

The Inquisitive Prosecutor's Guide



A Publication of the Santa Clara County District Attorney's Office

The Santa Clara County District Attorney's Office is a State Bar of California
Approved MCLE Provider: 2748

www.santaclara-da.org

Date: September 21, 2020

**2020-IPG-46 (SUBPOENAS FOR THIRD-PARTY
RECORDS -FACEBOOK V. SUPERIOR COURT)**

This IPG discusses the latest case from the California Supreme Court on subpoenaing third party records in a criminal case with a focus on obtaining social media records. (*Facebook v. Superior Court of San Diego County (Touchstone)* (2020) 10 Cal.5th 329. If you ever plan to subpoena such records or to quash a subpoena seeking such records, this is the IPG for you. Accompanying this IPG is a bench memo based on this latest decision (and other relevant case law) that can be used to help provide guidance for a trial court asked to decide whether a criminal defendant is entitled to receive the documents despite a motion to quash the subpoena in whole or part – assuming that the federal Stored Communications Act does not otherwise bar disclosure. The memo also discusses how a court should determine whether to allow the defense to seek disclosure by way of sealed affidavits and ex parte.

The podcast features Santa Clara County Deputy District Attorney Daniel Kassabian and provides **65 minutes of (self-study) MCLE general credit**.

It may be accessed and downloaded at: <http://sccdaipg.podbean.com/>.

***IPG is a publication of the Santa Clara County District Attorney's Office©. Reproduction of this material for purposes of training and use by law enforcement and prosecutors may be done without consent. Reproduction for all other purposes may be done only with the consent of the author.**

**A Defendant Subpoenaing Social Media Records of a Third Party Must Establish Good Cause (Which is *Not* the Same as “Plausible Justification”) for Their Release. And a Court Deciding Whether Good Cause Has Been Established Must: (i) Explicitly Consider and Balance 7 Factors as Described in the Opinion; (ii) Place Significant Weight on the Confidentiality and Constitutional Rights of Persons (Including Those Provided by Marsy’s Law) Whose Records are Sought; and (iii) Be Cautious in Allowing Defendants to Proceed Ex Parte and Under Seal.
Facebook v. Superior Court of San Diego County (Touchstone)
(2020) 10 Cal.5th 329 [citations to 2020 WL 4691493]**

Facts and (Somewhat Convolved) Procedural Background*

The defendant (Touchstone) was charged with shooting and attempting to murder a man named Renteria. (*Id.* at p. *2.) Renteria is the boyfriend of defendant’s sister (Rebecca) and lived with her. The defendant joined them for a few days to visit with his sister. (*Id.* at p. *3.)

On the morning of the shooting (for unspecified reasons), Renteria decided to hide Rebecca’s firearms, and some of defendant’s ammunition by placing them into a secure container in Rebecca’s attic. (*Ibid.*) Renteria left the home sometime after that. Renteria then began receiving increasingly aggressive messages from Rebecca. Renteria responded to Rebecca and her brother, telling them that “if you try anything, you’re going to jail for a long time.” Renteria stated that “he had told Rebecca and defendant that if they were ‘setting [him] up for something,’ then they ‘would be arrested.’” (*Id.* at p. *4.) Renteria told Rebecca over the phone that he would return to the house to speak with her. After sundown, Renteria returned to the home. He unlocked and entered the front door. The defendant shot Renteria. Photographs taken by Renteria on his cell phone after he entered the home showed Renteria was unarmed when the defendant raised his gun and prepared to shoot Renteria. (*Ibid.*)*

***Editor’s note:** The above facts were elicited at the preliminary examination.

After the shooting incident, Renteria “posted updates of his physical recovery from the hospital, requesting private messages over the Facebook messaging system. On the public portion of his Facebook page that is visible to all Facebook users, [Renteria] posted updates of court hearings in this case, asking his friends to attend the preliminary hearing. In public posts [Renteria] also

discussed his personal use of guns and drugs, and described his desire to rob and kill people.” (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 733.)*

***Editor’s note:** Some of the relevant facts are drawn from the lower court of appeal opinion cited directly above. That opinion, of course, if not citable, but information from that opinion helps explain things.

Five months after the preliminary hearing, defendant issued a subpoena demanding “*all* of Renteria’s Facebook communications (including restricted posts and private messages), and [made] a related request that Facebook preserve all such communications, by offering a *sealed* declaration describing and quoting [but not attaching] certain public Facebook posts made by Renteria after the shooting that, defendant asserted, revealed Renteria’s violent general musings.” (*Id.* at p. *5, emphasis added by IPG.)

The sealed declaration (*which was later unsealed*, see this IPG, at p. 7) stated: “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.” (*Ibid.*)

“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.” (*Ibid.*) Facebook then preserved Renteria’s account as directed. But it moved to quash the subpoena on the ground the Stored Communications Act (SCA) (18 U.S.C.2 § 2701 et seq.) prohibited disclosure of the contents of the account and asserted the defendant “could obtain the requested contents directly from the victim or by working with the prosecutor to obtain a search warrant based on probable cause.” (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 734.)

Defendant opposed the motion to quash, disagreeing that the SCA prohibited disclosure and claiming he had established the requisite “plausible justification” based on facts recited in his *publicly*-filed brief that: “(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.’” (*Id.* at p. *5, emphasis added by IPG.)

In conjunction with his brief, defendant filed a second *sealed* declaration. The defendant's reason for seeking to file a sealed declaration was 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." (*Ibid.*)

In a redacted version of the second declaration, 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 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]." (*Id.* at p. *5, emphasis added.)

At the motion to quash, "defense counsel represented that the prosecution refused to issue a search warrant for the material and that she has been unable to locate the victim to serve him with a subpoena." (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 734.)

The trial court, which reviewed both the unredacted and redacted declarations, "denied the motion to quash and ordered Facebook to produce the contents of the victim's account for in camera inspection by a certain date." (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 734.)

Facebook then sought a writ in the Court of Appeal "directing the trial court to vacate its order denying the motion to quash the subpoena and to enter a new order granting the motion to quash. Facebook contend[ed] the trial court abused its discretion by denying the motion to quash and ordering production of documents for in camera inspection because the SCA prohibit[ed] Facebook from disclosing the content of its users' accounts in response to a subpoena. Facebook further contend[ed] that compelling it to disclose the contents of [Renteria's] account is not necessary to preserve [the defendant's] constitutional right to a fair trial because [the defendant] can obtain the contents directly from the victim or through the prosecutor via a search warrant." (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 734.)

NOTE TO READER

Pages 5-7 of this IPG discuss the various issues raised in the Court of Appeal and *additional* issues upon which briefing was request by the California Supreme Court. However, **none** of these issues were ultimately decided by the California Supreme Court, which instead focused on the question of whether there had been an adequate showing of good cause and what factors should go into the analysis when confidential third party records are subpoenaed by the defense. The other issues are worth being aware of (because some or all may eventually have to be litigated) but they are *not necessary* to understanding the existing opinion and a reader should feel free to skip to the middle of page 7 if understanding the existing opinion is all that is desired.

The Lower Court of Appeal Opinion: **Facebook, Inc. v. Superior Court (2017) 15 Cal.App.5th 729**

The Court of Appeal **did not focus** on the question of whether there had been a sufficient showing of good cause. Rather, it focused on the issue of whether the federal SCA prohibited Facebook from disclosing the information sought and on whether the defendant, nevertheless, had a constitutional right to obtain social media records from an electronic communication or remote computing service at the pre-trial stage. (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 733.) The Court of Appeal also requested briefing on (i) whether the supremacy clause prohibited enforcement of the subpoenas; (ii) whether, assuming “the materiality of private electronic communications is shown during trial,” a trial court can compel a subscriber (such as [Renteria]) or a witness who is also a recipient of a private electronic communication from the victim to consent to disclosure by Facebook of electronic communications for an in camera review”; and (iii) whether a trial court “may compel a witness to produce private electronic communications, what procedures or protections exist, or may be implemented to prevent a witness from deleting the communications.” (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 733.)

The Court of Appeal treated Facebook as an electronic communication service provider and held that, subject to inapplicable exceptions, the SCA expressly prohibited such a service provider from “knowingly divulg[ing] to any person or entity the contents of a communication.” (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 748, citing to U.S.C. § 2702(a)(1).) The Court of Appeal also treated the nonpublic information sought as “privileged” and **rejected** defendant’s claims that the SCA violated the Confrontation Clause or Due Process insofar as it barred disclosure of otherwise privileged information for purposes of his pretrial investigation of the prosecution’s case. (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 741, 745.)

Accordingly, the Court of Appeal held the “supremacy clause (U.S. Const., art. VI) prohibit[ed] enforcement of the trial court’s order because ‘California’s discovery laws cannot be enforced in a way that compels [a provider] to make disclosures violating the [SCA].’” (*Facebook, Inc. v. Superior Court* (2017) 15 Cal.App.5th 729, 748.)

The defendant then sought review in the California Supreme Court. And review was granted.

The Issues Identified in the Original Grant of Review

In granting review, the California Supreme Court asked the parties “to include and address the following:

“(1) If, on remand and in conjunction with continuing pretrial proceedings, the prosecution lists the victim as a witness who will testify at trial (see Pen. Code, §§ 1054.1, subd. (a); 1054.7) and if the materiality of the sought communications is shown, does the trial court have authority, pursuant to statutory and/or inherent power to control litigation before it and to insure fair proceedings, to order the victim witness (or any other listed witness), on pain of sanctions, to either (a) comply with a subpoena served on him or her, seeking disclosure of the sought communications subject to in camera review and any appropriate protective or limiting conditions, or (b) consent to disclosure by provider Facebook subject to in camera review and any appropriate protective or limiting conditions?”

(2) Would a court order under either (1)(a) or (1)(b) be valid under the Stored Communications Act, 18 U.S.C., section 2702(b)(3)?

(3) Assuming orders described in (1) cannot properly be issued and enforced in conjunction with continuing pretrial proceedings, does the trial court have authority, on an appropriate showing during trial, to issue and enforce such orders?

(4) Would a court order contemplated under (3) be proper under the Stored Communications Act, 18 U.S.C., section 2702(b)(3)? With regard to questions (1)-(4), see, e.g., *O’Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 44 Cal.Rptr.3d 72; *Juror Number One v. Superior Court* (2012) 206 Cal.App.4th 854, 142 Cal.Rptr.3d 151; *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 179 Cal.Rptr.3d 215; and the Court of Appeal decision below, *Facebook, Inc., v. Superior Court (Touchstone)* (2017) 15 Cal.App.5th 729, 745-748, 223 Cal.Rptr.3d 660.

(5) As an alternative to options (1) or (3) set forth above, may the trial court, acting pursuant to statutory and/or inherent authority to control the litigation before it and to insure fair proceedings, and consistently with 18 U.S.C. section 2702(b)(3), order the prosecution to issue a search warrant under 18 U.S.C. section 2703 regarding the sought communications? (Cf. *State v. Bray* (Or.App. 2016) 281 Or.App. 584, 383 P.3d 883 [pets. for rev. accepted June 15, 2017. . .].) In this regard, what is the effect, if any, of California Constitution, article I, sections 15 and 24?” (*Facebook v. S.C. (Touchstone)* (Cal. 2018) 227 Cal.Rptr.3d 1 [408 P.3d 406].)

Additional Issues Identified

In 2018, the San Diego District Attorney’s Office asked to intervene in the case (i.e., to represent the interests of the prosecution in the outcome of the decision). The California Supreme Court permitted intervention but deferred briefing pending finality of another case being reviewed: *Facebook v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245 [hereinafter “*Hunter*”].)*

***Editor’s note:** In *Hunter*, the California Supreme Court had the opportunity to address some of the same issues raised in the instant case. However, the Court ultimately decided the case by finding that while the federal SCA appeared “to bar providers from disclosing electronic communications configured by the user to be private or restricted” (*Hunter*, at p. 1262), “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. (*Facebook, Inc. v. Superior Court of San Diego County (Touchstone)* 2020 WL 4691493 [hereinafter “*Touchstone*”] at p. *2 citing to *Hunter* at pp. 1250.)

After the San Diego District Attorney’s Office intervened, two additional potentially dispositive issues were spawned: “whether Facebook users expansively consent to disclosure of all communications; and whether Facebook’s business model removes it from coverage under the SCA.” (*Touchstone* at p. *3.)

Eventually, however, the California Supreme Court in *Touchstone* pivoted and began focusing on a different question than those previously raised: “***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.*** (*Touchstone* at p. *1.)

The California Supreme Court may have shifted its focus after it looked at the sealed declaration and exhibits filed by the defendant and realized that things were not exactly as they appeared to

be. It then informed all parties that it contemplated fully unsealing the April 21, 2017 sealed declaration and related exhibits as to all *the parties* and partially unsealing the declaration and exhibits for everyone else.* None of the parties objected and relevant previously sealed portions of defendant’s sealed declarations were unsealed. (*Touchstone* at p. *6.)

***Editor’s note:** As to the parties, *all* of the April 21, 2017 sealed declaration and related exhibits (which quote from and present copies of public social media posts and conditionally confidential probation reports) were unsealed pursuant to California Rules of Court, rule 8.46(f)(3). (*Touchstone* at p. *6, fn. 4.) As to what was made available to the public via the opinion, the Court stated: “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.” (*Touchstone* at p. *6, fn. 4.)

Holding and Analysis

1. The California Supreme Court did not actually decide any of the “significant substantive legal issues” because it determined that, due to underlying factual and related problems (such as the absence of good cause and too readily allowing the defense to proceed *ex parte* and under seal), the underlying subpoena might not be enforceable. (*Touchstone* at pp. *1-*2.)
2. Instead, after noting the lack of a “clear roadmap or set of factors to be applied by trial courts” in deciding whether to grant a motion to quash a subpoena *duces tecum* directed to a third party and the lack of “full adversarial engagement” in the trial court, the California Supreme Court decided to use the opinion to issue a set of guidelines highlighting seven factors that a trial court should explicitly consider and balance “both for the benefit of this litigation and other similar cases.” (*Id.* at p. *2.)
3. The California Supreme Court then held that, in light of these guidelines, “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.” (*Ibid.*)
4. Accordingly, the California Supreme Court directed “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.” (*Ibid.*) Moreover, the California Supreme Court ordered the trial court to consider the good cause issue anew with full participation by all three parties. (*Id.* at p. 16.)

“Relevant Law Concerning a Motion to Quash a Criminal Subpoena Duces Tecum”*

***Editor’s note:** This sub-title is taken directly from the opinion itself at p. *6.

5. “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.” (*Touchstone* at p. *6.)
6. However, “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.’” (*Id.* at p *6 citing to Pen. Code, § 1326, subd. (c).)
7. Moreover, while “no substantial showing is required to *issue* a criminal subpoena duces tecum, . . . 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.’” (*Ibid*, emphasis added.)

***Editor’s note (Part I of II):** Some of the California Supreme Court’s discussion in *Touchstone* regarding when a good cause showing is required could be interpreted as implying that it is *only* when a motion to quash is made that there is a need to show good cause for the records release – otherwise disclosure is automatic. However, for several reasons, it would be a mistake to infer such an implication from that discussion.

First, the *Touchstone* court itself stated that the reasons the documents are provided to the court, instead of the party, is so the court can do an in camera review to “determine whether or not the [requesting party] is entitled to receive the documents.” (*Id.* at p. *6.)

Second, previous case law has not placed such a limitation on the requirement of good cause. (See e.g., *People v. Superior Court* (2000) 80 Cal.App.4th 1305, 1316 [citing to *Pitchess v. Superior Court* (1974) 11 Cal.3d 531, 536 for the proposition that a “criminal defendant has a right to discovery by a subpoena duces tecum of third party records *by showing* ‘the requested information will facilitate the ascertainment of the facts and a fair trial’ and to *People v. Blair* (1979) 25 Cal.3d 640, 651 for the proposition that “issuance of a subpoena duces tecum ... is purely a ministerial act and does not constitute legal process in the sense that it entitles the person on whose behalf it is issued to obtain access to the records described therein *until a judicial determination has been made that the person is legally entitled to receive them*”], emphasis added by IPG.)

***Editor’s note (Part II of II):**

Third, in Justice Hoffstadt’s treatise on California Criminal Discovery, it expressly states that “[i]f a third party produces documents in response to a subpoena without moving to quash or otherwise objecting, the subpoenaing party is still not automatically entitled to those documents.” (*Id.* at p. 390.) The treatise then notes that the “subpoenaing party must show ‘good cause’ for acquiring the subpoenaed records” and identifies the factors a court must consider in assessing good cause. (*Ibid.*) This is highly significant because in *Touchstone*, the California Supreme Court repeatedly and approvingly cited to this treatise as identifying the proper guidelines for assessing good cause *at the very pages* in the treatise which discuss what showing is required when *no* motion to quash is made. (See *Touchstone* at pp. *6, citing to Hoffstadt at pp. 390-391.)

Fourth, courts have a sua sponte duty to protect third party privileges on behalf of absent victims. (See *People v. Superior Court (Humberto S.)* (2008) 43 Cal.4th 737, 751 [and cases cited therein].) This duty could not be fulfilled if the lack of a motion to quash obviated the need to make a good cause showing.

That said, as a practical matter, if the records appear to be freely provided in response to the subpoena and there is no obvious reason for keeping them from the party who subpoenaed them exist, courts are likely to be (and probably should be) relatively liberal in finding good cause for disclosure.

8. A court assessing whether there exists good cause to enforce a subpoena duces tecum in the face of a motion to quash “must consider and balance” seven factors. (*Ibid*, citing to *City of Alhambra v. Superior Court* (1988) 205 Cal.App.3d 1118.) These factors are as follows:
 - First, “[h]as the defendant carried his burden of showing a “plausible justification” for acquiring documents from a third party [citations omitted] 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”? [Citations omitted.] Or does the subpoena amount to an impermissible “fishing expedition”?” (*Id.* at p. *7.)

KEY POINT: It is important to note that “plausible justification” is not synonymous with “good cause.” “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.***” (*Id.* at p. *7, fn. 6 [and *rejecting* language in earlier decisions suggesting test is either good cause *or* plausible justification], emphasis added by IPG.)

“[E]ach legal claim that a defendant advances to justify acquiring and inspecting sought information must be scrutinized and assessed regarding its validity and strength.” (*Id.* at p. *12.)

A “plausible justification” “must in all cases be ‘so substantiated as to make the seizure constitutionally reasonable.” (*Id.* at p. *13.) However, because even submitting restricted posts and private messages on social media to a judge “constitutes a significant impingement on the social media user’s privacy,” the plausible justification “must be subject to even closer examination in the absence of an apparent relationship between the alleged crime and the sought private communications.” (*Id.* at p. *13 [and indicating that just because it “possible that material in a prior or subsequent social media post may be relevant to something that the defendant would like to rely upon,” this does not equate to a plausible justification for in camera review of the materials], emphasis added by IPG.)

- Second, “[i]s the sought material adequately described and not overly broad?” (*Id.* at p. *8.)
- Third, “[i]s the material ‘reasonably available to the ... entity from which it is sought (and not readily available to the defendant from other sources)’?” (*Ibid.*)

***Editor’s note:** In cases involving social media posts and messages, the information can often be sought directly from the victim or the witness or the defendant. (See *Facebook, Inc. v. Wint* (D.C. 2019) 199 A.3d 625, 631 [“the SCA does not prohibit subpoenas directed at senders or recipients rather than providers. 18 U.S.C.A. §§ 2701-12.”].) See this IPG memo at p. 28 for a discussion of concerns about senders or recipients deleting electronic communications.

- Fourth, “[w]ould production of the requested materials violate a third party’s ‘confidentiality or privacy rights’ or intrude upon ‘any protected governmental interest’?” (*Ibid.*)

***Editor’s note:** It is important to recognize that whether the materials are privileged or are otherwise confidential is both a factor in assessing good cause **and** a primary consideration in whether records should be released **even if** good cause for their release is shown. (See *Touchstone* at p. *14; Hoffstadt, California Criminal Discovery (5th Ed.) at p. 391; this IPG at p. 15.)

“[W]hen 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, . . . 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.” (*Touchstone* at p. *12 citing to *Pacific Lighting Leasing Co. v. Superior Court* (1976) 60 Cal.App.3d 552, 566-567.)

Moreover, when “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.” (*Touchstone* at p. *12.) Extra scrutiny is required when there is not an obvious relationship between the private communications and the alleged crime. (See *Touchstone* at p. *13; cf., *People v. Hammon* (1997) 15 Cal.4th 1117, 1126 [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].)*

***Editor’s note:** This heightened concern for the privacy of social media user’s confidential posts and messages does not mean there can *never* be good cause for their release. For example, in *Touchstone*, the California Supreme Court referenced its earlier decision in *Facebook, Inc. v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245 [hereafter “*Facebook (Hunter) I*”], as an example of a case where “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.” (*Touchstone* at p. *13.) In *Facebook (Hunter) I*, the defendants sought social media communications related to a homicide victim and a key witness for the prosecution where there was significant evidence that the underlying shooting and resulting homicide may have related to, and stemmed from, social media posts. The information about the homicide victim “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 (2) “locate exculpatory evidence’ (and attempt to establish a form of self-defense, or imperfect self-defense), in light of [the victim’s] public posts showing that he was a violent person who had previously threatened the defendants and others on social media.” (*Touchstone* at p. *13, fn. 11 citing to *Facebook (Hunter) I* at pp. 1256, 1257.) The information about the witness was “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.” (*Touchstone* at p. *13, fn. 11 citing to *Facebook (Hunter) I* at p. 1257.) In addition, the witness had been implicated by others “as the driver of the car used by defendants when the shooting occurred.” (*Touchstone* at p. *13, fn. 11 citing to *Facebook (Hunter) I* at p. 1253, fn. 4.) The California Supreme Court believed these facts “gave the defense a more specific basis for seeking the communications of the victim and witness, beyond identifying general character impeachment evidence.” (*Touchstone* at p. *13 fn. 11.) And noted that “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.” (*Ibid.*) However, in neither the *Touchstone* nor the *Facebook (Hunter)* decision did the California Supreme Court *actually* decide whether good cause had been shown in the *Facebook (Hunter)* case. (*Touchstone* at p. *18; *Facebook (Hunter) I* at pp. 1290-1291.)

In assessing whether there is a need to disclose non-public content from social media, trial courts must review the publicly available information that has been provided (e.g., *non-private* posts and messages) in order to determine how substantial is the need for the private content. (See *Touchstone* at p. *13, fn. 12 [quoting the appellate court holding in *Facebook v. Superior Court (Hunter)* (2020) 46 Cal.App.5th 109 (review granted June 10, 2020, S260846 [hereafter “*Facebook (Hunter) II*”]).)*

***Editor’s note:** In *Facebook (Hunter) II*, a defendant charged with murder served a subpoena duces tecum on several social media providers (e.g., Facebook, Inc., Instagram, LLC, and Twitter, Inc.) seeking public and private communications from the murder victim’s and a prosecution witness’s accounts. (*Id.* at p. 112.) The appellate court held the trial court (which had denied the social media provider’s motion to quash) should have quashed the subpoena because the record did not support the requisite finding of good cause for production of the private communications for in camera review. (*Ibid.*) Although the appellate opinion in *Facebook Hunter II* has been taken up for review by the California Supreme Court, the California Supreme Court in *Touchstone* telegraphed how it was likely to decide that case as it repeatedly and lovingly cited to the *Facebook (Hunter) II* opinion throughout its discussion. (*Touchstone* at pp. *6-*9, *15.)

- Fifth, “[i]s defendant’s request timely? [Citations omitted.] Or, alternatively, is the request premature? (*Touchstone* at p. *9.)

***Editor’s note:** This factor implicates the continuing validity of *People v. Hammon* (1997) 15 Cal.4th 1117, 1128, a California Supreme Court case upholding the refusal of a trial court to review or disclose *pretrial* discovery of statutorily privileged psychotherapy information subpoenaed by the defense - notwithstanding objections that the trial court’s refusal would violate defendant’s federal Fifth Amendment due process rights and his Sixth Amendment rights of confrontation, cross-examination, and counsel. (See *Touchstone* at p. *2.) The issue of the continuing validity of *Hammon* (insofar as it allowed trial courts to decline to review privileged information in general at the pretrial stage) was raised but not reached in *Facebook, Inc. v. Superior Court (Hunter I)* (2018) 4 Cal.5th 1245 at p. 1261. (*Touchstone* at p. *2.) And it was not addressed by the appellate court in the follow-up case to *Hunter I*. (See *Facebook, Inc. v. Superior Court (Hunter II)* 46 Cal.App.5th 109, 117.) As of now, *Hammon* remains binding precedent. (See *People v. Caro* (2019) 7 Cal.5th 463, 501 [declining to reconsider *Hammon* in the context of the case before it but recognizing that “the advent of digitized, voluminous records may conceivably raise new and challenging issues” when it comes to pretrial discovery in general].)

However, it is important to recognize that just because *Hammon* held there is no constitutional *right* to pre-trial review and discovery of privileged information, this does not mean a trial court is *prohibited* from reviewing or granting disclosure of privileged material pre-trial. It just means that “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.” (See *Touchstone* at p. *13, cf^g *Hammon* at p. 1127.)

- Sixth, “[w]ould the “time required to produce the requested information ... necessitate an unreasonable delay of defendant’s trial”?” (*Id.* at p. *9.)
- Seventh, “[w]ould ‘production of the records containing the requested information ... place an unreasonable burden on the [third party]’?” (*Ibid.*)

9. As illustrated in *Hill v. Superior Court* (1974) 10 Cal.3d 812, all these factors must be balanced. (*Id.* at p. 11, fn. 9.) Thus, in *Hill*, the court upheld the disclosure of any “public records of felony convictions that might exist regarding the prosecution’s prospective key witness against him — in order to impeach that witness.” (*Touchstone* at pp. 10, 11.) But the *Hill* court also upheld the *nondisclosure* of any general arrest and detention records of the prosecution’s prospective key witness (which were sought under the speculative theory that the witness who reported the crime was the actual burglar) because of their minimal value. (*Id.* at pp. 10, 11, fn. 9.)*

***Editor’s note:** The *Hill* court reasoned that even if the arrest and detention records might conceivably 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” and even assuming “such evidence would be admissible as tending to show that [the prospective witness] committed the instant offense” by showing he had a motive to lie, “[i]n 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,” the request for these records was properly denied. (*Hill* at pp. 822-823; see also *Touchstone* at p. 11, fn. 9.)

10. If the *subpoena seeks information implicating privileged or confidential information* of a crime victim, “the California Constitution, as amended to incorporate Marsy’s Law, calls for yet *additional* special inquiry.” (*Touchstone* at p. *14 citing to Cal. Const., art. I, § 28, subds. (b)(4), (b)(5), (c), emphasis added by IPG.) A victim has a “right to prevent disclosure of matters ‘otherwise privileged or confidential by law’ (. . . subd. (b)(4)) and to refuse a discovery request by a defendant (. . . subd. (b)(5)). Moreover, subdivision (c)(1) of section 28 allows the prosecution to enforce a victim’s rights under subdivision (b).” (*Touchstone* at p. *14.) These constitutional 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.’ (Citation omitted).” (*Touchstone* at p. *14.) Accordingly, when a victim’s constitutional privacy rights are implicated “it would be appropriate [for a court] to inquire whether such notice has been, or should be, provided.” (*Ibid.*) Moreover, where the holder of the records has preserved the sought after information “(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.” (*Touchstone* at p. *14, fn. 13.)*

***Editor’s note:** It is important to recognize that when the subpoena seeks materials that are privileged or are otherwise confidential, the court must engage in a balancing test **even if** good cause for their release is shown. As discussed by Justice Hoffstadt in California Criminal Discovery (5th Ed.) at p. 391: “If the third party, opposing party or court asserts that the subpoenaed documents may be privileged, then the court must take an *additional step*: *Not only must the court find “good cause” for the disclosure, the court must also assess* (1) whether the documents are privileged; and (2) if so, whether the subpoenaing party has any interest that *overrides any applicable privileges*. (*Id.* at p. 391, citing to *People v. Superior Court (Humberto S.)* (2008) 43 Cal.4th 737, 751 [and cases cited therein], emphasis added by IPG.)

When *privileged* or otherwise confidential information may *potentially* constitute favorable material evidence under *Brady*, the decision of the United States Supreme Court governing a trial court’s obligations is *Pennsylvania v. Ritchie* (1987) 480 U.S. 39. In *Ritchie*, the High Court “considered the circumstances under which the due process clause of the Fourteenth Amendment entitled the defendant in a child molestation case to obtain pretrial discovery of the files of Pennsylvania’s children and youth services agency to determine whether they would assist in his defense at trial. The statutory scheme evidently authorized the agency to investigate cases in which the child abuse had been reported to the police; information compiled during the agency’s investigation was made confidential, subject to numerous exceptions, including court-ordered disclosure.” (*People v. Hammon* (1997) 15 Cal.4th 1117, 1124-1125 citing to *Ritchie*.) The *Ritchie* court did not decide whether the records should have been released but remanded the case to the trial court for it to determine “whether the CYS file contains information that may have changed the outcome of his trial had it been disclosed.” (*Id.* at p. 61; *Rubio v. Superior Court* (1988) 202 Cal.App.3d 1343, 1350 [remanding case for trial court to decide whether defendant’s right to due process outweighed the state and federal constitutional rights of privacy and statutory privilege not to disclose confidential marital communications of the victim’s parent in a videotape subpoenaed by the defense].) This balancing test should be applied even when the records are subpoenaed during trial. (See e.g., *Hammon* at p. 1127 [leaving open the possibility that when a defendant proposes to impeach a critical prosecution witness at trial “with questions that call for privileged information, the trial court may be called upon . . . to balance the defendant’s need for cross-examination and the state policies the privilege is intended to serve.”].)

Ordinarily, if the information sought constitutes favorable material for the defense (i.e., *Brady* evidence), the privilege or state constitutional right of privacy must give way. (See e.g., *J.E. v. Superior Court* (2014) 223 Cal.App.4th 1329, 1335 [citing to *Ritchie* for the proposition that “[d]isclosure may be required even when the evidence is subject to a state privacy privilege, as is the case with confidential juvenile records.”].) However, when a privilege is absolute, even a defendant’s federal due process rights may not trump it. (See *People v. Bell* (2019) 7 Cal.5th 70, 96 [“a criminal defendant’s right to due process does not entitle him to invade the attorney-client privilege of another.”]; *People v. Gurule* (2002) 28 Cal.4th 557, 594 [same].)

Problems Raised by Proceeding Ex Parte and Under Seal — and Related “Best Practices” Considerations*

*Editor’s note: This sub-title is taken directly from the opinion itself at p. *15.

11. “[P]roceeding ex parte is “generally disfavored” [citation omitted] because doing so may lead judges, uninformed by adversarial input, to incorrectly deny a motion to quash and grant access to pretrial discovery.” (*Ibid.*) Among the “inherent deficiencies” in 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.’”” (*Id.* at p. *15.)*

*Editor’s note: Should there be any doubt about the California Supreme Court’s distaste for ex parte sealed proffers by the defense, it should be noted that the court expressly used the *Touchstone* opinion to, inter alia, “**reiterate** [its] 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.” (*Id.* at p. *2, emphasis added by IPG.)

12. Penal Code section 1326 does permit “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. (*Id.* at p. *15 citing to *Kling v. Superior Court* (2010) 50 Cal.4th 1068, 1075.) But trial courts should not allow “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.”” (*Touchstone* at p. *15, emphasis added.) And the decision as to whether to allow defendant to proceed ex parte and by way of sealed documents must take into consideration the People’s “right to due process and a meaningful opportunity to effectively challenge the discovery request.” (*Id.* at pp. *15 citing to *Kling v. Superior Court* (2010) 50 Cal.4th 1068, 1079.)
13. Accordingly, 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.” (*Ibid.*) And “[a] trial court has discretion to balance these ‘competing interests’ in determining how open proceedings concerning the subpoena should be.” (*Ibid.*)

However, if “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.*** (*Id.* at p. *16, emphasis added by IPG.)

14. Although a trial court is not required to issue a written decision concerning its ruling (and regardless of whether proceedings are ex parte), “a trial court ruling on a motion to quash — especially one that . . . 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.” (*Id.* at p. *16.) “[A] trial court should, at a minimum, articulate orally, and have memorialized in the reporter’s transcript, its consideration of the [seven factors that courts must balance when ruling on a motion to quash].” (*Ibid.*)

How the Trial Court (Understandably) Messed Up and How It Should Handle Its Business on Remand*

***Editor’s note:** This sub-title is *not* taken directly from the opinion itself.

15. After noting that “[n]either the reporter’s transcript of the hearing, nor the resulting minute order, reflect[ed] that the [trial] court expressly considered and balanced the most relevant *Alhambra* factors” (*Touchstone* at p. *14), the California Supreme Court provided *specific* guidance to the trial court as to how it should best decide whether to quash the subpoena on remand in light of the factors discussed *in the instant case*. (See *Touchstone* at pp. *2, *14-*17.)
16. The California Supreme Court strongly suggested the trial court should not have been so quick to give credence to defense counsel’s assertion of the need for the information considering how significantly the preliminary hearing transcript and exhibits from the superior court “paint[ed] a picture *different from* the facts set forth by defendant in his petition for review and related prior (and subsequent) briefs.” (*Id.* at p. *3.)

The California Supreme Court pointed to three separate factual representations made by defense counsel and stated, “defendant’s characterization of the facts in his presentation to the lower courts and this court appears inconsistent with the evidence submitted at the preliminary hearing.” (*Id.* at p. *4; see also this IPG [and compare the facts as stated on page 1 with the “plausible justification” asserted by defense counsel as recounted on page 3].)

The facts as elicited at the preliminary hearing and exhibits from superior court, specifically called 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.” (*Id.* at p. *4.)

17. The California Supreme Court also pointed out that the trial court (i) made “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”; (ii) failed to “explicitly address the potential overbreadth of the subpoena”; (iii) did not “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” (while agreeing “Renteria would not be a reliable source for handing over the communications); and (iv) did not assess nor balance “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.” (*Id.* at p. *14.)

The California Supreme Court emphasized that while the factors of “plausible justification, and confidentiality or constitutional interests that a person in Renteria’s position might have” deserve “special attention in the present circumstances,” all “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.” (*Touchstone* at pp. *14-*15.)

18. The California Supreme Court advised that “[I]n 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.” (*Touchstone*, at p. *12, emphasis added by IPG.)

***Editor’s note:** Typically, courts deciding good cause for disclosure of subpoenaed records do not consider evidence aside from the declarations of counsel alleging the need for the records. However, as DDA Karl Husoe (the prosecutor who argued the case of *Touchstone* in the California Supreme Court) has astutely pointed out, the California Supreme Court’s direction to consider the preliminary examination transcript in assessing good cause suggests that trial courts should be engaging in a more comprehensive review that entails looking at additional evidence – even evidence not provided by the parties – in assessing whether good cause has been shown.

“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.” (*Touchstone* at p. *12.) “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.” (*Ibid.*)

19. The California Supreme Court also seriously questioned whether the trial court should have allowed defense counsel “to proceed ex parte and to file under seal the key declaration and exhibits opposing the motion to quash” as this prevented both the district attorney and Facebook from learning “what public posts defendant relied upon” and being in a position to address “whether those posts support a finding of good cause for the underlying subpoena.” (*Id.* at p. *15; [and indicating, at p. *16, that the trial court overlooked important input from the district attorney and Facebook by allowing defendant to proceed ex parte and under seal].)

It cautioned that because the subpoena sought “restricted social media posts and private messages, in the absence of an apparent relationship between the underlying crime and such communications” that the trial court “should examine *even more closely* the proffered showing of plausible justification in support of such a privacy intrusion.” (*Touchstone*, at p. *12, emphasis added.) And that if the defense were allowed to proceed ex parte and under seal, the trial court must take on “a heightened obligation to undertake critical and objective inquiry, keeping in mind the interests of others not privy to the sealed materials” and make a record allowing for appellate review. (*Id.* at p. *16.)

What the California Supreme Court Said About the Other Issues Raised But Not Decided

20. As noted above, the California Supreme Court declined to address many significant substantive legal issues raised in the case. However, it did *discuss* a claim made by Facebook (and contested by both the district attorney and the defendant) that the court’s earlier decision in *Facebook v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245 resolved the question of whether Facebook is covered and bound by the federal SCA. (*Touchstone* at p. *17.)

Under the federal SCA, entities that provide “electronic communication service” (ECS) or remote computing service” (RCS) are, subject to certain exceptions, barred from divulging to others the contents of their users’ communications. (See *Touchstone* at p. *17, fn. 17; 18 U.S.C. § 2702(a)(1) [barring disclosure by an entity that provides ECS of any communication “in electronic storage by that service”]; § 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].)

The district attorney and the defendant in *Touchstone* argued 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 Facebook from qualifying as either a provider of ECS or of RCS under the provisions of the federal SCA. Thus, Facebook can and must comply with a lawful state-issued subpoena. (*Ibid.*)

The California Supreme Court declined to decide whether or not Facebook qualified as a provider of ECS or RCS. However, they rejected the claim of Facebook that they had already determined that “Facebook is a provider of either ECS or RCS under the Act.” (*Touchstone* at p. *18.) Rather, in *Hunter*, the California Supreme Court simply “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.” (*Touchstone* at p. *18.) Moreover, they noted the theory that Facebook’s business model placed them outside the federal SCA was not considered in *Hunter*. (*Touchstone* at p. *18.)

***Editor’s note:** Facebook asserted 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.) But the California Supreme Court pointed out that no court, including, *Facebook (Hunter) II* (see this IPG at pp. 12-13), “has considered the issue in light of the business model theory.” (*Touchstone* at p. *18, fn. 18.)

The Concurring Opinions of Chief Justice Cantil-Sakauye and Justice Cuéllar

21. Although, as noted above, the California Supreme Court did not decide the issue of whether Facebook is prohibited from complying with the subpoena because of the federal SCA or is permitted to do so because it does not qualify as either an ECS or RCS provider. However, two justices urged courts to “explore” this theory in greater depth because they believed it deserved additional and focused attention in the instant case on remand as well as in other similar future litigation. (Concurring opinions of J. Cantil Sakauye at pp. *18-26 and J. Cuéllar at p. *27.)*

***Editor’s note:** The issue is discussed in this IPG, below, at pp. 23-28.

Questions an Inquisitive Prosecutor Might Have After Reading *Facebook v. Superior Court (Touchstone)*

1. Will the rules governing subpoenas for third party records apply equally to subpoenas for social media records requested by the government?

The specific reason the California Supreme Court in *Touchstone* granted review was “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.” (*Id.* at p. *1, emphasis added by IPG.) And some of the factors laid out in *Touchstone* would only be pertinent when the information is requested by the defense. However, most of the factors laid out in *Touchstone* are pertinent *regardless* of whether the records are subpoenaed by the prosecution or the defense. (See *Kling v. Superior Court* (2010) 50 Cal.4th 1068, 1075 [with exception of subdivision (c), the provisions of Penal Code section 1326 “concerning third party subpoenas apply equally to the People and the defense” and this includes the requirement of a “good cause showing of the need therefor”].)

However, in most cases, if the *prosecution* seeks information from social media providers such as private messages, texts, or posts, it will have to comply with the California Electronic Communications Privacy Act of 2015 (Pen. Code, § 1546 et seq.) which “generally requires a warrant or comparable instrument to acquire such a communication (*id.*, § 1546.1, subd. (b)(1)–(5)), and . . . precludes use of a subpoena ‘or 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].)” (*Touchstone* at p. *26, fn. 13 (conc. opn. of Cantil-Sakauye, J.)). Thus, as pointed out by Justice Cantil-Sakauye, it is not likely that law enforcement actors will be able to compel entities to disclose users’ communications of the kind sought in *Touchstone* with “a mere subpoena.” (*Id.* at p. *26.)

2. If a trial court is not inclined to delay reviewing third party records (especially those potentially implicating privileged or otherwise confidential records) of victims or prosecution witnesses until trial, should prosecutors consider asking the court to, at least, delay disclosure until additional information that might bear on whether good cause can be shown is elicited at the preliminary examination?

As noted in this IPG at p. 14, the holding in *People v. Hammon* (1997) 15 Cal.4th 1117 that “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” (*Touchstone* at p. *13) remains good law. However, a trial court still has discretion to consider pre-trial review and potential disclosure even when the information is privileged or confidential. If a trial court is thinking about pre-trial review and disclosure, DDA Husoe recommends that prosecutors consider asking the court to delay review and disclosure until after the preliminary examination – at least in those circumstances where the testimony of a witness or victim at the preliminary examination might potentially eliminate or diminish the need for accessing confidential or private records of the witness or victim. Support for taking this approach can be found throughout the *Touchstone* opinion, which repeatedly highlighted ways in which the assessment of good cause would have been enhanced by consideration of the preliminary hearing transcript. (*Id.* at pp. *3-*4, *10, *12.) Failing that - and *especially* if defense has filed a sealed affidavit and/or the records sought would implicate privileges or the state constitutional right of privacy - prosecutors should consider providing trial courts with as much information (e.g., police reports, witness statements, etc.,) as possible so that the court can better assess whether the defense has shown good cause for release of the records in advance of trial.

Presumably, prosecutors will only be seeking to oppose the release of the records for a good reason. Otherwise, the opposition may be counterproductive. The information sought by the defense may help show the defendant is, in fact, innocent or help inform plea negotiations if it is disclosed. At a minimum, early release of the information may avoid later delays at trial. True, Penal Code section 1326(c) permits the defense to keep the information obtained pursuant to the subpoena hidden unless disclosure is required by Penal Code section 1054.3. But nothing stops a defense counsel acting in good faith from agreeing to share whatever information is disclosed (perhaps in exchange for a promise from the prosecution to refrain from filing a motion to quash or otherwise opposing release of the subpoenaed records). And if the documents are

released to a defense attorney who chooses to keep the records hidden, the prosecution can also attempt to seek access to those records based on the information that must be provided to the prosecution, notwithstanding Penal Code section 1326(c).*

***Editor’s note:** As discussed by Justice Hoffstadt in California Criminal Discovery, the court handling the subpoena request or the party in a criminal case that has subpoenaed third party records “must at some point prior the hearing notify the opposing party of (1) the identity of the subpoenaed third party; (2) the nature of the documents subpoenaed; (3) the identity of the person to whom the subpoenaed records pertain; and the (4) the date and time of the subpoena’s return.” (*Id.* at p. 389; see also p. 387 [citing cases].)

3. Should prosecutors argue that the prohibitions imposed by the federal SCA on disclosure of information kept by entities that provide “electronic communication service” (ECS) or remote computing service” (RCS) do not apply to Facebook or similar entities?

As noted above, when defense counsel seeks social media records of a witness (or victim) in a criminal case from an entity like Facebook, it may be expected that Facebook will assert that it cannot release the records without running afoul of the federal Stored Communications Act (SCA) - even if “good cause” for the records has been established. Assuming the defense can otherwise show entitlement to the records, if Facebook is correct and the *only* means by which the defense can obtain that information is through use of a subpoena, then several other issues will necessarily arise – especially if the defense can also show the records contain material favorable evidence. (See this IPG at pp. 5-7.) And, depending on the circumstances, it is not clear, how those issues are likely to be resolved – creating potential risks to convictions even if the trial court agrees the defense is not entitled to the records.

***Editor’s note:** Many of these issues are discussed at length in one or more of the 32(!) briefs filed in the *Touchstone* case – all of which are accessible at <https://www.courts.ca.gov/44048.htm>

On the other hand, if the SCA does *not* apply to Facebook or similar entities because their business model disqualifies them as either an ECS or an RCS provider, then most, if not all, the other issues disappear. Moreover, the argument that Facebook or similar entities are not subject to the SCA prohibition on disclosure of the records rests on pretty solid reasoning.*

***Editor’s note:** That reasoning was developed by DDA Husoe, whose excellent brief arguing that the SCA does not apply to the types of communications sought in *Touchstone* may be freely accessed at: <https://www.courts.ca.gov/documents/15-s245203-san-diego-county-dist-atty-brief-072618.pdf>

And if the records are disclosed because a trial court agrees the SCA does not apply, then convictions are not placed at risk on appeal. Accordingly, *if* the trial court has properly considered all the factors discussed in *Touchstone* and disclosure of the information is not otherwise improper, it is respectfully recommended that prosecutors take the position that the SCA does not bar disclosure of the information.

We summarize the arguments (as elucidated in the concurring opinions of Justice Cantil-Sakauye) in favor of finding the SCA does not bar Facebook (and comparable entities) from disclosing electronic communications – as well as how to reply to the counter-arguments below.

Argument for Why the SCA Does Not Bar Facebook from Disclosing Electronic Communications

“[T]he SCA covers, and prohibits disclosure of, stored and/or electronic communications by only two specific types of entities – (1) those that provide ‘electronic communication service’ (ECS), and/or (2) those that provide ‘remote computing service’ (RCS). (§ 2702(a).)” (*Touchstone*, conc. opn of J. Cantil Sakauye at p. *20.)

“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.” (*Ibid.*)

Section 2702 of the federal Stored Communications Act, in pertinent part, provides:

“(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in *electronic storage* by that service; and

(2) a person *or 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 ¶ (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) *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; . . .*” (Emphasis added by IPG.)

***Editor’s note:** “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.” (*Touchstone*, conc. opn of J. Cantil Sakauye at p. *20.)

Remote computing service (RCS), “is defined as ‘the provision to the public of computer storage or processing services by means of an electronic communications system.’ (§ 2711(2).)” (*Id.* at p. *21.)

Section 2702(a)(2)(B) “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.” (*Id.* at p. *21.)

It follows “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.” (*Ibid.*)

Under the terms and conditions a subscriber agrees to when signing up for a Facebook account, the subscriber authorizes Facebook to access the contents of the communication for purposes of storing, copying, and sharing the content with others, including businesses and organizations that pay Facebook to promote and show ads targeted to the user. (See Facebook, Terms of Service <www.facebook.com/legal/terms/plain_text_terms> (revised July 31, 2019) [as of August 10, 2020] and Facebook, Data Policy <www.facebook.com/full_data_use_policy> (revised Apr. 19, 2018) [as of August 10, 2020]; *Touchstone*, conc. opn of J. Cantil Sakauye at p. *18, fns. 2 and 3.) That is, the subscriber authorizes access the contents of their communications for purposes of providing services other than storage or computer processing. Thus, the SCA’s bar on disclosure of those communications is inapplicable. And a state court may order disclosure of the “contents” of the communications without running afoul of the SCA.*

***Editor’s note:** “[W]ith 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.” (*Touchstone*, conc. opn of J. Cantil Sakauye at p. *22.)

Argument for Why the SCA Does Bar It from Disclosing Electronic Communications

Facebook has argued “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.” (*Touchstone*, conc. opn of J. Cantil Sakauye at p. *2t.)

Moreover, Facebook has argued that even if it has authority to access electronic communications for purposes other than storage or computer processing such that subdivision (a)(2) of section 2702 does not bar disclosure, it still 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).” (*Touchstone*, conc. opn of J. Cantil Sakauye at p. *23.) Accordingly, whether it “has authority to access [a] communication in connection with the service is ... irrelevant to whether [the communication] is in electronic storage.” (*Ibid.*)

Facebook has relied on previous cases finding it qualified as an ECS or RCS under the SCA and has argued 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.” (*Id.* at p. *25.)

Counter Argument to Why the SCA Bars Facebook from Disclosing Electronic Communications

The fact that Facebook provides some form of 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)) does not mean it falls within Congress’s understanding of an entity that provides ECS. “[B]ecause (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,

“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.” (*Id.* at p. *23.)

Moreover, “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.*” (*Id.* at p. *23.) Consistent with this understanding, when an entity like Facebook “retains a communication beyond the initial sending and provisional backup stage, then once that message has been opened/accessed, *the entity no longer acts as a provider of ECS but rather transforms into a provider of RCS.* (*Id.* at p. *24.)

In addition, the legislative history and case law interpreting the SCA suggest that— that the term “computer processing services” was “intended to have a narrow, rather than broad, interpretation.” (*Id.* at p. *25.)

As to the policy arguments - while a holding that entities like Facebook are not generally barred from voluntarily disclosing their users’ communications, including restricted posts and private messages, might cause market disruption is a theoretical possibility, “for practical marketplace reasons, it may be doubted that such a holding would likely lead to such disruptions or voluntary disclosures because an entity that became known for disclosing its users’ communications on its own, without legal compulsion (i.e., a subpoena) “would not long survive in the market — and hence would refrain from doing so in the first place.” (*Id.* at p. * 26.) Settled expectations of users would not be significantly undermined considering that law enforcement would not, in almost all cases, be able to access the information without a warrant. And it does not “seem that a narrower construction of the phrase would leave Facebook and similar entities unable to protect against malware” since there exist reasons to protect against malware regardless of whether the federal SCA applies. (*Id.* at p. *26 and fn. 14.)

The argument that if “computer processing” is given a narrow construction, then entities like Facebook will not engage in “monitoring and resulting measures to counteract malware” because doing so would open the door to the communications being viewed as outside the scope of the SCA’s bar on release of those communications is dubious. This is because taking those monitoring and resulting measures would not necessarily fall outside 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.” (*Ibid.*)

“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.” (*Ibid.*)

4. Regardless of whether the SCA’s prohibition against release of information applies to Facebook, can a simple request to *preserve* data be made to an *entity such as Facebook* in conjunction with a subpoena to the sender or recipient of an electronic communication?

Per DDA Husoe, one of the reasons provided by the defendant in *Touchstone* for why requiring the defense to pursue other available avenues to obtain the information (i.e., by subpoenaing the subscriber directly) was not feasible was because such a subpoena would put the subscriber on notice that the records are being sought, giving the subscriber an opportunity to destroy the records. However, DDA Husoe points out, that in footnote 13 of the opinion, the California Supreme Court implicitly recognized that notification to a victim whose records were sought could be done *after* the entity storing the victim’s communications had been subject to an order for preservation, “presumably addressing concerns about possible spoliation by a social media user.” (*Touchstone*, at p. *14, fn. 13.) This suggests that an order for preservation could be served on the service provider regardless of whether a subpoena on the provider would be proper. Moreover, there is no reason to believe that a preservation order to the subscriber could not be issued when seeking records from the subscriber him or herself. A preservation order would potentially avoid some of the issues involving the scope of the federal SCA while also addressing the concern that the victim or witness will delete the communications upon receiving the subpoena.

SPECIAL THANKS: TO SAN DIEGO DEPUTY DISTRICT ATTORNEY KARL HUSOE WHOSE INSIGHTS SIGNIFICANTLY IMPROVED THE CONTENT OF THIS IPG.

NEXT EDITION - ONE OF THE FOLLOWING: A REVIEW OF THE LATEST DEVELOPMENTS IN SEARCH AND SEIZURE; AN OVERVIEW OF ALL THE ISSUES CROPPING UP IN APPLYING THE FELONY MURDER RULE, THE NATURAL AND PROBABLE CONSEQUENCES DOCTRINE, AND PENAL CODE SECTION 1170.95; OR A PRINT ONLY EDITION ON PROTECTING CONFIDENTIAL INFORMATION AND INFORMANTS;

Suggestions for future topics to be covered by the Inquisitive Prosecutor’s Guide, as well as any other comments or criticisms, should be directed to Jeff Rubin at (408) 792-1065. 🐕