionally reasonable." (*Id.*, at pp. 566–567.) When, as in the present case, a litigant seeks to effectuate a significant intrusion into privacy by compelling production of a social media user's restricted posts and private messages, the fourth *Alhambra* factor — concerning a third party's confidentiality or constitutional rights and protected governmental interests — becomes especially significant.

It is important, as an initial matter, to bear in mind the substantial differences underlying the justifications offered in the two cases that we have encountered to date — *Facebook (Hunter), supra*, 4 Cal.5th 1245 (see also *Facebook (Hunter) II, supra*, 46 Cal.App.5th 109, rev. granted)), and the present matter.

In the earlier case, *Facebook (Hunter)*, there was significant evidence that the underlying shooting and resulting homicide may have related to, and stemmed from, social media posts — and hence the nexus, and justification for intruding into a victim's or witness's social media posts (public and restricted,

and/or private messages), was substantial.[11] Indeed, the Court of Appeal, in its recent treatment of the plausible justification factor issue in that prior case, had no difficulty finding such justification for the proposed intrusion. (*Facebook (Hunter) II, supra*, 46 Cal.App.5th at p. 119, rev. granted].)[12]

---

[11] In *Facebook (Hunter)* the defendants sought social media communications related to two persons: The homicide victim, Rice; and the prosecution's key witness, Lee. Concerning the deceased Rice, the information was sought, not for character impeachment, but to (1) *directly challenge the prosecution expert's anticipated testimony that the underlying shooting was gang-related*; and also to (2) " 'locate exculpatory evidence' " (and attempt to establish a form of self-defense, or imperfect self-defense), in light of Rice's public posts showing that he was a violent person who *had previously threatened the defendants and others on social media*. (*Facebook (Hunter), supra,* 4 Cal.5th at p. 1256; see also *id.*, at p. 1257.) Concerning witness Lee, defendants sought to obtain yet more of her violence-inflected social media posts so as to *impeach* her by emphasizing her threats made to others, and to argue that her testimony against defendants, one of whom was her former boyfriend, was motivated by jealous rage. (*Id.*, at p. 1257.) In addition, Lee had been implicated by some witnesses as the driver of the car used by defendants when the shooting occurred. (*Id.*, at p. 1253, fn. 4.) These facts gave the defense a more specific basis for seeking the communications of Rice and Lee, beyond identifying general character impeachment evidence. Under the *Alhambra* framework, a trial court may take into account these kinds of case-specific considerations in evaluating whether a defendant has established a colorable and substantial basis for seeking social media communications by subpoena.

[12] Ultimately the Court of Appeal determined that the trial court abused its discretion in denying Facebook's motion to quash by failing to properly consider and balance *all* of the relevant good cause factors — "particularly options for obtaining materials from other sources." (*Facebook (Hunter) II,* 46 Cal.App.5th at p. 119, rev. granted; see also, *id.*, at pp. 120–

In the present case, by contrast, it is questionable whether there is any similar substantial connection between the victim's social media posts and the alleged attempted murder. Moreover, although it is always possible that material in a prior or subsequent social media post may be relevant to something that the defendant would like to rely upon, the requirement that a social media user or a social media provider disclose social media posts, even to a judge for ex parte review (see Pen. Code, § 1326, subd. (c)), as a predicate to possible broader disclosure, itself constitutes a significant impingement on the social media user's privacy with respect to restricted posts and private messages. Accordingly, plausible justification — which, as noted above, must in *all* cases be "so substantiated as to make the seizure constitutionally reasonable" (*Pacific Lighting, supra,* 60 Cal.App.3d at p. 567) — must be subject to even closer examination in the absence of an apparent relationship between the alleged crime and the sought private communications. (Cf. *Hammon, supra,* 15 Cal.4th at p. 1127 [courts should be especially reluctant to facilitate pretrial disclosure of privileged or confidential information that, as it may turn out, is unnecessary to use or introduce at trial].) An appropriate

---

121.) Moreover, and significantly, the appellate court correctly observed that the trial court also failed to "evaluate [the] continuing need for private content *after* the public content [had been] produced" by Facebook, as we had directed. (*Id.*, at p. 121.) In the latter regard, the court stated: "[W]e do not know whether providers had already produced the key communication . . . , or comparable communications, as part of their *public* production. We question how the trial court could properly balance all the good cause factors, including [the prospective prosecution witness's] privacy interests and the other policies served by the Act, without any review of what had already been produced." (*Ibid.*)

assessment of a social media user's rights implicated by such a subpoena would take into account the likelihood of that the asserted connection between an underlying crime and any sought private communications actually exists.

Finally, we note that in the present circumstances, the California Constitution, as amended to incorporate Marsy's Law, calls for yet additional special inquiry. (Cal. Const., art. I, § 28, subds. (b)(4), (b)(5), (c).) As alluded to earlier, the subpoena seeking Renteria's private communications implicates these constitutional provisions, which recognize a victim's right to prevent disclosure of matters "otherwise privileged or confidential by law" (*id.*, at subd. (b)(4)) and to refuse a discovery request by a defendant (*id.*, at subd. (b)(5)). Moreover, subdivision (c)(1) of section 28 allows the prosecution to enforce a victim's rights under subdivision (b). We have observed that these provisions contemplate "that the victim and the prosecuting attorney would be aware that the defense had subpoenaed confidential records regarding the victim from third parties." (*Kling, supra*, 50 Cal.4th 1068, 1080.) Accordingly, in circumstances like those here it would be appropriate to inquire whether such notice has been, or should be, provided.[13]

---

[13] As recited *ante*, part III, the trial court ordered Facebook to preserve the sought files and information, and Facebook reported that it had done so. In these circumstances an appropriate assessment of a victim's rights under the constitutional provision would consider whether, after such preservation has occurred (hence presumably addressing concerns about possible spoliation by a social media user), notice to a victim/social media user should be provided in order to facilitate the victim's confidentiality and related rights.

V. THE UNDERLYING HEARING ON THE MOTION TO QUASH, AND THE COURT'S RULING UPHOLDING THE SUBPOENA TO FACEBOOK

The superior court judge who conducted the hearing on the motion to quash (and who had not been involved in any of the earlier proceedings in this matter) denied the motion, finding good cause for the subpoena. Neither the reporter's transcript of the hearing, nor the resulting minute order, reflects that the court expressly considered and balanced the most relevant *Alhambra* factors.

Specifically, there was no express mention of, let alone explicit assessment concerning, the primary good cause factor — whether defendant had shown plausible justification for acquiring crime victim Renteria's restricted posts and private messages. Neither did the court explicitly address the potential overbreadth of the subpoena. Nor did the court adequately consider defendant's ability to obtain the material from other sources, such as the messages' recipients, or friends who could view Renteria's restricted posts and private messages. The court did consider, and evidently credited, defense counsel's assertion that Renteria would not be a reliable source for handing over the communications. Yet nothing in the record suggests that the court assessed, or balanced, any confidentiality or constitutional interests or privileges that Renteria might have, including possible rights under Marsy's law, in securing notice and avoiding cooperation with defense counsel and disclosure of his restricted posts and private messages.

The absence of such a record of consideration in the present case is somewhat understandable. At the time of the

hearing, *Alhambra*'s useful seven-factor balancing summary, although having been set forth nearly 30 years prior, had gone uncited except for in the 2015 edition of Justice Hoffstadt's California Criminal Discovery treatise in a passage addressing a trial court's in camera review of produced documents. (See Hoffstadt on Criminal Discovery, *supra,* at pp. 390–391.)

Nevertheless, as shown above, a number of long-established decisions have discussed, quite extensively, several of these factors, including the two that deserve special attention in the present circumstances — plausible justification, and confidentiality or constitutional interests that a person in Renteria's position might have. In other words, as these and related cases demonstrate, the *Alhambra* framework is built upon a firm foundation, and the *Alhambra* decision itself is innovative only in the sense that it collected these principles in a handy list.

As recently acknowledged by the Court of Appeal in *Facebook (Hunter) II, supra,* 46 Cal.App.5th 109, 119–121 (rev. granted), the seven *Alhambra* factors are relevant, and properly should be considered by a trial judge, when ruling on a motion to quash a subpoena directed at a third party. It is especially at *that point in the subpoena process* that the judicial officer should assess and balance, not only the important plausible justification factor, but also all of the other factors — including the adequacy of the description/overbreadth, availability of the sought material from other sources, privacy/confidentiality and constitutional concerns, timeliness, potential for delay of trial, and asserted undue burden on a producing third party. The trial court did not do so here.

VI. PROBLEMS RAISED BY PROCEEDING EX PARTE AND UNDER SEAL — AND RELATED "BEST PRACTICES" CONSIDERATIONS

In addition to failing to clearly apply the *Alhambra* factors, the trial court also chose to proceed ex parte and under seal. We have acknowledged in cases such as *Kling, supra,* 50 Cal.4th 1068, that in criminal proceedings, by virtue of Penal Code section 1326, "[t]he Legislature granted the defense special protections" — permitting criminal defendants to make the necessary showing of need for any sought materials outside the presence of the prosecution, if necessary to protect defense strategy and/or work product. (*Kling, supra*, 50 Cal.4th at p. 1075.)[14] At the same time, we have cautioned trial courts against allowing sealing in this setting unless there is " 'a risk of revealing privileged information' and a showing 'that filing under seal is the only feasible way to protect that required information.' " (*Ibid*.) Moreover, we explained, proceeding ex

---

[14] See also *Kling, supra*, 50 Cal.4th, at page 1075 [the defense " 'is not required, on pain of revealing its possible defense strategies and work product, to provide the prosecution with notice of its theories of relevancy of the materials sought' "].) Instead, a defendant may make " 'an offer of proof at an in camera [and ex parte] hearing.' " (*Ibid.*; see also *id*., at pp. 1076–1077.) Nonetheless, as noted earlier, a failure to establish good cause — amounting to a mere fishing expedition — will lead to the granting of a motion to quash. (*Id.*, at p. 1075; see also *Barrett, supra,* 80 Cal.App.4th 1305, 1320, fn. 7.)

In this case, defendant has freely disclosed his self-defense and impeachment strategy, both in the trial court and the Court of Appeal, and also in this court. As he concedes, it "is no secret" that his strategy has been and will be (1) *primarily* to claim self-defense; and (2) *secondarily* and alternatively, to impeach the victim's character and portray him as violent.

parte is "generally disfavored" (*id.,* at p. 1079) because doing so may lead judges, uninformed by adversarial input, to incorrectly deny a motion to quash and grant access to pretrial discovery. (*Ibid.*) We elaborated on the "inherent deficiencies" of ex parte proceedings: " ' "[T]he moving party's . . . presentation is often abbreviated because no challenge from the [opposing party] is anticipated at this point in the proceeding. The deficiency is frequently crucial, as reasonably adequate factual and legal contentions from diverse perspectives can be essential to the court's initial decision. . . .' " [Citations.] Moreover, 'with only the moving party present to assist in drafting the court's order there is a danger the order may sweep "more broadly than necessary." ' " (*Ibid.*) Accordingly, we explained, a trial court should "balance the People's right to due process and a meaningful opportunity to effectively challenge the discovery request against the defendant's constitutional rights and the need to protect defense counsel's work product." (*Id.* at p. 1079.) A trial court has discretion to balance these "competing interests" in determining how open proceedings concerning the subpoena should be. (*Id.* at p. 1080.)

The balancing called for in circumstances such as these can be complex and nuanced. For example, as noted, defendant stresses *his* right to acquire and present all relevant evidence in his defense, and insists he has established good cause to invade Renteria's privacy interests by acquiring his restricted posts and private communications via his underlying subpoena. Yet the district attorney asserts that *victim* Renteria's constitutional rights, including under Marsy's Law, were violated when the trial court ordered Facebook to preserve the information, and then issued the subpoena, without giving the victim or the

People adequate notice and an opportunity to be heard concerning issuance of the subpoena.

In the trial court in present case, defense counsel was allowed to proceed ex parte and to file under seal the key declaration and exhibits opposing the motion to quash. Accordingly neither the district attorney nor Facebook was permitted to learn what public posts defendant relied upon — and neither was in a position at the hearing concerning the motion to quash to address whether those posts support a finding of good cause for the underlying subpoena. When a trial court does conclude, after carefully balancing the respective considerations, that it is necessary and appropriate to proceed ex parte and/or under seal, and hence to forego the benefit of normal adversarial testing, the court assumes a heightened obligation to undertake critical and objective inquiry, keeping in mind the interests of others not privy to the sealed materials.

Finally, we caution that even when other entities are not excluded from full participation in the proceedings, a trial court ruling on a motion to quash — especially one that, like this, involves a request to access restricted social media posts and private messages held by a third party — should bear in mind the need to make a record that will facilitate appellate review. We acknowledge that the trial court below was not required to issue a written statement of decision concerning its ruling on the motion. (See *In re Marriage of Askmo* (2000) 85 Cal.App.4th 1032, 1040 [Code of Civil Proc. § 632, which requires a trial court to issue a statement of decision that explains the factual and legal basis for its determinations, generally applies only "when there has been a trial followed by a judgment," and "does not apply to an order [resolving a] motion"].) Yet because we today articulate seven factors that courts must balance when ruling

on a motion to quash, we emphasize that courts should create a record that facilitates meaningful appellate review. Accordingly, a trial court should, at a minimum, articulate orally, and have memorialized in the reporter's transcript, its consideration of the relevant factors.

VII. WE WILL REMAND TO THE TRIAL COURT TO CONSIDER THE GOOD CAUSE FACTORS WITH FULL PARTICIPATION BY ALL THREE PARTIES, AND WE WILL DECLINE TO RESOLVE THE CONSTITUTIONAL AND RELATED SUBSTANTIVE ISSUES RAISED IN THE BRIEFS

Defendant insists in his most recent briefing, and at oral argument, that the underlying subpoena is supported by good cause, and that although its scope should be narrowed, the subpoena is generally enforceable. After recently being permitted to see the unsealed declaration and supporting exhibits, Facebook and the district attorney both contend the subpoena is *not* supported by good cause. The trial court, having allowed defendant to proceed ex parte and under seal, has not considered the input that we have obtained from the district attorney and Facebook.

We review a ruling on a motion to quash, like other discovery orders, for abuse of discretion. (*Pitchess, supra,* 11 Cal.3d at p. 535; see also *Facebook (Hunter) II, supra,* 46 Cal.App.5th at p. 118, rev. granted.) We conclude that the trial court below abused its discretion when ruling on the motion to quash by failing to apply the seven-factor *Alhambra* test. Under these circumstances we find it prudent to afford the trial court an opportunity to consider the good cause issue anew, this time with full participation by all three parties.

Facebook nevertheless urges, and the district attorney suggests, that we should overlook questions concerning the enforceability of the underlying subpoena and proceed to address and decide the various important underlying substantive legal issues discussed in the briefs. We recognize that the parties have undertaken substantial efforts to explore the Fifth and Sixth Amendment issues implicated in this case, as well as the various theories under which a proper state subpoena might be enforced against Facebook without resolving those constitutional issues. In light of the potential significance of all of these issues, however, we conclude it is preferable to reserve judgment on these questions until we can be confident that we are dealing with an otherwise enforceable subpoena.

Accordingly, in light of questions concerning whether the underlying subpoena is supported by good cause, we will direct the Court of Appeal to vacate the trial court's denial of the motion to quash and instruct the trial court to reconsider that motion.

VIII. WHETHER FACEBOOK IS COVERED UNDER THE SCA

Although we will not decide the important constitutional and related issues raised in the earlier briefs, we briefly address Facebook's suggestion that in *Facebook (Hunter), supra,* 4 Cal.5th 1245, we resolved in its favor the question of whether it is covered and bound by the SCA.

Facebook raises this argument in response to the assertion, jointly advanced by defendant and the district attorney, that Facebook's business model places it outside key provisions of the SCA and renders it subject to an enforceable state subpoena. The theory suggested by defendant and the

district attorney, which is premised on Facebook's Terms of Service[15] and Data Policy,[16] is that Facebook's business model of mining its users' communications content, analyzing that content, and sharing the resulting information with third parties to facilitate targeted advertising, precludes it from qualifying as an entity subject to the SCA. That law, defendant and the district attorney observe, covers only two types of entities — (1) those that provide "electronic communication service" (ECS) and (2) those that provide "remote computing service" (RCS) — and the law bars such entities from divulging to others the contents of their users' communications.[17] Defendant and the district attorney assert that Facebook is neither a provider of ECS nor of RCS under the provisions of the Act.

As noted, Facebook suggests our opinion in *Facebook (Hunter) supra*, 4 Cal.5th 1245, and decisions by other courts in

---

[15] Facebook, *Terms of Service* <www.facebook.com/legal/terms/plain_text_terms> (revised July 31, 2019) [as of August 10, 2020]. All Internet citations in our opinion will be archived by year, docket number and case name at <https://www.courts.ca.gov/38324.htm>.

[16] Facebook, *Data Policy* <www.facebook.com/full_data_use_policy> (revised April 19, 2018) [as of August 10, 2020].

[17] Regarding an entity that provides ECS, see 18 U.S.C. section 2510(15) [defining that term, as incorporated into the SCA by *id.,* § 2711(1)]; *id.*, section 2702(a)(1) [barring disclosure by an entity that provides ECS of any communication "in electronic storage by that service"]; *id.*, section 2510(17)(A)–(B) [defining "electronic storage"]. Regarding an entity that provides RCS, see *id.*, section 2711(2) [defining that term]; *id.*, section 2702(a)(2) [barring disclosure by an entity that provides RCS of "the contents of any communication which is carried or maintained on that service" when certain conditions apply].

prior litigation, have determined that Facebook operates as a provider of either ECS or RCS, and hence is covered by the Act. We will not assess the underlying merits of the business model thesis. Yet we observe that, contrary to Facebook's view, we have not determined that Facebook is a provider of either ECS or RCS under the Act.

Our opinion in *Facebook (Hunter) supra*, 4 Cal.5th 1245, undertook no substantive analysis concerning whether the entities in that case (including Facebook) provide ECS or RCS with regard to the communications there at issue. Because (1) prior decisions had found or assumed that Facebook and analogous social media entities provide *either* ECS or RCS with regard to the type of sought posts and/or messages at issue in those prior cases and in *Facebook (Hunter)*, and (2) neither party in *Facebook (Hunter)* contested the issue, we stated that we saw "no reason to question [that] threshold determination." (4 Cal.5th at p. 1268.) Accordingly, we assumed, but did not decide, that Facebook provided either ECS or RCS with regard to the communications sought — and hence was covered by the Act's general ban on disclosure of content by any entity providing those services. (4 Cal.5th at p. 1268 & fn. 26.) In so proceeding, we did not consider whether, under the business model theory subsequently proffered in this case, Facebook provides either ECS or RCS, or neither, under the Act. *That* potentially dispositive issue remains unresolved.[18]

---

[18] Facebook also asserts in its briefing that "*every* court to consider the issue has concluded that Facebook and other social media providers qualify as either an ECS or an RCS provider." (See, e.g., *State v. Johnson* (Tenn. Crim. App. 2017) 538 S.W.3d 32, 68–69, and cases cited.) And yet, it appears, *no* court,

IX. CONCLUSION

We direct the Court of Appeal to remand this matter to the trial court with instructions that the trial court vacate its order denying the motion to quash and reconsider the motion, with full participation by the parties, by assessing and balancing the seven *Alhambra* factors outlined *ante*, part IV.[19]

CANTIL-SAKAUYE, C. J.

We Concur:

CHIN, J.
CORRIGAN, J.
LIU, J.
CUÉLLAR, J.
KRUGER, J.
GROBAN, J.

---

including, most recently, two decisions relied upon by Facebook — *Facebook, Inc. v. Wint* (D.C. 2019) 199 A.3d 625, and *Facebook (Hunter) II*, *supra*, 46 Cal.App.5th 109 (rev. granted) — has considered the issue in light of the business model theory advanced by defendant and the district attorney.

[19] On June 12, 2020 — a week before oral argument — defendant filed a motion seeking to "augment" the record in this writ proceeding under California Rules of Court, rule 8.340(c), by presenting a "printout from the California Department of Corrections" concerning Renteria. Because the proffered document was not, as required by corresponding rule 8.155(a)(1), "filed or lodged in the case in superior court," nor does it constitute a "certified transcript — or agreed or settled statement — of oral proceedings," it is not properly subject to augmentation under rule 8.340(c), and the motion is hereby denied. In any event, the document's contents are irrelevant to our analysis and disposition in this proceeding.

FACEBOOK, INC. v. SUPERIOR COURT

S245203

Concurring Opinion by Chief Justice Cantil-Sakauye

As observed in the majority opinion, Lance Touchstone, defendant in the prosecution below (defendant), and intervener San Diego County District Attorney (the district attorney) jointly advance a business model theory that, they contend, places Facebook, Inc., outside the ambit of a 34-year-old federal law, the Stored Communications Act (18 U.S.C. § 2701 et seq.; hereafter SCA or Act).[1] I write separately to explore this theory in greater depth because, in my view, it deserves additional and focused attention, perhaps on remand in this case or at least in other similar future litigation.

Defendant and the district attorney focus on Facebook's authorization to undertake, and its practice of, mining its users' communications content, analyzing that content, and sharing the resulting information with third parties to facilitate targeted advertising. They assert this business model renders Facebook subject to a viable state subpoena duces tecum seeking the content of user communications, including restricted social media posts and private messages.

---

[1] All future section citations are to title 18 of the United States Code unless otherwise indicated.

This contention, which is grounded on Facebook's Terms of Service[2] and Data Policy,[3] posits that the mining, analyzing,

---

[2] Facebook, Terms of Service <www.facebook.com/legal/terms/plain_text_terms> (revised July 31, 2019) [as of August 10, 2020]. (All Internet citations in this opinion are archived by year, docket number, and case name at <http://www.courts.ca.gov/38324.htm>.) These "Terms" provide: "Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms, you agree that we can show you ads that businesses and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you. [¶] . . . . [¶] We collect and use your personal data in order to provide the services described above to you." (*Id.*, at pt. 2, *How our services are funded*.) Moreover, the Terms provide: "We need certain permissions from you to provide our services: [¶] . . . . [¶] [T]o provide our services we need you to give us some legal permissions (known as a 'license') to use this content . . . . [¶] Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means, for example, that if you share a photo on Facebook, you give us permission to store, copy, and share it with others (again, consistent with your settings) such as service providers that support our service or other Facebook Products you use." (*Id.*, at pt. 3, *Your Commitments to Facebook and Our Community,* pt. 3.3, *The permissions you give us,* pt. 3.3.1, *Permission to use content you create and share*.)

[3] Facebook, Data Policy <www.facebook.com/full_data_use_policy> (revised Apr. 19, 2018) [as of August 10, 2020]. The Data Policy describes what Facebook mines: "We collect the content, communications and other information you provide when you use our Products, including when you . . . message or

communicate with others. This can include information in or about the content you provide . . . . Our systems automatically process content and communications you and others provide to analyze context . . . . [¶] . . . . [¶] We also receive and analyze content, communications and information that other people provide when they use our Products." (*Id.*, at pt. I, *What kinds of information do we collect?/ Things you and others do and provide/ Information and content you provide/ Things others do and information they provide about you.*) Thereafter, Facebook's Data Policy explains, it employs users' mined and analyzed content to facilitate various services, including to "[p]rovide, personalize, and improve our Products [¶] . . . and make suggestions for you" by showing users "personalize[d] ads, offers, and other sponsored content." (*Id.*, at pt. II, *How do we use this information?/ Provide, personalize and improve our Products/ Ads and other sponsored content.*) In that regard, Facebook relates, it shares information about its users' content with "third-party partners . . . which [in turn] makes it possible to operate our companies and provide free services to people around the world." (*Id.*, at pt. III, *How is this information shared?/ Sharing with Third-Party Partners.*) Facebook states that it "do[es]n't *sell* any of your information to anyone," but instead "[s]har[es] with," "work[s] with," and "provide[s]" that information to "third-party partners." (*Ibid.*, italics added.) Specifically, for some partners, it supplies "aggregated statistics and insights that help people and businesses understand how people are engaging with their posts . . . and other content." (*Id.* at pt. III, *Partners who use our analytics services.*) And for advertisers, Facebook explains: "We provide . . . reports about the kinds of people seeing their ads and how their ads are performing." (*Id.*, at pt. III, *Sharing with Third-Party Partners/ Advertisers.*) At the same time, Facebook stresses: "[W]e don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better

and sharing activities that these provisions permit Facebook to undertake preclude Facebook from qualifying under the SCA *as a provider that is prohibited by the Act from disclosing user content*. Accordingly, defendant and the district attorney assert, Facebook cannot hold up the Act as a shield that protects it from complying with a viable state subpoena seeking such user communication content, including restricted posts and private messages.

Facebook does not contest that it mines, analyzes, and shares with third party advertisers information about content found in, among other things, its users' communications — including restricted posts and private messages. Facebook maintains, however, that these practices do not remove it from the applicable provisions of the SCA.

I outline below the key statutes and summarize defendant's and the district attorney's arguments, as well as Facebook's responses.

I. OVERVIEW OF THE BUSINESS MODEL ARGUMENT: ASSERTION THAT FACEBOOK DOES NOT PROVIDE "ECS" OR "RCS" — AND HENCE IS NOT PRECLUDED BY THE SCA FROM COMPLYING WITH A VIABLE STATE SUBPOENA

As we observed in *Facebook v. Superior Court* (*Hunter*) (2018) 4 Cal.5th 1245, 1264–1265, the SCA covers, and prohibits disclosure of, stored and/or electronic communications by *only* two specific types of entities — (1) those that provide "electronic

---

understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser." (*Ibid*.)

communication service" (ECS), and/or (2) those that provide "remote computing service" (RCS).[4] (§ 2702(a).) If an entity does not act as a provider of ECS or RCS with regard to a given communication, the entity is not bound by any limitation that the SCA places on the disclosure of that communication — and hence the entity cannot rely upon the SCA as a shield against enforcement of a viable subpoena seeking that communication.

Defendant and the district attorney argue that stored communications, including restricted posts and private messages, are subject to disclosure by Facebook pursuant to a viable subpoena. They assert this is so because, in light of the mining, analyzing, and sharing of licensed information about content that is authorized by Facebook's policies, Facebook does not qualify as an entity that provides either ECS or RCS with respect to the sought communications — and hence Facebook cannot rely on the SCA provisions that bar disclosure of stored communications.

To understand the business model argument, it is necessary to first review the SCA's statutory definitions of ECS and RCS.

II. ECS AND RCS AS DEFINED BY THE SCA

ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (§ 2510(15) [*incorporated into the SCA by* § 2711(1)].) Section 2702(a)(1), directs that an "*entity providing an electronic communication service to the public shall not*

---

[4] The Act lists exceptions under which such providers may (or in some circumstances must) disclose communications content (§ 2702(b)–(c) but no exception applies with regard to any restricted post or private message at issue in this case.

knowingly divulge to any person or entity the contents of a communication while [*the communication*] *is in electronic storage by that service.*" (Italics added.) "Electronic storage" is defined in section 2510(17), as "(A) *any temporary, intermediate storage of a* wire or *electronic communication incidental to the electronic transmission thereof*; and [¶] (B) *any storage of such communication by an electronic communication service for purposes of backup protection of such communication*." (Italics added.)[5]

RCS, by contrast, is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." (§ 2711(2).) Section 2702 (a)(2)'s introductory language directs that an "*entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service*" when certain conditions are met. (Italics added.)

The next parts of section 2702(a)(2) describe the conditions that will trigger the duty of an entity providing RCS to "not knowingly divulge" the contents of any communication carried or maintained by that entity. Defendant and the district attorney do not contend that Facebook fails to satisfy the first condition set out in subsection (a)(2)(A): the "carried or maintained" communication must be "on behalf of, and received

---

[5] By their terms, the two subdivisions of section 2510(17) establish that they refer to two separate types of storage, and past decisions have interpreted the statute to mean that "electronic storage" can be established by meeting either the definition in (A) or that in (B).

by means of electronic transmission from . . . a subscriber or customer of such service."

It is the second condition set out in section 2702(a)(2)(B) that lies at the center of the business model argument advanced by defendant and the district attorney. Under section 2702(a)(2)(B), the prohibition on disclosure by an entity that provides RCS applies only if the communication is carried or maintained on the service "*solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing*." (Italics added.)

This crucial passage is hardly a model of clarity. It appears to express two related conditions in order to qualify as a communication held by an entity that provides RCS: (1) the user's data must be transmitted to the provider "solely for the purpose of providing storage or computer processing services"; *and* (2) the entity must "not [be] authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." (§ 2702(a)(2)(B); see, e.g., Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act* (2010) 98 Geo. L.J. 1195, 1213–1214 (*Free at What Cost?*) [so construing the statute].) Based on this language, the author of the cited law journal and other commentators have argued that if the entity *is* "authorized to access the contents of any such communication for purposes of providing any services *other than* storage or computer processing" (§ 2702(a)(2)(B), italics added) — that is, for the purposes of providing any services *in addition to* storage or computer processing — the Act's bar on

disclosure is inapplicable.[6] In other words, these commentators reason, such an entity would not be acting as an RCS that is, in

---

[6] See *Free at What Cost?*, *supra*, 98 Geo. L.J. at page 1214 ["The Act's RCS privacy protections require that 'storage or computer processing' be the sole reason that a customer transmits her data to the cloud provider" but "[w]hen data is also shared with the cloud provider to facilitate contextual advertising, this requirement is not satisfied"; moreover, "[t]he Act . . . requires that the cloud provider . . . be authorized to access the customer's data [only] to provide the processing or storage service" — yet "by agreeing to share her data with the cloud provider for contextual advertising purposes, this additional requirement is unfulfilled"]; see also Katten, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud* (2011) 13 Vand. J. Ent. & Tech. L. 617, 640, fn. omitted (*Cloudy Privacy Protections*) [asserting that "when a customer consents to a user agreement which permits the service provider to access his data to provide targeted advertising, the user's emails may not be protected [under the SCA] as communications maintained by" an ECS or RCS]; Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing* (2012–2013) 29 Santa Clara Computer & High Tech. L.J. 451, 472 (fn. omitted) ["if the service provider and the user agreed that the provider can access the communication contents of users, for . . . purposes of contextual advertising, such contents can be disclosed" because such an entity is not acting as an RCS]; Fairfield & Luna, *Digital Innocence* (2014) 99 Cornell L.Rev. 981, 1062–1063 [observing that "Google (and many other free e-mail providers) scan e-mails for purposes of targeted advertising" and that resulting user information is not stored " 'solely for the purpose of providing storage or computer processing services' " — hence "[o]n this statutory reading" the SCA would not apply]; Raquel, Comment, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud* (2015) 55 Santa Clara L.Rev. 467, 495–496 (*Blue Skies Ahead*) [concluding that when "customers authorize access to their data for . . . advertising services in exchange for free access to the

turn, generally barred from disclosing communications content — and hence the entity would be subject to a viable subpoena duces tecum.

It is important to recognize that with regard to both general directives against disclosure by an entity providing ECS or RCS, "contents" is broadly defined by the SCA to "include[] any information concerning the substance, purport, or meaning of [the] communication." (§ 2510(8).) This definition would appear to encompass information *about* or relating to the content of a communication — not just the bare or exact text of a communication, including of any restricted post or private message.

III. THE ACT'S ECS AND RCS CATEGORIES SHOULD BE UPDATED OR REPLACED BY CONGRESS

Courts and commentators have long acknowledged that, as applied to contemporary entities, the 34-year-old SCA is woefully outdated. Eighteen years ago the decision in *Konop v. Hawaiian Airlines* (9th Cir. 2002) 302 F.3d 868, observed that because the SCA "was written prior to the advent of the Internet and the World Wide Web . . . , the . . . statutory framework is ill-suited to address modern forms of communication," and hence courts "have struggled to analyze problems involving modern technology within the confines of this statutory framework." Moreover, the court emphasized, "until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of

---

cloud services," the entity does not qualify as a provider under the SCA and "the data will be subject to disclosure"].

the law." (*Konop*, at p. 874.)[7] Seven years ago, a federal district court wrote, in evident frustration: "Most courts, including this one, would prefer that Congress update the statute to take into account the invention of the Internet." (*Ehling v. Monmouth Hosp. Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 666, fn. 2.)

The scholarly literature is similar. For example, Professor Orin S. Kerr has observed that the Act's ECS/RCS dichotomy "freez[es] into the law the understandings of computer network use as of 1986" — and he has urged Congress to amend the SCA to reflect current technology and conditions. (Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* (2004) 72 Geo.Wash. L.J. 1208, 1214 (*A User's Guide*).)[8] As Kerr has explained, Congress viewed

---

[7] See also, e.g., *Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965, 971, footnote 15 (*Crispin*) [observing that the "framework governing online communication is . . . old and has not been amended to keep pace with changes in technology"]; *In the Matter of the Application of the State of N.J. for Communications Data Warrants* (2017) 448 N.J.Super. 471, 484 ["Courts have expressed frustration with the failure to update the federal statute to keep pace with the advent of the Internet and social media platforms"]. Accord, *Anzaldua v. Northwest Ambulance & Fire Prot. Dist.* (8th Cir. 2015) 793 F.3d 822, 839, fn. 5 ["It is not always easy to square the decades-old SCA with the current state of email technology"]; *State v. Johnson* (Tenn.Crim.App. 2017) 538 S.W.3d 32, 68 ["Because the framework created in the SCA relies entirely on 1986 computing technology, determining the precise scope of its application to the type of social media communications at issue . . . presents difficulties"].

[8] See also, e.g., Zwillinger & Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field* (2007) 97 J. Crim. L. & Criminology 569, 597–598 [proposing the SCA be amended to

allow courts to order providers to disclose communications to criminal and civil litigants under specified circumstances]; Gleicher, Comment, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web* (2009) 118 Yale L.J. 1945, 1946 & 1954 [discussing the "dangers posed by the Act's continued reliance on" language "written for 1986 technology" — and observing that just as the sponsors of the SCA had warned that then-"existing law was 'hopelessly out of date,' . . . [t]oday, the Act itself suffers the same flaw"]; *Free at What Cost?, supra,* 98 Geo. L.J. 1195, 1196 & 1235 [observing that "[d]espite the rapid evolution of computer and networking technology since the SCA's adoption, its language has remained surprisingly static" and the "balance that the Act struck . . . may no longer be appropriate"]; Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act* (2011) 24 Harv. J. Law & Tech. 563, 566, fn. omitted ["Because Congress has not updated the statute, courts have struggled to apply the SCA in light of the explosive growth of the World Wide Web"]; *Cloudy Privacy Protections, supra*, 13 Vand. J. Ent. & Tech. L. 617, 620 [asserting the SCA "may not protect cloud-computing technologies" and proposing that Congress amend the Act to address that problem]; Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times* (2013) 63 Am.U. L.Rev. 267, 287 ["The Act's framework made sense in 1986 when service providers served two distinct functions," but subsequently the SCA "has become hopelessly outdated"]; Fairfield & Luna, *Digital Innocence, supra,* 99 Cornell L.Rev. 981, 1054–1063, 1056 [asserting "the advance of cloud computing" has rendered the ECS and RCS classifications "archaic," and those categories "largely obsolete"]; *Blue Skies Ahead, supra,* 55 Santa Clara L.Rev. 467, 492, fn. omitted [the "complicated ECS-RCS analytical framework . . . no longer bears any technological significance today"]; Brehm, Comment, *Downloading the Latest Protection Updates: Regularly Updating the Stored Communications Act* (2014) 16 Loy. J. Pub. Int. L. 1, 28–30 [urging creation of a commission to update the SCA by issuing regulations to accommodate new technologies and revise "antiquated definitions"]; Schlabach, Note, *Privacy in*

entities that provided ECS as those that afforded phone services and rudimentary e-mail. With regard to e-mail, "it was common for computers to copy the messages and store them temporarily pending delivery. The copies that these providers of 'electronic communication service' created and placed in temporary 'electronic storage' in the course of transmission, sometimes stayed on a provider's computer for several months." (*A User's Guide*, at p. 1213 [citing legislative history].) By contrast, as a general matter Congress viewed entities that provided RCS as those that undertook "outsourcing computer tasks" — for example, affording extra storage or data processing, both of which were then difficult if not impossible to accomplish with rudimentary home computers. And yet, "[r]emote computing services raised privacy concerns because the service providers often retained these copies of their customers' files for long periods of time." (*Id.*, at p. 1214 [citing legislative history].)

Because Congress has not acted to alter the relevant provisions of the SCA despite the pleas of courts and commentators that it do so, litigants and judges have no option but to apply the Act's outdated definitions to the evolved and still developing technology and entities of today.

---

the Cloud: The Mosaic Theory and the Stored Communications Act (2015) 67 Stan. L.Rev. 677, 695 [asserting the Act's "dated terminology threatens its effectiveness" and proposing amendments]; Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home* (2018) 86 Geo. Wash. L.J. Arguendo 1, 19, 24–29 [asserting that modern technology has rendered the Act's ECS/RCS distinctions outdated, making application of the SCA to modern stored information unclear — and proposing amendments to the Act].

IV. THE PARTIES' CONTENTIONS REGARDING WHETHER, UNDER THE ACT, FACEBOOK PROVIDES ECS, RCS, OR NEITHER

A. Whether Facebook Provides ECS

Defendant and the district attorney implicitly assert that, even if Facebook does to *some* extent provide electronic storage that is "temporary [and] intermediate . . . incidental to the electronic transmission thereof" (§ 2510(17)(A)) — or "for purposes of backup protection of [a] communication" (§ 2510(17)(B)) — nevertheless, Facebook still falls outside Congress's understanding of an entity that provides ECS. They argue that because (1) Facebook is authorized to mine, analyze, and share with third party advertisers licensed information about its users' content (and actually does all these things), and (2) Facebook stores users' communications indefinitely, lets users share the stored data with others, and facilitates manipulation of the data by the user thereafter, Facebook conducts itself in ways that go far beyond what Congress contemplated in 1986 that any ECS would undertake. Accordingly, they argue, a court should find that Facebook does not act as an entity that provides ECS with regard to communications such as those sought in this case, and hence is subject to a viable state subpoena.

Facebook, for its part, asserts that it qualifies as a provider of ECS because communications such as those sought in this case are either in "temporary or intermediate storage" (§ 2510(17)(A)), or they are housed "for purposes of backup protection" (§ 2510(17)(B)) and thus are barred from disclosure under section 2702(a)(1). Facebook insists that whether it "has authority to access [a] communication in connection with the service is . . . irrelevant to whether [the communication] is in electronic storage."

Facebook relies on a number of decisions finding or stating that it qualifies as a provider of ECS. (Maj. opn., *ante*, at p. 41, fn. 18.) But as observed in *In the Matter of the Application of the United States of America for a Search Warrant* (D.Or. 2009) 665 F.Supp.2d 1210, 1214, whether an entity provides ECS, or RCS, or neither, is a context-dependent inquiry: The "distinction serves to define *the service* that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), *rather than to define the service provider itself*." (Italics added.)[9]

Consistent with this understanding, other federal decisions have held that when an entity analogous to Facebook (in those cases, providers of e-mail and text messages) retains a communication beyond the initial sending and provisional back-up stage, then once that message has been opened/accessed, the entity *no longer acts as a provider of ECS but rather transforms*

---

[9] Accord, Kerr, *A User's Guide, supra,* 72 Geo.Wash. L.J. 1208, 1215–1216: "The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract. A provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications." See also *id.*, at pages 1216–1218 [asserting that e-mails in transit or that have been delivered yet not opened, are stored by a provider of ECS; whereas e-mails that have been opened and left on a server are stored by a provider of RCS].

into a provider of RCS.[10] Under the reasoning of these cases, the same would seem to apply concerning Facebook — in which event its conduct should be examined under RCS, rather than ECS standards. At least one court appears to have so held. (*Crispin, supra,* 717 F.Supp.2d 965, 987 [regarding private messages that had been opened, Facebook operates not as a provider of ECS, but as a provider of RCS].)

Thus, whether Facebook should be found to qualify as a provider of ECS under the SCA appears open to question. Moreover, assuming that Facebook might qualify initially or provisionally as an entity that provides ECS, it seems that Facebook may also be obligated to establish its qualification as an entity that provides RCS with respect to stored communications sought in a viable state subpoena.

B. Whether Facebook Provides RCS

By the language and conditions established in section 2702(a)(2)(B), it appears Congress was aware that, in connection with rendering storage and computer processing services, an

---

[10] *U.S. v. Weaver* (C.D.Ill. 2009) 636 F.Supp.2d 769, 772–773, quoting § 2703(b)(2) [relying on the language and legislative history of the SCA to conclude that once a user opened an e-mail message and kept that message on the user's Hotmail account, Microsoft maintained the message " 'solely for the purpose of providing storage or computer processing services to such subscriber or customer,' " ceased being a provider of ECS, and transformed into a provider of RCS]; *Flagg v. City of Detroit* (E.D.Mich. 2008) 252 F.R.D. 346, 362–363 [finding that Skytel, an entity that provided text message services, had initially been a provider of ECS; but after text communications had been accessed and stored, Skytel transformed into a provider of RCS]. See generally the useful discussion of these and related cases in *Crispin, supra,* 717 F.Supp.2d 965, 984–987.

entity that provides RCS would be expected to have some authority to access its users' data and communications for the purpose of affording such storage and computer processing services. As noted, the section bars a provider of RCS from divulging "the content of any electronic transmission that is carried or maintained on its service — . . . solely for the purpose of providing storage or computer processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." (§ 2702(a)(2)(B).) On the other hand, because the subsection precludes disclosure only if the entity is *not* authorized to access its users' communications for purposes "other than storage or computer processing," the court in *Juror Number One v. Superior Court* (2012) 206 Cal.App.4th 854, 862 reasoned in dictum: "[I]f the [entity] *is* authorized to access the customer's information for other purposes, such as to provide targeted advertising, SCA protection may be lost." As observed *ante*, footnote 6, commentators have suggested or concluded the same, asserting that when social media users authorize an entity to access their data and communications in order to facilitate targeted advertising, the entity may not, or does not, qualify under the SCA as one that provides RCS — and thus the entity is not barred from disclosing such content.

Consistent with these views, defendant and the district attorney both assert that in light of Facebook's business model of mining, analyzing, and sharing information about its users' communications content, Facebook cannot qualify under section 2702(a)(2)(B) as an entity that provides RCS. They argue that by compelling its users to give it authorization (a broad and transferable worldwide license — see *ante*, fn. 2) to utilize

information about its users' mined and analyzed content for sharing with third party advertisers, Facebook goes substantially beyond the limited authorization that would be necessary for it "solely" to provide "storage and computer processing." This, they assert, shows that Facebook *is* "authorized to access the contents of . . . communications *for purposes of providing . . . services other than* storage or computer processing" — and demonstrates that Facebook is authorized to act *in precisely the manner the statute says it must not* if it wishes to qualify as a provider of RCS that is prohibited from disclosing its users' communications content. Accordingly, they argue, Facebook cannot qualify as an entity that provides RCS under the Act and thus cannot raise the SCA as a shield against being forced to comply with a viable state subpoena.

Facebook responds that everything it is authorized to do — including all mining, analyzing, and sharing of its licensed information about its users' communications — constitutes "computer processing services," and hence is contemplated by and covered under the Act in section 2702(a)(2)(B). In other words, Facebook maintains that the phrase "computer processing services" should be broadly construed, and so interpreted, Facebook's authority to access information is not for a purpose *other than* computer processing but instead is *for* computer processing. Although Facebook cites a federal decision and legislative history, along with Professor Kerr's article, to support its view that "computer processing services" in section 2702(a)(2)(B) should be broadly construed, it seems questionable whether those sources buttress Facebook's position. Indeed, they may suggest the opposite — that the term

was intended to have a narrow, rather than broad, interpretation.[11]

Finally, Facebook insists, "every court to consider" whether Facebook *itself* qualifies as an entity that provides RCS (or ECS, or both) has held that it meets at least one if not both tests. Yet, as the majority opinion observes, it appears that *no* court has ever been asked to address, with regard to Facebook itself (or, for that matter, any analogous entity), the specific claim advanced by defendant and the district attorney here: That by virtue of its business model (under which it mines, analyzes, and shares licensed information about its users' communications), and because Facebook has motivating purposes beyond facilitating temporary storage during transmission, or backup of its users' communications, Facebook falls outside Congress's contemplation of an entity that provides RCS or ECS. Indeed, as the majority opinion observes, *ante* at page 41 and footnote 18, the issue remains unresolved.

---

[11] See *Low v. LinkedIn Corp*. (N.D.Cal. 2012) 900 F.Supp.2d 1010, 1024, fn. omitted [rejecting an argument that LinkedIn, by "disclos[ing its users'] IDs and the URLs of viewed [profile] pages to third parties," acted as an RCS provider, and in the process, appearing to endorse a narrow, rather than broad, view of the term computer " 'processing services' "]; Senate Report No. 99-541, 2d Session, page 3 (1986) [suggesting that Congress, in focusing on entities that provide data processing "outsourcing functions," contemplated a narrow understanding of "computer processing" when it established the RCS category]; Kerr, *A User's Guide, supra*, 72 Geo.Wash. L.Rev. 1208, 1230–1231 [asserting that the key term "processing services" should be limited and construed narrowly, to "refer to outsourcing functions," and not broadly, which would essentially include every website].)

C. Tentative Assessment of Facebook's Policy Arguments

In addition to contending that the statutory language supports its status as an entity that provides ECS or RCS, Facebook asserts that policy considerations demonstrate it *must* be found to so qualify because concluding otherwise would (1) unduly disrupt and impair technological innovation, (2) disappoint users' settled privacy expectations, and (3) frustrate its ability to protect against malware.

The first two contentions certainly should give a court pause before holding that Facebook and similar entities fall outside section 2702(a), and thus are not generally barred by that provision from voluntarily disclosing their users' communications, including restricted posts and private messages. Nonetheless, for practical marketplace reasons, it may be doubted that such a holding would likely lead to such disruptions or voluntary disclosures by most internet entities, absent legal compulsion.[12]

Neither does it appear likely that law enforcement actors would attempt to compel entities to disclose users' communications with, as Facebook asserts in its briefing, "a

---

[12] Facebook posits that if disclosure is not prohibited by the SCA, a "provider could choose to disclose a communication to anyone." Moreover, as Facebook observes, if an entity were to do so it might cause users to "quickly lose confidence in communications technology as their privacy rights disappear, undermining the stated intent of Congress in enacting the SCA." Yet it appears that an entity that became known for disclosing its users' communications on its own, without legal compulsion, would not long survive in the market — and hence would refrain from doing so in the first place.

mere subpoena"; other laws and authority already protect against that.[13] Nor does it seem that a narrower construction of the phrase would leave Facebook and similar entities unable to protect against malware.[14] Finally, as a matter of policy, a holding finding Facebook to lie outside the SCA might have the beneficial effect of spurring long-needed congressional adjustment of the outdated Act, as repeatedly advocated by courts and commentators. (See *ante*, pt. III.)

---

[13] California's Electronic Communications Privacy Act of 2015 (Pen. Code, § 1546 et seq.) generally requires a warrant or comparable instrument to acquire such a communication (*id*., § 1546.1, subd. (b)(1)–(5)), and in any event, it *precludes use of a subpoena* "for the purpose of investigating or prosecuting a criminal offense" (*id*., subd. (b)(4)). Moreover, federal case law requires a search warrant, instead of a mere subpoena or court order, before a governmental entity may obtain private electronic communications. (*U.S. v. Warshak* (6th Cir. 2010) 631 F.3d 266, 288 [pertaining to e-mail communications].)

[14] Facebook asserts that it and similar entities should not be forced to "choose between the security and integrity of their service, and the privacy of the communications maintained on that service." But this appears to be a questionable dichotomy. It would seem that protection against malware and viruses, etc., might be viewed as reasonably necessary to ensure the safety and integrity of any computer system, and in that sense, such monitoring and resulting measures to counteract malware might well be found to fall within a narrower definition of "computer processing," even if that same term would not broadly encompass the sharing with third party advertisers of mined and analyzed information about content. In any event, Facebook or any similar entity might, presumably, revert to an old-school pay-for-service business model, and still undertake such services to scan and protect against malware, and viruses, etc., while at the same time avoiding sharing with third party advertisers mined and analyzed information about content.

V. CONCLUSION

For reasons outlined above, the business model theory deserves additional and focused attention. Perhaps the issue will arise on remand below, if the trial court again determines — this time after full and open participation by the parties and consideration of the good cause factors discussed in the majority opinion — that the underlying subpoena, as it exists or as it might be revised, is viable. In any event, the business model issue deserves to be addressed when a similar issue arises in analogous future litigation.

CANTIL-SAKAUYE, C. J.

FACEBOOK, INC. v. SUPERIOR COURT

S245203

Concurring Opinion by Justice Cuéllar

Lance Touchstone served a subpoena on Facebook, but the company denies it has any responsibility to honor it because it claims protection under the federal Stored Communications Act (18 U.S.C. § 2701 et seq.; the SCA). We decline to address the parties' arguments about this issue because it remains unclear whether good cause supports Touchstone's subpoena. (Cf. *Loeffler v. Target Corp.* (2014) 58 Cal.4th 1081, 1102.) But as the Chief Justice observes in her own separate opinion, nothing in our majority opinion renders any less important the crucial matter of how broadly to read the SCA — and, in particular, whether it protects Facebook and similar entities from the duty to honor valid subpoenas issued by our state courts. I write to explain why, in the appropriate case, courts ought to take up that very question.

Congress enacted the SCA in 1986 to create a "fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." (H.R.Rep. No. 99-647, 2d Sess., p. 19 (1986).) To this end, the SCA "creates limits on the government's ability to compel [network service] providers to disclose information in their possession about their customers and subscribers." (Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* (2004) 72 Geo.Wash. L.J. 1208, 1212, fn. omitted.) Yet the SCA does not apply to all providers storing online communications.

As the majority opinion explains, the only entities covered are those providing "electronic communication service" or "remote computing service." (Maj. opn., *ante*, at p. 40; see also Kerr, at p. 1214 ["The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications"].) Courts — including our own — have nonetheless assumed that social media entities such as Facebook are regulated by the SCA. (See, e.g., *Facebook v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245, 1268, fn. omitted ["We see no reason to question [the] threshold determination" that Facebook is "governed by . . . the SCA"].)

Why that assumption deserves to be probed is something this case starkly illustrates. Touchstone and the San Diego County District Attorney devote a substantial portion of their briefing to a theory that no court appears to have addressed: that because Facebook's terms of service grant Facebook legal rights to users' communications content, and because Facebook shares users' data with third parties, the company doesn't fall within the ambit of the SCA. For this reason, they argue, Facebook may not rely on the SCA as a shield that protects it from complying with a subpoena seeking users' communications.

Whether or not these arguments are ultimately persuasive, courts should examine them in the appropriate cases. They should endeavor to discern whether Congress's purpose in enacting the SCA encompassed protecting communications held by social media companies such as Facebook. That question is an important one: Computers, smartphones, and digital media have become ubiquitous in our society, making ever more cases turn on evidence stored by digital platforms. (See, e.g., *Facebook v. Superior Court (Hunter*) (2020) 46 Cal.App.5th 109, review granted June 10,

2020, S260846).) Facebook acknowledged as much at oral argument, admitting that if it were free from any obligation "not to turn over this information, then we wouldn't be here" — its "only interest in this case" is in resolving the scope of the SCA and the protections it provides. So the Chief Justice is right to admonish: Arguments regarding the SCA "deserve[] additional and focused attention" in future litigation. (Conc. opn. of Cantil-Sakauye, C. J., *ante*, at p. 21.) Given the SCA's potentially profound implications on the availability of such digital evidence, I agree. The companies storing ever-expanding troves of data about our lives would surely benefit from greater clarity about the full extent of their responsibility to honor a valid subpoena. So would the people of California.

CUÉLLAR, J.

See next page for addresses and telephone numbers for counsel who argued in Supreme Court.

Name of Opinion Facebook, Inc. v. Superior Court

Unpublished Opinion
Original Appeal
Original Proceeding
Review Granted XX 15 Cal.App.5th 729
Rehearing Granted

Opinion No. S245203
Date Filed: August 13, 2020

Court: Superior
County: San Diego
Judge: Kenneth Kai-Young So

Counsel:

Perkins Coie, James G. Snell, Christian Lee; Gibson, Dunn & Crutcher, Joshua S. Lipshutz and Michael J. Holecek for Petitioner.

Horvitz & Levy, Jeremy B. Rosen, Stanley H. Chen and Eric S. Boorstin for Google Inc., Oath Inc., Twitter, Inc., and California Chamber of Commerce as Amici Curiae on behalf of Petitioner.

No appearance for Respondent.

Megan Marcotte, Chief Deputy Alternate Public Defender, and Katherine I. Tesch, Deputy Alternate Public Defender, for Real Party in Interest.

Todd W. Howeth and Michael C. McMahon for the California Public Defenders Assocation and the Public Defender of Ventura County as Amici Curiae on behalf of Real Party in Interest.

Law Offices of J.T. Philipsborn, John T. Philipsborn; Sanger Swysen & Dunkle, Stephen K. Dunkle; The Law Office of Donald E. Landis, Jr., and Donald E. Landis, Jr., for California Attorneys for Criminal Justice as Amicus Curiae on behalf of Real Party in Interest.

Jeff Adachi, Public Defender, Matt Gonzalez, Chief Attorney, Dorothy Bischoff, Deputy Public Defender, for San Francisco Public Defender's Office as Amicus Curiae on behalf of Real Party in Interest.

Summer Stephan, District Attorney, Mark A. Amador, Linh Lam and Karl Husoe, Deputy District Attorneys for Intervener.

Counsel who argued in Supreme Court (not intended for publication with opinion):

Katherine Tesch
Deputy Alternate Public Defender
450 B. Street, Suite 1200
San Diego, CA 92101
(619) 446-2900

Kal Husoe
Deputy District Attorney
330 W. Broadway, Suite 860
San Diego, CA 92101
(619) 531-4213

Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP
555 Mission Street
San Francisco, CA 94105
(415) 393-8200