# 1061. UNLAWFUL ACCESS TO STORED COMMUNICATIONS—18 U.S.C. § 2701

The 1986 Act added new statutory provisions, 18 U.S.C. §§ 2701 to 2710, to protect the privacy of stored electronic communications, either before such a communication is transmitted to the recipient, or, if a copy of the message is kept, after it is delivered. These provisions focus on technologies such as electronic mail and computer transmissions, where copies of the messages are kept. Electronic storage is defined in 18 U.S.C. § 2510(17) as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Section 2701 of Title 18 makes it an offense to either (a) intentionally access, without authorization, a facility through which an electronic communication service is provided; or (b) intentionally exceed the authorization of such facility; and as a result of this conduct, obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system. 18 U.S.C. § 2701(a). This section covers "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, U.S.C. § 2701, as well as "voice mail" service.

This provision is intended to address "computer hackers" and corporate spies. The provision is not intended to criminalize access to "electronic bulletin boards," which are generally open to the public. A communication will be found to be readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. To access a communication on such a system is not a violation of the law. 18 U.S.C. § 2701(a).

If a violation of 18 U.S.C. § 2701(a) was committed for commercial advantage, malicious destruction or damage, or private financial gain, the violator could receive up to a year in prison and a fine as provided by Title 18, United States Code, for the first offense and up to two years imprisonment and a fine as provided by Title 18 for a second or subsequent offense. In all other cases, a jail term of up to six months and a fine under Title 18 could be imposed. 18 U.S.C. § 2701(b)(2).

[cited in JM 9-60.200]

‹ 1060. Scope of 18 U.S.C § 2512 Prohibitions | up | 1062. Unauthorized Installation or Use of Pen Registers and Trap and Trace Devices—18 U.S.C. § 3121 ›

*Updated January 21, 2020*

Up^ << Prev ous Next >> cross-reference chaptered bills PDF | Add To My Favorites

Search Phrase: Highlight

**EVIDENCE CODE - EVID**

**DIVISION 11. WRITINGS [1400 - 1605]** *( Division 11 enacted by Stats. 1965, Ch. 299. )*

**CHAPTER 1. Authentication and Proof of Writings [1400 - 1454]** *( Chapter 1 enacted by Stats. 1965, Ch. 299. )*

**ARTICLE 1. Requirement of Authentication [1400 - 1402]** *( Article 1 enacted by Stats. 1965, Ch. 299. )*

**1400.** Authentication of a writing means (a) the introduction of evidence sufficient to sustain a finding that it is the writing that the proponent of the evidence claims it is or (b) the establishment of such facts by any other means provided by law.

*(Enacted by Stats. 1965, Ch. 299.)*

**EVIDENCE CODE - EVID**

**DIVISION 11. WRITINGS [1400 - 1605]** *( Division 11 enacted by Stats. 1965, Ch. 299. )*

**CHAPTER 1. Authentication and Proof of Writings [1400 - 1454]** *( Chapter 1 enacted by Stats. 1965, Ch. 299. )*

**ARTICLE 2. Means of Authenticating and Proving Writings [1410 - 1421]** *( Article 2 enacted by Stats. 1965, Ch. 299. )*

**1410.** Nothing in this article shall be construed to limit the means by which a writing may be authenticated or proved.

*(Enacted by Stats. 1965, Ch. 299.)*

Up^ << Prev ous Next >> cross-reference chaptered bills PDF | Add To My Favorites

Search Phrase: Highlight

**EVIDENCE CODE - EVID**

**DIVISION 11. WRITINGS [1400 - 1605]** *( Division 11 enacted by Stats. 1965, Ch. 299. )*

**CHAPTER 1. Authentication and Proof of Writings [1400 - 1454]** *( Chapter 1 enacted by Stats. 1965, Ch. 299. )*

**ARTICLE 2. Means of Authenticating and Proving Writings [1410 - 1421]** *( Article 2 enacted by Stats. 1965, Ch. 299. )*

**1413.** A writing may be authenticated by anyone who saw the writing made or executed, including a subscribing witness.

*(Enacted by Stats. 1965, Ch. 299.)*

# Facebook, Inc. v. Superior Court (Hunter)

Supreme Court of California

May 24, 2018, Filed

S230051

**Reporter**
4 Cal. 5th 1245 *; 417 P.3d 725 **; 233 Cal. Rptr. 3d 77 ***; 2018 Cal. LEXIS 3635 ****; 2018 WL 2347162

FACEBOOK, INC., et al., Petitioners, v. THE SUPERIOR COURT OF THE CITY AND COUNTY OF SAN FRANCISCO, Respondent; DERRICK D. HUNTER et al., Real Parties in Interest.

**Subsequent History:** Reported at *Facebook, Inc. v. Superior Court, 2018 Cal. LEXIS 4017 (Cal., May 24, 2018)*

Writ granted by *Facebook, Inc. v. Superior Court of San Francisco, 2020 Cal. App. Unpub. LEXIS 1039 (Cal. App. 1st Dist., Feb. 13, 2020)*

**Prior History:** [****1] Superior Court of San Francisco City and County. Nos. 13035657, 13035658, Bruce E. Chan, Judge. Court of Appeal, First Appellate District, Division Five, No. A144315.

*Facebook, Inc. v. Superior Court, 240 Cal. App. 4th 203, 192 Cal. Rptr. 3d 443, 2015 Cal. App. LEXIS 786 (Cal. App. 1st Dist., Sept. 8, 2015)*

## Case Summary

### Overview

HOLDINGS: [1]-The Supreme Court concluded that the court of appeal was correct to the extent it found subpoenas that were served on social media providers by criminal defendants unenforceable under the Stored Communications Act, *18 U.S.C. § 2701 et seq.*, with respect to communications addressed to specific persons, and other communications that were and have remained configured by the registered user to be restricted; [2]-However, the court of appeal's determination was erroneous to the extent it held that *18 U.S.C. § 2702* also bars disclosure by providers of communications that were configured by the registered user to be public, and that remained so configured at the time the subpoenas were issued; [3]-Under the Act's lawful consent exception, a provider must disclose any such communication pursuant to a subpoena that is authorized under state law.

### Outcome

Decision of court of appeal vacated; that court directed to remand matter to trial court.

**Counsel:** [*1248] Perkins Coie, Christian Lee, James G. Snell, Eric D. Miller, John R. Tyler, Sunita Bali; Gibson, Dunn & Crutcher, Joshua S. Lipshutz and Michael J. Holecek for Petitioners.

Mayer Brown and Donald M. Falk for Google LLC as Amicus Curiae on behalf of Petitioners.

No appearance for Respondent.

Jose Pericles Umali for Real Party in Interest Derrick D. Hunter.

Susan B. Kaplan and Janelle E. Caywood for Real Party in Interest Lee Sullivan.

Jeff Adachi, Public Defender (San Francisco), Matt Gonzalez, Chief Attorney, and Dorothy Bischoff, Deputy Public Defender, as Amici Curiae on behalf of Respondent and Real Parties in Interest.

Stephen P. Lipson, Public Defender (Ventura) and Michael C. McMahon, Chief Deputy Public Defender, for California Public Defenders Association and Public Defender of Ventura County as Amici Curiae on behalf of Real Parties in Interest.

David M. Porter; Law Offices of Donald E. Landis, Jr., Donald E. Landis, Jr.; Law Offices of J.T. Philipsborn and John T. Philipsborn for California Attorneys for Criminal Justice [****2] and National Association of Criminal Defense Lawyers as Amici Curiae on behalf of Real Parties in Interest.

**Judges:** Opinion by Cantil-Sakauye, C. J., with Chin, Corrigan, Liu, Cuéllar, Kruger, and Yegan, JJ.,* concurring.

**Opinion by:** Cantil-Sakauye

## Opinion

[***79] [**727] **CANTIL-SAKAUYE, C. J.**—

### INTRODUCTION AND OVERVIEW

Real parties in interest Derrick D. Hunter and Lee Sullivan (defendants) were indicted by a grand jury and await trial on murder, weapons, and gang-related charges arising out of a driveby shooting in San Francisco. Each defendant served a subpoena duces tecum on one or more petitioners, social media service providers Facebook, Inc. (Facebook), Instagram, LLC (Instagram), and Twitter, Inc. (Twitter) (collectively, social media providers, [*1249] or simply providers). The subpoenas broadly seek public and private communications, including any deleted posts or messages, from the social media accounts of the homicide victim and a prosecution witness.

As explained below, the federal Stored Communications Act (*18 U.S.C. § 2701 et seq.*; hereafter SCA or Act)[1] regulates the conduct of covered service providers, declaring that as a general matter they may not disclose stored electronic communications except under specified circumstances (including with the consent [****3] of the social media user who posted the communication) or as compelled by law enforcement entities employing procedures such as search warrants or prosecutorial subpoenas. Providers moved to quash defendants' subpoenas, asserting the Act bars providers from disclosing the communications sought by defendants. They focused on *section 2702(a)* of the Act, which states that specified providers "shall not knowingly divulge to any person or entity the contents of" any "communication" that is stored or maintained by that provider. They asserted that *section 2702* prohibits disclosure by social media providers of *any* communication, whether it was configured to be public (that is, with regard to the communications before us, one as to which the social media user placed no restriction regarding who might access it) or private or restricted (that is, configured to be accessible to only authorized recipients). Moreover, they maintained, none of various exceptions to the prohibition on disclosure listed in *section 2702(b)* applies here. And in any event, providers argued, they would face substantial technical difficulties and burdens if forced to attempt to retrieve deleted communications and should not be required to do so.

Defendants implicitly [****4] accepted providers' reading of the Act and their conclusion that [**728] it bars providers from complying with the subpoenas. Nevertheless, defendants asserted that they need all of the requested communications (including any that may have been deleted) in order to properly prepare for trial and defend against the pending murder charges. They argued that the *SCA* violates their constitutional rights under the *Fifth* and *Sixth Amendments to the United States Constitution* to the extent it precludes compliance with the pretrial subpoenas in this case.

The trial court, implicitly accepting the parties'

* Associate Justice of the Court of Appeal, Second Appellate District, Division Six, assigned by the Chief Justice pursuant to *article VI, section 6 of the California Constitution*.

[1] Future undesignated statutory references are to title 18 of the United States Code.

understanding of the SCA, agreed with defendants' constitutional contentions, denied providers' motions to quash, and ordered them to produce the requested communications for the court's review in camera. Providers sought, and the Court of Appeal issued, a stay of the production order. After briefing and argument, the appellate court disagreed with the trial court's constitutional conclusion and issued a writ of mandate, directing the trial court [***80] to quash the subpoenas. We granted review.
[*1250]

Our initial examination of the Act, its history, and cases construing it, raised doubts that section 2702 of the Act draws no distinction between public and restricted communications, [****5] and that no statutory exception to the prohibition on disclosure could plausibly apply here. In particular, we questioned whether the exception set out in section 2702(b)(3), under which a provider may divulge a communication with the "lawful consent" of the originator, might reasonably be interpreted to permit a provider to disclose posted communications that had been configured by the user to be public.

Accordingly, we solicited supplemental briefing concerning the proper interpretation of section 2702. In that briefing, all parties now concede that communications configured by the social media user to be public fall within section 2702(b)(3)'s lawful consent exception to section 2702's prohibition, and, as a result, may be disclosed by a provider. As we will explain, this concession is well taken in light of the relevant statutory language and legislative history.

The parties differ, however, concerning the scope of the statutory lawful consent exception as applied in this setting. Defendants emphasize that even those social media communications configured by the user to be restricted to certain recipients can easily be shared widely by those recipients and become public. Accordingly, they argue that when any restricted communication is sent [****6] to a "large group" of friends or followers, the communication should be *deemed* to be public and hence disclosable by the provider under the Act's lawful consent exception. On this point we reject defendants' broad view and instead agree with providers that restricted communications sent to numerous recipients cannot be deemed to be public—and do not fall within the lawful consent exception. Yet we disagree with providers' assertion that the Act affords them "discretion" to defy an otherwise proper criminal subpoena seeking public communications.

**(1)** In light of these determinations we conclude that the Court of Appeal was correct to the extent it found the subpoenas unenforceable under the Act with respect to communications addressed to specific persons, and other communications that were and have remained configured by the registered user to be restricted. But we conclude the court's determination was erroneous to the extent it held section 2702 also bars disclosure by providers of communications that were configured by the registered user to be public, and that remained so configured at the time the subpoenas were issued. As we construe section 2702(b)(3)'s lawful consent exception, a provider must disclose any such [****7] communication pursuant to a subpoena that is authorized under state law.

Ultimately, whether any given communication sought by the subpoenas in this case falls within the lawful consent exception of section 2702(b)(3), and [*1251] must be disclosed by a provider pursuant to a subpoena, cannot be resolved on this record. Because the parties have not until recently focused on the need to consider the configuration of communications or accounts, along with related issues concerning the reconfiguration or deletion history of the communications at issue, the record before us is incomplete in these respects. Accordingly, resolution of whether any communication sought by the defense subpoenas [**729] falls within the statute's lawful consent exception must await development of an adequate record on remand.

We will direct the Court of Appeal to remand the matter to the trial court to permit the parties to appropriately further develop the record so that the trial court [***81] may reassess the propriety of the subpoenas under the Act in light of this court's legal conclusions.

## I. Facts and Lower Court Proceedings

### A. *Grand Jury Proceedings and Indictment*[2]

According to testimony before the grand jury, at midday on June 24, 2013, Jaquan [****8] Rice, Jr., was killed and his girlfriend, B.K., a minor, was seriously injured in a driveby shooting at a bus stop in the Bayview district

[2] This and the following parts are based on the grand jury transcripts, of which we have taken judicial notice, as well as material in providers' appendix of exhibits—including pretrial moving papers and the transcripts of two sessions of a pretrial hearing.

of San Francisco. Various surveillance videos showed a vehicle and someone firing a handgun from the rear window on the driver's side. A second person was depicted leaving the vehicle from the rear passenger-side door and firing a gun with a large attached magazine.

Witnesses identified defendant Derrick Hunter's 14-year-old brother, Q.H., as one of the shooters. During questioning in the early morning hours after the events, police homicide detectives told Q.H. that they had "pulled all Instagram … [and] Facebook stuff," and were aware that he knew the shooting victim. Q.H. related that the victim had "tagged" him on Instagram in a video featuring guns. The detectives responded that they had been "working all day" on the matter and had "seen those posts." Q.H. admitted that he shot the victim six times—and asserted that the victim "would have done the same thing to us."[3]

Q.H. stated that "Nina," his girlfriend's sister, had provided the car in which he, his brother, and one other male had driven. Within a few minutes [*1252] of the shooting, [****9] police had stopped Nina, whose real name is Renesha Lee (hereafter sometimes Renesha), while driving the vehicle shown in the videos.

Renesha was codefendant Lee Sullivan's then girlfriend. She had rented the car used in the shooting and gave varying accounts of the events. According to her testimony before the grand jury, during the course of multiple interviews on the day and night of the killings, she initially "just made up names and stuff." Eventually she told the police that defendant Derrick Hunter and his younger brother Q.H. were among those who had borrowed her car. Renesha did not mention defendant Sullivan's name until a few days later, when she "told them the truth about [Sullivan]," and that he had been involved along with the Hunter brothers.

Renesha related that on the day of the shooting she had driven with Sullivan and the Hunter brothers to a parking lot where they "got out and walked to [Q.H.'s] house." She explained that Sullivan told her the three young men were going to a store. Renesha recalled that she replied she would remain at the house and talk to her sister. She testified that Sullivan had not been wearing gloves when he and the others initially approached [****10] her to borrow the car, but she noticed that he was wearing gloves when they came out of [***82] Q.H.'s house and when they departed. According to Renesha, Sullivan drove away with Derrick and his Hunter brother Q.H. in the backseat. She testified that when the three returned the car to her shortly thereafter it contained the phones of Sullivan and Derrick Hunter. She also testified that she had never seen Sullivan or either of the brothers with a gun.

[**730] Renesha explained that she had initially not revealed Sullivan's involvement because she had been scared and "just didn't want to have no parts of it because I'm the one that still has to live and walk these streets." She elaborated that once the police informed her that she might be arrested for murder, she "told them the truth," and yet still avoided implicating Sullivan until later in the process because she remained fearful of him. She maintained that after being threatened with prosecution she eventually told the full truth about Sullivan's role.

In presenting the case to the grand jury, the prosecution contended that defendants and Q.H. were members of Big Block, a criminal street gang, and that Rice was killed for two reasons: (1) Rice was a [****11] member of West Mob, a rival gang, and (2) Rice had publicly threatened defendant Derrick Hunter's younger brother Q.H. on social media. Inspector Leonard Broberg, a gang [*1253] expert and member of the San Francisco Police Department gang task force, testified that in his opinion the alleged crimes were committed for the benefit of the Big Block gang. He explained that "gangsters are now in the 21st century, and they've taken on a new aspect of being gangbangers, and they do something they call cyber banging. [¶] They will actually be gangsters on the internet. They will issue challenges; they will show signs of disrespect, whether it's via images or whether it's via the written word. … [¶] [They use] Facebook, … Instagram, Socialcam, Vine … [and] YouTube. … They will disrespect each other in cyberspace." Inspector Broberg described a YouTube video made by victim Rice and shared by him via his Facebook account, in which he gave a tour of his West Point/Middle Point neighborhood and identified specific places where he could be located—including the bus

---

[3] Ultimately Q.H. was tried in juvenile court, found to be responsible for Rice's murder and the attempted murder of B.K., declared a ward of the court, and committed to the Division of Juvenile Justice for a term of 83 years four months to life. Under *Welfare and Institutions Code section 607, subdivision (b)*, however, because of his age at the time of the crimes, he will not be confined beyond his 25th birthday. After the Court of Appeal affirmed in an unpublished opinion (*In re Q.H.* (Sept. 21, 2016, A142771 [nonpub. opn.], review granted Jan. 11, 2017, S238077), we granted review and held that matter pending disposition of the present litigation.

stop where he was shot. Broberg characterized the video as a challenge to others. In a subsequent declaration, Broberg [****12] explained that he "rel[ies] heavily on records from social media providers such as Facebook, Instagram, and Twitter to investigate and prosecute alleged gang members for gang crimes," and that in the present case, he "relied in part on" such records to secure evidence that Rice, Sullivan, and Derick and his brother Q.H. "were members of rival gangs and that the shootings were gang related." The same declaration adds: "We [the police] have not sought search warrants as to Renesha Lee."[4]

Defendants were indicted and are presently charged with the murder of Rice and the attempted murder of B.K. They also face various gang and firearm enhancements. (*Pen. Code, §§ 187*, *664*, *186.22, subd. (b)(1)*, *12022, subd. (a)*, *12022.53, subds. (d) & (e)(1)*.)

B. *Description of the Subpoenas*

Prior to trial, in late 2014, both defendants served subpoenas duces tecum (*Pen. Code, § 1326, subd. (b)*) on Twitter. Defendant Sullivan's subpoena sought "[a]ny [***83] and all public and private content" that had been "published by" Renesha Lee, who was identified by an attached photocopied screenshot of one of her Twitter accounts. The request specified no temporal boundary and stated that it "includes but is not limited to" (1) so-called record data, consisting of "user information [and] associated e-mail addresses," "activity logs," and "location [****13] data"; and (2) content information, such as "photographs, videos, private messages, … posts, status updates, … and comments including information deleted by the account holder." It further sought the identity and contact information concerning the custodian of records who [*1254] could authenticate the requested materials. Defendant Hunter's subpoena, issued a few weeks later, sought all "accounts" and tweets originating from Renesha Lee's "account and in response to or linking her account" from the beginning of 2013 "to the present." Neither defendant sought from Twitter any communication concerning victim Rice.

Only defendant Sullivan served subpoenas on Facebook and Instagram. The Facebook [**731] subpoena requested information regarding the accounts of both Rice and Renesha Lee. The language of the subpoena tracked Sullivan's request to Twitter, broadly seeking "[a]ny and all public and private content," including deleted material, that had been "published by" either Rice or Renesha Lee, each of whom was identified by an attached photocopied screenshot of that person's Facebook account. As with Sullivan's subpoena served on Twitter, the subpoena specified no temporal boundary and sought the [****14] same record data, content, and authentication information mentioned above.

Sullivan's subpoena served on Instagram similarly sought "[a]ny and all public and private content," including deleted material, published by Rice and Renesha Lee, each of whom was again identified by photocopied screenshots showing their account information.[5] In all relevant respects the demands for record, content, and authentication information tracked the demands directed to the other social media providers.

C. *Providers' Responses to the Subpoenas*

Counsel for Facebook and its subsidiary Instagram responded to the Sullivan subpoenas by a single letter in December 2014, asserting that as providers governed by federal statute (the *SCA*), they are precluded under that law from divulging the requested stored communications. The letter stated that under the SCA only the government may compel covered providers to divulge such stored content. Accordingly, the letter recommended that defense counsel instead seek the requested information directly from the account holder or from "any party to the communication"—persons who, unlike a covered provider, are "not bound by the SCA." Alternatively, the letter suggested that [****15] defense

[4] Toward the end of the proceedings, the prosecutor read to the grand jury some "exculpatory evidence … that was requested by the defense attorneys in this case be presented to you." The panel was told that two witnesses reported to police that a young woman had been driving the car, and that one witness had identified the driver as Renesha Lee. Yet another witness identified the driver as Q.H.

[5] It appears from the record that there may have been up to four relevant Instagram accounts, at least one for Renesha Lee and possibly three for Rice. A photocopied screenshot attached as an exhibit to the subpoena pertaining to Renesha Lee indicated the account had four posts, one follower, and eight accounts that the account holder was following. It also shows an image of a padlock, with a notation, "this user is private." According to subsequent pretrial briefing by defendants, "Mr. Rice had multiple social media accounts" and "many … have been deleted, including accounts gang expert Leonard Broberg relied upon at the grand jury hearing." Moreover, according to that same subsequent briefing, defendants also asserted that "many of [Renesha Lee's social media] accounts have been deleted."

counsel might "work[] with the prosecutor to [*1255] obtain" the requested information via an [***84] additional search warrant issued by the government.[6] A few days later, different counsel in the same law firm responded similarly on behalf of Twitter to defendant Sullivan.

Eventually all three providers moved to quash the subpoenas. They reiterated the assertions in their letters that defendants might try to obtain the requested information directly from the social media user who posted the communication, or from any recipient[7]—or perhaps via an additional search warrant issued by the prosecution.[8] They also [**732] objected that the requests as drafted were overbroad and vague. In any event, providers asserted, disclosure *directly from them*, as entities covered by the SCA, was barred by that federal law. In that respect providers' motions relied upon section 2702(a), which broadly states that a covered "person or entity" such as providers [*1256] "shall not knowingly *divulge to any person or entity the contents of a communication while in electronic storage by that service*." (Italics added.) Based on this language, providers asserted that the SCA's prohibition on a provider entity's ability to disclose any content [****16] information applies broadly and does not depend on whether the registered [***85] user configured a given communication as private/restricted as opposed to public. Moreover, providers asserted, none of section 2702(b)'s exceptions to the bar on disclosure by a provider applies here. Nor, they observed, does the Act contemplate procedures for criminal defendants to compel production of such communications.

D. *Defendants' Opposition to the Motions To Quash*

Defendants opposed the motions to quash,[9] but they did not contest providers' assertion that section 2702(a) prohibits providers from disclosing any of the sought communications—even those configured by the registered user to be public. Nor did defendants challenge providers' assertion that none of section 2702(b)'s exceptions apply in this case. Instead, defendants argued that their federal constitutional rights under the Fifth and Sixth Amendments to a fair trial, to present a complete defense, and to cross-examine

---

[6] Finally, the letter explained that if defense counsel were to withdraw each subpoena "to the extent it seeks content," Facebook and Instagram might produce "non-content information" regarding the specified accounts, "such as basic subscriber information and [Internet protocol] logs"—information that defense counsel might use to contact other parties to the communications, in order to attempt to obtain the information directly from them. ("Basic subscriber information" (more fully described *post*, fn. 23) and Internet protocol logs are forms of record/non-content data that, as implied in the letter, might be employed to identify a recipient of a communication in order to attempt to obtain electronic communications directly from that person.)

[7] In this regard, providers relied on decisions such as O'Grady v. Superior Court (2006) 139 Cal.App.4th 1423, 1447 [44 Cal. Rptr. 3d 72] (*O'Grady*) (even when the Act precludes disclosure by a provider, it "does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the [SCA-regulated service provider] bailee" who is barred from disclosure). (See generally Fairfield & Luna, *Digital Innocence* (2014) 99 Cornell L.Rev. 981, 1058 [suggesting that a "defendant could locate the relevant originator or recipient by accessing non-content identifying information, such as an IP address, and then seek production [from that person] directly"].)

[8] Of course defendants are independently entitled to general criminal discovery, including exculpatory evidence, from the prosecution under Penal Code section 1054.1. Moreover, under authority such as Brady v. Maryland (1963) 373 U.S. 83 [10 L. Ed. 2d 215, 83 S. Ct. 1194], People v. Salazar (2005) 35 Cal.4th 1031, 1042–1043 [29 Cal. Rptr. 3d 16, 112 P.3d 14], and cases cited, and Barnett v. Superior Court (2010) 50 Cal.4th 890, 900–901 [114 Cal. Rptr. 3d 576, 237 P.3d 980], the prosecution is obligated to share with the defense *any* material exculpatory evidence in its possession—including that which is potentially exculpatory. (See also Rules Prof. Conduct, rule 5-110(D), as amended Nov. 2, 2017 [requiring "timely disclosure to the defense of all evidence or information known to the prosecutor that the prosecutor knows or reasonably should know tends to negate the guilt of the accused, mitigate the offense, or mitigate the sentence"] and corresponding discussion [observing that "the disclosure obligations in paragraph (D) are not limited to evidence or information that is material as defined by *Brady v. Maryland* … and its progeny. For example, these obligations include, at a minimum, the duty to disclose impeachment evidence or information that a prosecutor knows or reasonably should know casts significant doubt on the accuracy or admissibility of witness testimony on which the prosecution intends to rely"].) As explained below, consistent with its discovery obligations under state and federal law, the prosecution has apparently shared with defendants information relating to victim Rice's social media accounts. (See *post*, fn. 10.)

[9] As the Court of Appeal observed below: "[T]he record before us [makes it unclear whether defendant] Hunter joined in the opposition to the motions to quash below, but he has formally joined in Sullivan's arguments in this court. For simplicity's sake, we refer to the opposition below as that of [d]efendants collectively." We adopt the same approach.

witnesses support their subpoenas and render the SCA unconstitutional to the extent it purports to afford providers a basis to refuse to comply with their subpoenas. Defendants acknowledged that no court had ever so held, and asked the trial court to be the first [****17] in the nation to do so.

Defendants presented offers of proof concerning the information sought from the various accounts. The prosecution had secured from Facebook and Instagram some of the available social media communications attributed to Rice and, as obligated, had shared that information with defendants in the course of discovery.[10] Regarding the information concerning Rice's communications, defendants asserted that review of the full range of content from those various accounts is required in order to "locate exculpatory evidence" and to confront and cross-examine Inspector Broberg, in order to challenge his assertion that the shooting was gang related. In support defendants cited Broberg's grand jury testimony and attached examples of five [**733] Facebook [*1257] screenshots reflecting videos alleged to have been posted by Rice. Counsel asserted that the subpoenaed records would show that Rice was "a violent criminal who routinely posted rap videos and other posts threatening [Q.H.] and other individuals."

Although the prosecution had secured and shared *some* of Rice's Facebook communications and a portion of the Instagram posts attributed to him, the prosecution had not sought from [****18] providers the social media communications of their key witness, Renesha Lee. Nevertheless, it appears from the record that at least one of Renesha Lee's Twitter accounts was public and contained numerous tweets that were accessible to defense counsel. Counsel evidently accessed that account and identified content that, they asserted, indicated a strong likelihood that other similar, yet undiscovered—and possibly deleted—communications might exist. Defendants alleged [***86] that the prosecution's case turns on Renesha Lee's credibility and that "she is the only witness who implicates Sullivan in the killing."[11] Moreover, defendants explained, they sought additional corroborating information, consistent with that found already in Renesha Lee's public tweets, to demonstrate that she was motivated by jealous rage over Sullivan's involvement with other women and that she had repeatedly threatened others with violence.

In support of these assertions defendants' opposition appended, as an exhibit, photocopied screenshots of what was represented as two of Renesha Lee's Twitter accounts. They quoted a September 2013 tweet showing a photograph of a hand holding a gun and making specific threats: [****19] "I got da. 30 wit dat extend clip. … . BIIIITCH I WILL COME 2YA FRONT DOOR. … ." Various other tweets from both accounts suggested a similar theme. Defendants asserted their need for and intention to use these and any other similar tweets, posts, comments, or messages, including deleted content, made by Renesha Lee on Twitter, Facebook, or Instagram, in order to impeach her anticipated testimony at trial. Defense counsel stated that, despite diligent efforts, Renesha Lee could not be located to be served with a subpoena duces tecum.

E. *The Hearing on the Motions To Quash*

The first session of the bifurcated hearing on the motions to quash was held in early January 2015. The trial court began by explaining that, in light of the pleadings, it was inclined to find the sought material "critical" to the defense against the pending charges, and to conclude that "defendants have a [*1258] [constitutional] right to … information that's authentic … [and] reliable." The court questioned providers' alternative proposal that the prosecution could or should issue additional search warrants to them (the service providers) on behalf of defendants: "First, I think the District Attorney's office is going to [****20] … say[], … our job is not to perform your investigation for you. And, besides, the Penal Code … authorizes search warrants to be obtained [only] under certain circumstances, and … not to find evidence that might support an affirmative defense or mitigate a mental state [or impeach a witness]." The court also expressed concern about defendants' ability to obtain any tweets or posts that may have been deleted by the account holder, and regarding how those communications might be

[10] (See *ante*, fn. 8.) Defendants subsequently asserted, however, that although they have had "access to some of Mr. Rice's social media records through the discovery process that tend to support the prosecution's theory of the case," still they lacked "access to records necessary to present a complete defense and to ensure the right to effective assistance of counsel." Thereafter, in their joint reply brief filed in this court, defendants characterized the prosecution as having declined to obtain all of Rice's various Instagram accounts.

[11] Q.H., in his earlier confession, acknowledged that his brother Derrick was with him in the car when the shooting occurred, but he did not mention Sullivan as being in the car with them. Instead, he asserted that a third person, named Johnson, had been with him and his older brother in the car.

authenticated sufficiently to be allowed into evidence. In that respect, the court questioned whether Renesha Lee would be willing to "take ownership" of tweets attributed to her and quoted above, "[s]ome [of which] could be subjecting her to criminal liability."

The trial court next addressed Twitter's assertion that any "deleted contents" would "not [be] reasonably available" and hence providers would "not … be able to produce deleted contents or authenticate deleted content." The court expressed skepticism concerning Twitter's assertion that it would be unable to produce deleted content, observing: [**734] "[W]hat I … know from my time in discovery [is] that when I delete e-mails, they are not all deleted. [****21] [¶] Now, I don't know … to what extent they are kept on some server or archive that could be retrieved through some sort of search function, or whether some forensic [***87] computer person has a way of reconstructing files or not. [¶] So … if you are going to say that you complied and … state under penalty of perjury [supported by a] showing … that you have done what you can do, that's a separate thing. But, I doubt very much I am going to change my position that this material is critical, it has to be produced, and you are the ones holding it." Accordingly, the court tentatively denied the motions to quash and ordered that the materials be provided to it for in camera review pursuant to *Penal Code section 1326*. At the same time, the trial court allowed additional briefing to be filed before it ruled finally on the matter.

In its subsequent brief Twitter reiterated its assertion that *section 2702 of the SCA* fails to "distinguish between 'private' and 'public' content for purposes of its restrictions on providers' disclosure" and it maintained that "service providers are prohibited from producing *any* content, regardless of status." Facebook and Instagram asserted in their own subsequent brief that *section 2702 of the SCA* bars the requested discovery [****22] and that the Act "contains no exception for criminal defense subpoenas." Consistent with their broad assertion that no exception applied under *section 2702*, they did not address whether any of the sought communications had been configured by the account holder to be public or private/restricted. Twitter, by contrast, directly confronted that issue in its own final supplemental responsive brief, noting [*1259] that one of the accounts in question is public, and that, "[a]s of this filing, anyone can visit the account and review its content, including messages, photos, and videos. In fact, defendant has already done this and included some public content from the account in … support of his Opposition [brief]."[12]

In response, defendants contested the assertions by Facebook and Instagram that defendants could gain access to the sought communications by other means.[13] They argued that unless providers are ordered to comply with the subpoenas, they will be deprived of the information they need and also will be hampered in their effort to "persuade a jury that the records in question originated from Ms. Lee's social media accounts."

After considering the additional briefing, in late January 2015 the trial court [****23] confirmed its earlier conclusions, commenting that it would be "untenable" to deny the requested material to defendants. The court further explored with the parties the issues of deleted communications and burdens that compliance would impose [***88] on providers. In that regard counsel for providers asserted that deleted *tweets* "don't persist in backup for all eternity" and to the extent some remained in storage, "they are going to be very cumbersome and burdensome to obtain." The court responded that it had insufficient information with which to weigh the benefit of production versus burdens, and noted that it could easily impose a temporal restriction on the information sought in order to render the [**735] request more reasonable and less burdensome. The court then asked

---

[12] Twitter also stated: "On Twitter, if an account is public, its Tweets are public—a user cannot make individual Tweets public or private on a post-by-post basis." Further, Twitter addressed the trial court's stated concerns regarding retrieval of deleted content. It asserted that even if the SCA permitted it to comply with the subpoenas' demands, still, any "content deleted by the user is not reasonably available to Twitter."

[13] Regarding Rice, defendants noted that because Facebook allows the default to be changed—and posts to be configured as public or private on a post-by-post basis—not all friends might have "content that Mr. Rice decided to withhold from a particular user." As observed *ante*, footnote 10, defendants conceded that they had access to some of Rice's social media records through the discovery process. But, they insisted, they nevertheless lacked access necessary to present a complete defense. Regarding Renesha Lee's social media records, defendants did not contest Twitter's assertions that one of her Twitter accounts was public and remained open and accessible to all as of the time of the trial court briefing and hearings. Still, defendants asserted, "many of [her other] accounts" (apparently referring especially to the Facebook and Instagram accounts mentioned earlier) "have been deleted," and hence they had no access to them, and yet providers did possess those "inactive and active accounts."

counsel to address recovery of deleted content concerning "your other clients"—Facebook and Instagram. But that discussion never occurred, producing an evidentiary lacuna as to those providers. Thereafter, neither the parties nor the court addressed whether any of the sought tweets had been configured as public, or whether, for any time period, the user had [*1260] protected the account and made tweets sent during that time accessible [****24] to followers only. Nor did the court or parties address the privacy configurations of the remaining Facebook and Instagram communications sought by defendants.

F. *The Trial Court's Ruling on the Motions To Quash*

The trial court finalized its tentative rulings, denying all three motions to quash and ordering that providers submit all of the sought materials for its in camera review by a deadline in late February 2015.[14] The court stated that it understood providers might seek writ review challenging its oral production order, and recognized that the Court of Appeal might stay its production order.

After discussing the need for a preservation order (see *post*, fn. 47), the court vacated the trial date, which had been set for the next day. All parties agreed to reconvene in early March, after the trial court had an opportunity to conduct in camera review of the information that providers had been ordered to produce, or alternatively at a later date pending resolution of the writ proceeding providers intended to file contesting the court's oral production order.

G. *The Writ of Mandate Proceeding*

Providers jointly filed a petition for a writ of mandate in the Court of Appeal contending that [****25] the trial court abused its discretion in denying the motions to quash. They asked the appellate court to "preserve the status quo" by issuing an immediate stay of the trial court's production order and planned in camera review. That court stayed the trial court's production order and issued an order to show cause asking why the relief sought in the petition should not be granted.

After full briefing and oral argument, the Court of Appeal filed an opinion concluding that the SCA barred enforcement of defendants' pretrial subpoenas and rejecting defendants' arguments that the Act violated their rights under the *Fifth* and *Sixth Amendments to the federal Constitution*. Reviewing the relevant case law with respect to the constitutional claims, the appellate court concluded: "The consistent and clear teaching of both United States Supreme Court and California Supreme Court jurisprudence is that a criminal [*1261] defendant's right to *pretrial* discovery is limited, and lacks any solid constitutional foundation." The appellate [***89] court stressed, however, that its conclusion was confined to "*this stage of the proceedings*" and limited to the "pretrial context in which the trial court's order was made." It observed [****26] that defendants would remain free to seek "at trial the production of the materials sought here." The appellate court commented that the trial judge who would eventually conduct the trial "would be far better equipped" than the appellate court itself "to balance [defendants'] need for effective cross-examination and the policies the SCA is intended to serve," and suggested that the SCA might eventually need to be declared unconstitutional to the extent it precludes enforcement of such a *trial* subpoena issued by the trial court itself, or by defendants, with production to the court. With respect to the pretrial context, however, the appellate court directed the trial court to vacate its order denying providers' motions to quash the pretrial subpoenas, and to grant the motions to quash.

## II. Proper Interpretation of the Stored Communications Act

Because the parties agreed in the trial court that the *SCA* precluded providers from [**736] complying with defendants' subpoenas and the court accepted that proposition, the trial court proceeded on the assumption that providers' refusal to comply with the subpoenas raised only constitutional questions. It then decided the matter by resolving those constitutional [****27] issues in defendants' favor. As explained above, the Court of Appeal likewise viewed the case as raising only constitutional issues, and its decision in providers' favor was grounded on the appellate court's conclusion that defendants' constitutional claims were not viable in the pretrial context.

In their initial briefing in this court, the parties again proceeded on the assumption that the litigation raised only constitutional issues, and they debated the merits of defendants' constitutional contentions. Defendants reiterated the view that their federal constitutional right to due process under the *Fifth Amendment*, and their

[14] As the Court of Appeal observed, defendant Hunter apparently did not formally oppose Twitter's motion to quash his subpoena. Nevertheless, the trial court assumed such a motion and denied it on the same basis that it denied the motions to quash defendant Sullivan's subpoenas.

confrontation, compulsory process, and effective assistance of counsel rights under the *Sixth Amendment*, require that the Act be declared unconstitutional to the extent it precludes the enforcement of their subpoenas in this case. They candidly recognized that case authority supporting their position is sparse. Ultimately, they suggested that we should overrule or distinguish our own decisions (especially *People v. Hammon (1997) 15 Cal.4th 1117 [65 Cal. Rptr. 2d 1, 938 P.2d 986]* and its progeny) in order to declare the SCA unconstitutional as applied and uphold their pretrial subpoenas. Providers, by contrast, asserted that no decision of any court supplies authority [****28] supporting defendants' entitlement to pretrial enforcement of their subpoenas. They argued that, to the extent defendants might later *at [*1262] trial* be able to establish a due process right to the information they seek in order to secure a fair trial, their remedy at trial would not lie in a judicial declaration that the SCA is unconstitutional as applied to them. Instead, providers asserted, the trial court should at that time put the prosecution to a choice: (1) use its authority under the Act to acquire the sought materials on behalf of defendants and share them with defendants at trial, or (2) suffer consequences in the form of an adverse evidentiary ruling at trial, including potentially pivotal instructions to the jury, or outright dismissal of the prosecution's case.

As mentioned, our initial review of the SCA and the relevant legislative history of the pertinent provisions, as well as prior judicial decisions addressing related issues, led us to question the validity of the statutory interpretation of the SCA on which [***90] the case was litigated below. Specifically, we questioned whether the relevant statute, *section 2702(a)*, which appears to bar providers from disclosing electronic communications configured [****29] by the user to be private or restricted, *also* bars providers from disclosing communications that had been configured by the user to be public. Accordingly, we requested supplemental briefing directed to that issue, identifying the portions of the legislative history that appeared most relevant.

**(2)** As explicated *post*, part III.A., in the ensuing supplemental briefing all parties concede that *section 2702(b)(3)*'s lawful consent exception permits providers to disclose public communications. In order to understand the relevant provisions of the SCA and why we also conclude that the statute should be so construed, it is appropriate to review the Act's general history, the language of the relevant statutory provisions, the specific legislative history of those provisions, and prior relevant case law.

A. *The SCA—History and General Background*

Congress enacted the *Electronic Communications Privacy Act in 1986. (ECPA; Pub.L. No. 99-508 (Oct. 21, 1986), 100 Stat. 1848, 1860*.) Title I of that law, amending the prior "Wiretap Act," addresses the interception of wire, oral, and electronic communications. (*§§ 2510–2521*.) Title II of the law, set out in chapter 121, is often referred to as the *Stored Communications Act*, or SCA. It addresses unauthorized [****30] access to, and voluntary and compelled disclosure of, such communications and related information. (*§§ 2701–2712*.)

Prior to the *ECPA*'s enactment, the respective judiciary committees of the House of Representatives and the Senate prepared detailed reports concerning the legislation. [**737] Each explained that the main goal of the *ECPA* in general, and of the SCA in particular, was to update then existing law in light of dramatic [*1263] technological changes so as 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) (hereafter House Report); see also Sen.Rep. No. 99-541, 2d Sess., p. 3 (1986) (hereafter Senate Report) [speaking of protecting both "privacy interests in personal proprietary information" and "the Government's legitimate law enforcement needs"].)[15] Each report also highlighted a related objective: to avoid discouraging the use and development of new technologies.[16] These

[15] The House Report described privacy protection as "most important," and noted: "[I]f Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances." (House Report, *supra*, at p. 19, fns. omitted.) The Senate committee expounded on this theme, observing that "computers are used extensively today for the storage and processing of information," and yet because electronic files are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection" absent new legislation. (Sen. Rep., *supra*, at p. 3; accord, House Rep., *supra*, at pp. 16–19.)

[16] In this latter regard, the House Report, noting the "legal uncertainty" that surrounded the government's legitimate access to such stored information, expressed concern that such conditions may expose law enforcement officers to liability, endanger the admissibility of evidence, encourage some to improperly access communications, and at the same

three themes—(1) protecting the [***91] privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies (with privacy protection being the primary focus)—were [****31] also repeatedly emphasized by the bill authors in their debate remarks.[17] As this history reveals, and as a leading commentator on the SCA has explained, Congress was concerned that "the significant privacy protections that apply to homes in the physical world may not apply to 'virtual homes' in cyberspace," and hence "tried to fill this possible gap with the SCA." (Kerr, *A User's Guide to [*1264] the Stored Communications Act, and a Legislator's Guide to Amending It* (2004) 72 Geo. Wash. L.Rev. 1208, 1210.)[18]

B. *Key Provisions of the SCA*

1. *Rules regarding unauthorized access to stored communications: Sections 2701 and 2511(2)(g)(i)*

Section 2701(a) provides that, subject to specified exceptions, "whoever … [¶] … intentionally accesses without authorization a facility through which an electronic communication [**738] service is provided" or "intentionally exceeds an authorization to access that facility" and "thereby obtains" an "electronic communication while it is in electronic storage in such system" commits an offense punishable by a fine or imprisonment. At the same time, a separate provision contained in another part of the ECPA, section 2511(2)(g)(i), articulates [****32] a substantial limitation on section 2701's access prohibition: "It shall not be unlawful under … chapter 121 [that is, the SCA] … [¶] … to … access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[19]

2. *Rules prohibiting disclosure by service providers and listing exceptions under which providers are permitted to disclose "communications" or "customer records": Section 2702*

Section 2702 addresses disclosure by certain covered service providers—and by [***92] no other person or entity. (Wesley College v. Pitts (D.Del. 1997) 974 F.Supp. 375, 389.) Section 2702(a)(1) declares that, subject to specified exceptions, "a person or entity providing an electronic communication service[20] to the public *shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service*." [*1265] (Italics added.) Similarly, and again subject to the same exceptions, section 2702(a)(2) declares that "a person or entity

---

time, "unnecessarily discourage potential customers [from] using such systems." (House Rep., *supra*, at p. 19.) Similarly, the Senate Report cited the same potential problems, and added that legal uncertainty might not only discourage use of "innovative communications systems" but also "may discourage American businesses from developing new innovative forms of telecommunications and computer technology." (Sen. Rep., *supra*, at p. 5.)

[17] For example, Congressman Kastenmeier, the bill's primary author, stressed as a governing principle "that what is being protected is the sanctity and privacy of the communication." (Remarks of Rep. Kastenmeier, 132 Cong. Rec. 14886 (1986).) Senator Leahy, the bill's sponsor in the upper house, repeatedly referred to the need to "update our law to provide a reasonable level of Federal privacy protection to these new forms of communications" in order to address inappropriate acquisition by "overzealous law enforcement agencies, industrial spies, and just plain snoops" of "personal or proprietary communications of others." (Remarks of Sen Leahy, 132 Cong. Rec. 14600 (1986).) Cosponsor Senator Mathias described the legislation as "a bill that should enhance privacy protection, promote the development and proliferation of the new communications technologies, and respond to legitimate needs of law enforcement." (Remarks of Sen. Mathias, 132 Cong. Rec. 14608 (1986).)

[18] Congress's conception of the Internet more than 30 years ago was, of course, substantially different from the Internet that exists today. "The World Wide Web had not been developed, and cloud computing services and online social networks would not exist for nearly a decade. Internet users in 1986 could essentially do three things: (1) download and send e-mail; (2) post messages to online bulletin boards; and (3) upload and store information that they could access on other computers. The definitions and prohibitions listed in the SCA align with these three functions as they existed in 1986. 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." (Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act* (2011) 24 Harv. J.L. & Tech. 563, 566, fns. omitted (*Discovering Facebook*).)

[19] Section 2707 authorizes a civil action to enforce these and the following provisions of the SCA.

[20] An electronic communication service (ECS) is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (§ 2510(15).)

providing remote computing service[21] 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* … .” (Italics added.) [****33] Finally, section 2702(a)(3) bars any service provider from knowingly divulging any non-content “record or other information pertaining to a subscriber to or customer” to any governmental entity.

The next two subsections of section 2702—(b) and (c)—list *exceptions to the general prohibition* on disclosure by a service provider set forth in subsection (a). Subsection (b) describes eight circumstances under which a provider “may divulge the contents of a communication.” (§ 2702(b).) As relevant here, subparts (1) through (3) of subsection (b) permit disclosure: (1) “to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient” (§ 2702(b)(1)); (2) pursuant to section 2703, which, as described below, permits a “governmental entity” to compel a covered provider to disclose stored communications by search warrant, subpoena or court order; and (3) “with the *lawful consent of the originator or an addressee or intended recipient* of such communication, or the subscriber in the case of [a] remote computing service” (§ 2702(b)(3), italics added). As explained below, some of the communications sought under the subpoenas at issue here may fall within the lawful consent exception set forth in section 2702(b)(3).[22]

Finally, section 2702(c) describes six circumstances under which a covered provider may divulge *non-content information*—that is, any “record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications …).”[23] As [**739] relevant here, the last [*1266] [****34] of these exceptions permits disclosure “to any person other than a governmental entity” (§ 2702(c)(6))—which includes defendants in this case.[24]

[***93] 3. *Rules governing compelled disclosure by a service provider to agovernmental entity: Section 2703*

**(3)** As alluded to above, section 2703 governs compelled disclosure by covered providers to a “governmental entity.” It sets forth the rules under which law enforcement entities may compel ECS and RCS providers to disclose private as well as public communications made by users and stored by covered service providers.[25]

C. *House and Senate Reports Concerning the Relevant Provisions*

The 1986 congressional reports took special note of then-existing electronic bulletin boards—early analogues to the social media platforms at issue here. In the course of these discussions, the respective judiciary committees focused on the configuration of posts as being private or public and indicated an

---

[21] The term “‘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).)

[22] The five other exceptions listed in section 2702(b) include disclosure incidental to the provision of the intended service or protection of the rights or property of the service provider; matters related to child abuse; and disclosure to a law enforcement agency of inadvertently obtained information that appears to pertain to a crime.

[23] Such “non-content” records consist of logs maintained on a network server, as well as “basic subscriber information,” including the following: “(A) name; [¶] (B) address; [¶] (C) local and long distance telephone connection records, or records of session times and durations; [¶] (D) length of service (including start date) and types of service utilized; [¶] (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and [¶] (F) means and source of payment for such service (including any credit card or bank account number).” (§ 2703(c)(2).)

[24] The five preceding listed exceptions include disclosures of non-content information (1) authorized under compulsion by a “governmental entity” under section 2703; (2) with the lawful consent of the customer or subscriber; (3) as necessary and incidental to the provision of the intended service or protection of the rights or property of the service provider; (4) self-initiated to a law enforcement agency under emergency conditions; or (5) related to child abuse. (§ 2702(c).)

[25] (§ 2703(a) & (b).) As alluded to *ante*, footnote 23, section 2703(c) addresses compelled disclosure to a governmental entity of certain non-content information. Other subsections articulate the requirements of any court order compelling disclosure (§ 2703(d)), specify that there can be no cause of action against a provider that discloses information pursuant to this chapter (§ 2703(e)), and impose on providers a requirement to preserve evidence on request of a governmental entity “pending the issuance of a court order or other process” (§ 2703(f)(1)).

understanding that section 2701, governing [****35] unauthorized *access* to communications, was intended to cover and protect only private and not public posts. Significantly, the reports indicated the same understanding regarding section 2702's ban on provider *disclosure* of electronic communications, as reflected in that section's lawful consent exception to the ban.

The extensive House Report, issued first, repeatedly focused on the public/private theme. It did so initially in a passage addressing section 2511(2) of the ECPA, which as noted above states in subsection (g)(i) that it "shall not be unlawful" under either the omnibus ECPA or its SCA subset to "access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." The committee explained that under this provision, it would be "permissible to intercept electronic communications [*1267] made through an electronic communication system that is *configured so that such electronic communication is readily accessible to the general public*" and that "[t]he *term 'configure' is intended to establish an objective standard of design configuration to begin determining whether a system receives privacy protection*." (House Rep., *supra*, at p. 41, italics added.) Later, [****36] when the report addressed the SCA's analogue to this access rule, it explained that section 2701 would not "hinder the development or use of 'electronic bulletin boards' or other comparable services. *The Committee believes that where communications are readily accessible to the general public, the sender has, for purposes of Section 2701(a), extended an 'authorization' to the public to access those communications*. A person may reasonably conclude that a communication is readily accessible to the general public if the … means of access [is] widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. *To access a communication on such a system should not be a violation of the law*." (House Rep., *supra*, at p. 62, italics added.) [***94] On the other hand, the report noted, some electronic bulletin boards may provide, in addition to a public forum, private e-mail services—and it [**740] observed: "Section 2701 would apply differently to the different services. *Those … electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily [****37] accessible to the general public*." (*Id*., at p. 63, italics added.) The subsequent Senate Report similarly focused on electronic bulletin boards and repeatedly echoed the same public/private distinction. (Sen. Rep., *supra*, at pp. 8–9, 35–36.)

The House Report next turned to the provision that we must construe here, section 2702, prohibiting *disclosure* by covered providers of communications contents. The committee revealed its understanding that the theme of distinguishing between public and private posts carried over from section 2701's access rule and applied as well to section 2702's bar on the divulging of communications by providers.

The report observed that although section 2702(a) articulates a general prohibition on disclosure by a provider, section 2702(b)(3), setting out one of eight exceptions to that rule, permits such a provider to divulge contents "with the lawful consent of the originator or any addressee or intended recipient" of the communication. (House Rep., *supra*, at p. 66.) The committee explained that, in its view, *implied* lawful consent by a user—and hence permissible disclosure by service providers—would readily be found with regard to communications configured by the user to be accessible to the public. It stressed that consent as contemplated by section 2702(b)(3) "need not take the form of a formal written document [****38] of consent." (House Rep., *supra*, at p. 66.) The report viewed consent to disclosure as being implied by a user's act of posting publicly, and/or by a user's acceptance of a provider's [*1268] terms of service: "Consent may … flow from a *user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use—e.g., continued use of such an electronic communication system*." (*Ibid*., italics added.) The report explained that "[a]nother type of *implied consent* might be inferred from *the very nature of the electronic transaction*. *For example, a subscriber who places a communication on a computer 'electronic bulletin board,' with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication*." (*Ibid*., italics added.) Moreover, the report continued, "*If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent [****39] on the part of a user to disclosures or uses consistent with those rules*." (*Ibid*., italics added.) In other words, the committee indicated its

understanding that with regard to electronic communications configured by the user to be accessible to the public, a covered service provider would be free to divulge those communications under section 2702(b)(3)'s lawful consent exception. Nothing in the subsequent Senate Report took issue with this analysis. (Sen. Rep., *supra*, at pp. 36–38.)

D. *Cases Construing the SCA in Light of the House and Senate Reports*

Prior decisions have found that Facebook and Twitter qualify as either an ECS [***95] or RCS provider and hence are governed by section 2702 of the SCA.[26] All parties assume the same with respect to all three providers before us. We see no reason to question this threshold determination.

Only a few decisions have construed the relevant provisions of the SCA, and nearly all have concerned civil litigation. Most have focused on claims that a party had obtained unauthorized *access* to stored communications [**741] under section 2701, and hence are not directly applicable here. Two decisions have addressed the question we face in this criminal matter—whether section 2702 bars covered service providers from *divulging social media communications [****40]* in response to a subpoena. For context—and because, as we will see, one of the key section 2702 disclosure cases subsequently relied on some of [*1269] the section 2701 access cases—it is useful to briefly address the access cases before discussing the disclosure decisions.

1. *"Unauthorized access" cases interpreting section 2701*

Konop v. Hawaiian Airlines, Inc. (9th Cir. 2002) 302 F.3d 868 (*Konop*) concerned asserted unauthorized access to communications on a restricted and password-protected electronic bulletin board. The Ninth Circuit panel, citing some of the passages set out in the two judiciary committee reports noted above, concluded that this legislative history "suggests … Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards" and that Congress intended the configuration of communications would "'establish an objective standard [for] determining … privacy protection.'" (*Id., at pp. 875, 879, fn. 8*, quoting House Rep., *supra*, at p. 41.) Subsequently, *Snow v. DirecTV, Inc. (11th Cir. 2006) 450 F.3d 1314*, quoted and extended *Konop*'s observation. The Eleventh Circuit concluded that in light of *section 2511(2)(g)(i)* and some of the legislative history described earlier, Congress intended to confine the reach of *section 2701*'s access bar to those stored electronic communications that were configured to be restricted and [****41] not readily accessible to the general public. (*Snow, at pp. 1320–1321*.)

More recently, in *Ehling, supra, 961 F.Supp.2d 659*, a federal district court addressed a party's asserted unauthorized access to a user's restricted Facebook posts. The court highlighted the House Report's understanding that the configuration of communications would determine whether any given post is "accessible to the public" (*id., at p. 666*), and it relied on *section 2511(2)(g)(i)* (permitting *access* to communications that are "readily accessible to the general public") as well as *Konop* and *Snow* in concluding that "the SCA covers: (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) *that are not public*" (*Ehling, supra, at p. 667*, italics added). The court found that Facebook "posts … configured to be private meet all four criteria." (*Ibid*.) In reaching this conclusion the court observed that decisions "interpreting the SCA confirm that information is protectable *as long as the communicator actively restricts the public from accessing the information*." (*Id., at p. 668*, italics added.)

[***96] The *Ehling* court elaborated: "The touchstone of the *[ECPA]* is that it protects private information. The language of [****42] the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private." (*Ehling, supra, 961 F.Supp.2d at p. 668*.) It reasoned: "Facebook allows users to select privacy settings … . Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just [*1270] the user. *The Court finds that, when users make their Facebook … posts inaccessible to the general public*, [*those*] *posts are 'configured to be private' for purposes of the SCA. …* [W]hen it comes to privacy protection, the critical inquiry is whether Facebook users *took steps to limit access to the information* [in their posts]. Privacy protection provided by the SCA does not depend on the

[26] See, e.g., *Crispin v. Christian Audigier, Inc. (C.D.Cal. 2010) 717 F.Supp.2d 965, 987–990* (*Crispin*) (regarding Facebook posts and private messages); *Ehling v. Monmouth-Ocean Hospital Service Corp. (D.N.J. 2013) 961 F.Supp.2d 659, 665–670* (*Ehling*) (implicitly concluding the same regarding Facebook posts). A New York trial court has implicitly reached the same conclusion regarding Twitter tweets. (*People v. Harris (2012) 36 Misc.3d 868 [949 N.Y.S.2d 590, 596]*.)

number of Facebook friends that a user has." (*Ibid.*, italics added.)[27]

2. *"Prohibited disclosure" cases interpreting section 2702*

In addition to the civil decisions construing *section 2701*'s *access* rules and recognizing a [**742] public/private distinction in that setting, a few civil cases have concerned *section 2702*'s prohibition on disclosure, as applied to third party subpoenas designed to compel *providers* to *divulge* electronic communications by the providers' users.

a. O'Grady *and related cases regarding subpoenas to providers [****43] seeking e-mail communications*

The first group of decisions addresses requests for disclosure by e-mail providers of their users' e-mail communications. A leading example is *O'Grady, supra, 139 Cal.App.4th 1423*, in which a California appellate court held *section 2702* prevented an e-mail service provider from complying with a subpoena issued on behalf of Apple Computer (Apple). Apple sought the e-mail communications of an online news magazine to discover the identities of those who leaked confidential information about an impending Apple product. In concluding that *section 2702* prohibited disclosure by the provider of such private e-mails (*O'Grady, at pp. 1440–1451*), the court distinguished between public posts that were made available "to the world," and the "contents of private [e-mail] messages" at issue in that case. (*Id., at p. 1449*, italics omitted.) The court noted that it would reach a different conclusion, and presumably find disclosure permissible, "if the discovery [could] be brought within one of the statutory exceptions—most obviously, a disclosure with the consent of a party to the communication" under the lawful consent exception of *section 2702(b)(3)*. (*O'Grady, at p. 1446*; see also *id., at p. 1447*.) Likewise, other courts have concluded that *section 2702* bars e-mail service providers from divulging private e-mail [****44] communications in response [*1271] to third party civil subpoenas when, as in *O'Grady*, no exception to the Act's prohibitions on disclosure is applicable. (See, e.g., *In re Subpoena Duces Tecum to AOL, LLC (E.D.Va. 2008) 550 F.Supp.2d 606, 611* ["[a]greeing with the reasoning in [***97] *O'Grady*" and declining to enforce a subpoena seeking production of private e-mail communications absent an applicable exception to the prohibition on disclosure].)

*b.* Viacom *and* Crispin*—regarding subpoenas served on providers seeking social media communications*

Two additional *section 2702* disclosure cases are more pertinent to our present inquiry because they concerned disclosure by service providers, not of private e-mail, but of *social media communications*. As explained below, these decisions reflect an understanding that Congress intended *section 2702* to prohibit disclosure by providers of only private or restricted, but not public, social media communications.

The first opinion, *Viacom Internat. Inc. v. YouTube Inc. (S.D.N.Y. 2008) 253 F.R.D. 256*, addressed efforts by copyright owners to compel a social media provider, YouTube, to divulge stored information regarding videos that users had configured as private or restricted. (*Id., at p. 264*.) The federal district court quoted the House Report's observation, noted *ante*, part II.C., that one who posts a communication with a reasonable basis for knowing [****45] that it will be available to the public should be considered to have implicitly consented to such disclosure under *section 2702(b)(3)*. (*253 F.R.D. at p. 265*.) The court held, however, that YouTube was barred under *section 2702(a)* from disclosing "videos that [users] have designated as private and chosen to share only with specified recipients"—and that on the facts presented, *section 2702(b)(3)*'s lawful consent exception was inapplicable. (*Viacom, at pp. 264–265*.)

The second decision, *Crispin, supra, 717 F.Supp.2d 965*, also concerned disclosure by a social media service provider under *section 2702* in response to a civil discovery subpoena. The plaintiff in *Crispin*, an artist, sued the defendants, clothing manufacturers, asserting they violated a license to use his art. The defendants in turn issued subpoenas to various service providers, including Facebook and social media provider MySpace. The subpoenas broadly sought all manner of communications, ranging from public to private, between the plaintiff and others. The plaintiff moved to quash the subpoenas on various grounds, including that

[27] The court in *Ehling* observed that the plaintiff user had "approximately 300 Facebook friends" (*Ehling, supra, 961 F.Supp.2d at p. 662*), and concluded that because she had configured her communications as limited to them, the posts were covered by *section 2701* (*Ehling, at p. 668*). Nonetheless, the court ultimately rejected the plaintiff's claim of unauthorized access, finding that because an authorized recipient/friend had voluntarily shared the plaintiff's restricted communications with others, *section 2701*'s "authorized user" exception was applicable. (*Ehling, at pp. 669–671*.)

the providers were barred by section 2702 from making the disclosures. A magistrate concluded that the section did not apply, and declined to quash the subpoenas with respect to any of the communications.
[*1272]

[**743] On review, the district court, relying [****46] on the legislative history of the SCA and the decision in Konop, supra, 302 F.3d 868, discussed above, determined first that so-called "private messaging" communications, like the e-mails in *Konop*, were configured to be private and hence protected from disclosure by service providers under section 2702(a). (Crispin, supra, 717 F.Supp.2d at p. 987.) Turning to the other communications, Facebook posts and MySpace comments, the court analogized those communications to the technology that existed in 1986—postings on a "'computer bulletin board'" system. (Id., at p. 980.) The court concluded that "a completely public [bulletin board system] does not merit protection under the SCA"—and that "'[o]*nly electronic bulletin boards which are not readily accessible to the public are protected under the Act*.'" (Id., at p. 981, italics added.) In other words, the court determined that Facebook posts and MySpace comments configured by registered users to be public are not protected from disclosure under section 2702(a) of the Act. But, the court reasoned, those communications would not be subject to disclosure by a provider if the user, like users of older restricted-access electronic [***98] bulletin boards, had configured the post or comment to be accessible only by a restricted group. (Crispin, at p. 981.)

Accordingly, the court [****47] in *Crispin* determined that the dispositive question was whether the posts had been configured by the user as being "sufficiently restricted that they are not readily available to the general public." (Crispin, supra, 717 F.Supp.2d at p. 991.) Further, the court found that any restrictive privacy configuration employed by the user should be honored, and would bar disclosure by a service provider under section 2702 of the SCA, even if the restricted group is comprised of *all* of a user's Facebook friends. (Crispin, at p. 990.)[28]

Applying these principles to the motion to quash the civil subpoenas before it, the *Crispin* court observed that the parties had provided an incomplete record regarding the nature of the various private message services and other posts and comments services offered by those social media entities. Accordingly, the court remanded the matter "so that [the magistrate] can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings and the extent of access allowed to his Facebook [posts] and MySpace comments." (Crispin, supra, 717 F.Supp.2d at p. 991.)
[*1273]

The gist of *Crispin*'s discussion and treatment was that communications configured by the user to be restricted in some manner fall within section 2702's prohibition on disclosure by providers and are [****48] not subject to a civil subpoena directed to those providers. On the other hand, the subpoenas would be enforceable to the extent they sought Facebook posts and MySpace comments that had been configured by the registered user to be publicly accessible.

**(4)** In reaching these conclusions *Crispin* relied heavily on the SCA's *access* provisions and related case law—and it focused generally on section 2702's *disclosure* bar without also considering specifically the lawful consent exception set out in section 2702(b)(3). Accordingly, the decision can be read as concluding that if Congress intended to withhold liability under section 2701 concerning those who *access* public communications, Congress must also have intended not to protect those same public communications from *disclosure* by covered providers under section 2702. Under this view, which appears to have been endorsed by some commentators,[29] the Act [***99] simply would

---

[28] The *Crispin* court reasoned: "Although here a large number of [registered] users, i.e., all of plaintiff's Facebook friends, might access the storage and attendant retrieval/display mechanism, the number of users who can view the stored message has no legal significance. Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms, which may have thousands of employees who can access documents in storage, would be excluded from the statute." (Crispin, supra, 717 F.Supp.2d at p. 990.)

[29] See, e.g., Discovering Facebook, supra, 24 Harv. J.L. & Tech. at page 584 ("Under the SCA, information that is 'readily accessible to the general public' is not protected from disclosure"); Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act* (2012) 17 Suffolk J. Trial & App. Advoc. 295, 314–315, 319 ("case law has made clear that communications that are 'readily accessible' by the public are not protected by the SCA"; "where a user's privacy settings allow the general public to view such communications, it is clear that the SCA will not govern such 'readily accessible' communications"; and when comments can be "viewable by anyone with internet access"

not cover or protect communications that have been configured to be public. We do not endorse this reading of the Act, however. Instead, we conclude that, by virtue of section 2702(a), the Act generally [**744] and initially prohibits the disclosure of *all* (even public) communications—but that section 2702(b)(3)'s subsequent lawful consent exception allows providers to disclose [****49] communications configured by the user to be public. Thus, although we agree with the result in Crispin, we conclude that the decision in that case should have been grounded on the lawful consent exception to the general prohibition.

As observed *ante*, part II.C., the House Judiciary Committee discussed the public/private distinction articulated under section 2511(2)(g)(i) of the ECPA, and revealed that it viewed that same distinction as carrying over and applying under the related *access* provision of the SCA, section 2701. The House Report then proceeded to describe the *disclosure* provision, section 2702, in a manner showing that it considered the same public/private distinction to apply in that context as well *via the lawful consent exception* [*1274] contained in section 2702(b)(3). We conclude that the Crispin decision properly focused on the user's configuration of communications, and it also reached the correct result—even though it did not explicitly rely, as it should have, on the lawful consent exception and legislative history illuminating that exception.[30]

E. *Conclusion Regarding Section 2702(b)(3)'s Lawful Consent Exception*

**(5)** In light of the foregoing analysis, we conclude that communications configured [****50] by a social media user to be public fall within section 2702(b)(3)'s lawful consent exception, presumptively permitting disclosure by a provider.

## [***100] III. Application to This Case

A. *Overview: The Parties' General Agreement in Their Supplemental Briefs That Public Communications May Be Disclosed Under the Lawful Consent Exception; Limitation of Our Analysis to That Statutory Issue; and the Need for Remand to the Trial Court*

As alluded to earlier, in supplemental briefs concerning section 2702 filed in response [**745] to questions posed by this court, both parties now agree that a social media communication configured by a registered user to be public falls [*1275] within section 2702(b)(3)'s lawful consent exception.[31] In reaching this conclusion,

---

they "would not be protected by the SCA"); see also Comment, *Balancing the Scales of Justice* (2011) 9 J. on Telecomm. & High Tech. L. 285, 296–297 (distinguishing Facebook's private "user-to-user messaging functions," which are similar to e-mail, and that "would be protected by the SCA," from posts and "publicly-viewable" content "that would not be covered under the SCA").

[30] We also briefly note a recent Tennessee intermediate appellate court decision, State v. Johnson (Tenn.Ct.App. 2017) 538 S.W.3d 32 (*Johnson*). That litigation, like the present case, arose pretrial in a criminal prosecution. A percipient witness told the police that various "social media communications" concerning the events had been sent and received by her, as well as the victim and other friends of the victim, and both defendants, before and after the alleged offenses occurred. (*Id., at p. 38*.) One of two defendants issued subpoenas to, among others, the relevant social media service providers, broadly seeking all such communications. The state—but not the providers—moved to quash the subpoenas. (*Id., at pp. 44–48*.) The trial court denied the state's motion as to the providers, finding that the state lacked standing to object on their behalf. (*Id., at pp. 47–49*.) On review the appellate court agreed and then proceeded, in dictum, to address matters that might arise on remand.

The court described the evolution of the SCA, extensively quoted sections 2701, 2702 and 2703, and briefly discussed some of the cases cited above, including *Crispin.* (*Johnson, supra, 538 S.W.3d at pp. 63–69*.) The appellate court next focused solely on section 2703, which as noted earlier concerns a *governmental entity's* authority to compel disclosure from providers. (*Johnson, at pp. 69–70*.) The court observed that the underlying defendants did not qualify as governmental entities—and from there jumped to the broad conclusion that the defendants "could not obtain" pursuant to their subpoenas "*any* information directly from the social media providers under the terms of the SCA." (*Id., at p. 70*, italics added.) In proceeding as it did, the *Johnson* court's dictum failed to consider the legislative history outlined above, the scope of section 2702's disclosure bar, or the lawful consent exception to that bar. As a result, the court failed to consider whether any of the sought social media communications had been configured by the users to be public, and thus were disclosable by the providers pursuant to the defense subpoenas.

[31] In their supplemental brief, providers initially maintain that defendants' failure to challenge providers' proposed statutory interpretation in the lower courts precludes this court from addressing the propriety of that statutory interpretation at this juncture. We reject this contention. It is this court, not defendants, that has raised issues different from those argued below. When this court discovers a possible statutory

providers retreat from their assertions that no exception to the prohibition applies with respect to any of the sought communications. Providers concede that, based on the legislative history described earlier, "[w]hen a user chooses to make a communication freely accessible to the public, he or she has necessarily consented to its disclosure." Accordingly, providers acknowledge that "as applied to communications that are available to the public, [section 2702(b)(3)'s] lawful consent exception allows a provider to disclose communications [****51] to any member of the public."

Nevertheless, both parties urge us to address not only the scope of the lawful consent exception, but also the constitutional issues originally framed and briefed. As alluded to in footnote 31, *ante*, and as explained below, we find it proper at this point to address only the statutory issues, and not the constitutional claims.

As observed earlier, in the lower court proceedings the parties did not focus on the public/private configuration distinction. The trial court made no determination whether any communication sought by defendants was configured to be public (that is, with regard to the communications before us, one as to which the social media user placed no restriction on who might access it) or, if initially configured as public, was subsequently reconfigured as restricted or deleted. Nor is it clear that the trial court made a sufficient effort to require the parties to explore and create a full record concerning defendants' need for disclosure *from providers*—rather than from others who may have access to the communications. Consequently, at this point it is not apparent that the court had sufficient information by which to assess defendants' need for [****52] disclosure from providers when it denied the motions to quash and allowed discovery on a novel constitutional theory. In any event, because [*1276] the [***101] record is undeveloped, we do not know whether any sought communication falls into either the public or restricted category—or if any initially public post was thereafter reconfigured as restricted or deleted.

In light of our interpretation of the Act, it is possible that the trial court on remand might find that providers are obligated to comply with the subpoenas at least in part. Accordingly, although we cannot know how significant any sought communication might be in relation to the defense, it is possible that any resulting disclosure may be sufficient to satisfy defendants' interest in obtaining adequate pretrial access to additional electronic communications that are needed for their defense. For these reasons, we will not reach or resolve defendants' constitutional claims at this juncture. Instead, we conclude that a remand to the trial court is appropriate.

In order to provide guidance to the trial court on remand, we discuss two issues regarding the statutory question that have been raised by the parties in their supplemental briefs. [****53]

[**746] B. *Defendants' Contention That Implied Consent To Disclosure by a Provider Is Established When a Communication Is Configured by the User To Be Accessible to a "Large Group" of Friends or Followers*

The parties now generally agree that communications configured by a social media user to be public fall within section 2702(b)(3)'s lawful consent exception and presumptively may be disclosed by a provider. Beyond this point of agreement, the parties disagree starkly concerning the proper scope and interpretation of the implied consent exception.

Defendants advance an expansive interpretation of the exception. They argue that a user's implied consent to disclosure by providers under section 2702(b)(3) should be triggered not only by communications configured by the user to be public, but also by those configured by the user to be *restricted*, but nonetheless accessible to a "large group" of friends or followers. Defendants contend that, in practice, social media users "lose[] control over dissemination once the information is posted," and can have no reasonable expectation of privacy even with regard to such restricted communications in light of the fact that any authorized recipient can easily copy any communication and

---

interpretation question that may obviate the need to address a constitutional claim and solicits supplemental briefing on that issue, the statutory interpretation question is properly before us for resolution. (See ***Cal. Rules of Court, rule 8.516(b)(2)*** ["The court may decide an issue that is neither raised nor fairly included in the petition or answer if the case presents the issue and the court has given the parties reasonable notice and opportunity to brief and argue it"].) Here we are guided by the familiar principle that we should address and resolve statutory issues prior to, and if possible, instead of, constitutional questions (see, e.g., *Santa Clara County Local Transportation Authority v. Guardino (1995) 11 Cal.4th 220, 230–231 [45 Cal. Rptr. 2d 207, 902 P.2d 225]*, and cases cited), and that "we do not reach constitutional questions unless absolutely required to do so to dispose of the matter before us" (*People v. Williams (1976) 16 Cal.3d 663, 667 [128 Cal. Rptr. 888, 547 P.2d 1000]*, and cases cited).

share [****54] it with others. (Cf. *Moreno v. Hanford Sentinel, Inc. (2009) 172 Cal.App.4th 1125, 1129–1130 [91 Cal.Rptr.3d 858]* [social media user had no reasonable expectation that a communication configured as restricted would not be shared with others and hence could not maintain a tort action for public disclosure of private facts].) Defendants observe that the Internet, attendant technology, and social media itself did not exist when Congress [*1277] considered and enacted the SCA. (See *ante*, fn. 18.) Therefore, they assert, *section 2702* of the Act, generally prohibiting providers from disclosing stored communications, "should be deemed inapplicable" on the ground that "social media posts to large groups are essentially public posts in which the user has no reasonable expectation of privacy."

In support, defendants rely primarily on distinguishable decisions finding social media communications discoverable in civil litigation from a social media user, not, as here, from a social media provider. (E.g., *Fawcett v. Altieri (2013) 38 Misc.3d 1022 [960 N.Y.S.2d 592, 597]* [private social media posts may be compelled from a user in civil discovery "just as material from a personal diary may be discoverable"].) They also rely on cases such as *U.S. v. Meregildo (S.D.N.Y. 2012) 883 F.Supp.2d 523, 526* (*Meregildo*) [rejecting [***102] *4th Amend.* claim and holding that a criminal defendant who restricted Facebook communications to "friends" had no legitimate [****55] expectation that a friend would not share that information with the government]. But none of these cases involving the propriety of compelling disclosure by social media *users* concerned or construed *section 2702*'s prohibition on disclosure by *providers*.

Defendants criticize decisions such as *Crispin, supra, 717 F.Supp.2d 965*, and *Ehling, supra, 961 F.Supp.2d 659*, for analogizing social media communications to what they characterize as "nearly obsolete" electronic bulletin boards. They insist that focusing on such allegedly outdated sites prevented those courts from understanding that sharing is the essence of modern social media. Indeed, defendants and amici curiae on their behalf argue that, in the context of social media communications, there generally is no such thing as true privacy. Accordingly, they assert, even those social media communications configured by a user to be available to only specific friends or followers and that exhibit a "veneer of privacy" should nevertheless be treated as public. Defendants argue that such communications should not be protected by *section 2702(a)*—or that, alternatively, they should be deemed to fall within the lawful consent exception of *section 2702(b)(3)*.

Providers and amicus curiae Google LLC (Google) by contrast, assert that a registered user [****56] who configures a communication to be viewed by any number of friends or followers—but not by the public generally—evinces an intent *not* to consent to disclosure by a provider under *section 2702(b)(3)*, but instead to preserve some degree of privacy. They too [**747] rely on *Meregildo, supra, 883 F.Supp.2d 523, 525*, which observed that Facebook "postings using more secure privacy settings reflect the user's intent to preserve information as private." They also rely on *Ehling, supra, 961 F.Supp.2d at page 668*, which, as noted earlier, focused on whether a Facebook user "actively restrict[ed] the public from accessing the information" and found that when a user configures a communication to be available on only a limited basis and "inaccessible to [*1278] the general public," such a post is "'configured to be private' for purposes of the SCA." Under this authority, providers assert, a service provider remains prohibited from disclosing such communications. For reasons that follow, we agree with providers and Google on this point.

To begin with, we reject defendants' unsupported and rather startling assertion that social media communications and related technology fall categorically outside *section 2702(a)*'s general prohibition against disclosure by providers to "any person or entity."[32] Nor can we accept defendants'

---

[32] For similar reasons we reject a somewhat related alternative interpretation of that quoted phrase advanced by amici curiae on behalf of defendants, the California Public Defenders Association and the Public Defender of Ventura County. Asserting that the phrase "any person or entity" in *section 2702(a)* should be interpreted to exclude a court, amici curiae propose to interpret that phrase to permit providers to disclose any and all stored communications (no matter how configured) to a trial court for its in camera review—and then, presumably, for the trial court to release at least some of those private communications to defendants.

In support of their argument that a trial court does not qualify as a person or entity under the statute, amici curiae simply cite *Marbury v. Madison (1803) 5 U.S. 137 [2 L.Ed. 60]*. They argue that Congress must be presumed to have been aware of "existing law" (including *Pen. Code, § 1326*'s in camera review procedures) as well as the *Fifth* and *Sixth Amendment* rights of defendants—and hence, they postulate, Congress must have contemplated that such an exception for in camera and ex parte review by a trial court would be "read into the

interpretation [****57] of section 2702(b)(3)'s lawful consent exception, [***103] which would sweep far more broadly than was envisioned by Congress. The legislative history suggests that Congress intended to exclude from the scope of the lawful consent exception communications configured by the user to be accessible to only specified recipients. There is no indication in the legislative history of any intent to do otherwise in the case of communications sent by a user to a large number of recipients who, even in 1986 when the Act was adopted, could have shared such communications with others who were not intended by the original poster to be recipients.

In this respect, providers argue, defendants' view "would effectively eliminate expectations of privacy in *all* communications" and hence "would undermine the privacy rights of all users, including those of criminal suspects and defendants. If the SCA excluded electronic communications that are [*1279] made to ['large'] groups of people, then it would necessarily place no restriction on private party or *law enforcement* access to such communications. And if people had no reasonable expectation of privacy in communications sent through and maintained by the intermediary, simply because those [****58] communications could be later shared by their recipients, that would remove all Fourth Amendment protections for communications as well." Providers assert there is no indication that Congress contemplated such a result.[33]

[**748] As observed *ante*, part II.C., the House Judiciary Committee suggested, in its discussion of *access* rules, an understanding that a user's configuration would "establish an objective standard" to determine privacy protection. (House Rep., *supra*, at p. 41.) When subsequently addressing the *disclosure* rules—and the lawful consent exception to those rules—the House committee stressed that a user's consent to disclosure could be implied in view of, among other things, providers' available published policies. (House Rep., *supra*, at p. 66.) Providers' posted policies and answers to frequently asked questions (FAQs), described below, are readily available, and they appear to shed light on the issues presented in this litigation. Although we will highlight and quote some of these available policies and FAQs, we emphasize that in doing so we do not preclude any party from advancing any additional point or argument—including the legal significance that should or should not be accorded such policies and FAQs.

The policies and [****59] FAQs warn registered users that a communication configured as public will generally become, in the words of the House Report, *supra*, at page 62, "readily accessible to the general public," [***104] and available to *any* person via the Internet, whether that person is registered with the social media provider, or not.[34] This widespread availability of public posts on the [*1280] Internet is the result of providers' business model, which allows and facilitates crawling and indexing by search engines (and in some instances, use of a so-called firehose stream) that generate search results lists displaying a link to the user's current social

---

Act" by the courts, "when and if," as here, "the need arises." Amici curiae add that "Congress … knows that the courts are the forum where controversies such as the one here will be resolved and that the courts will determine their own procedures"—including amici curiae's contemplated compelled compliance with in camera review by the trial court. Finally, amici curiae assert that to the extent the Act "is interpreted to prohibit [in camera] judicial assessment of the exculpatory significance of the subpoenaed records," the SCA, as applied in this case, violates defendants' Fifth and Sixth Amendment rights, and hence is unconstitutional. Putting aside the constitutional claim, neither the statutory language nor its legislative history supports amici curiae's claim that the statute can reasonably be interpreted to permit disclosure of all electronic communications, private or public, to a court under all circumstances.

[33] Moreover, as amicus curiae Google notes, if defendants' "premise were correct, a communication shared with only one person would be equally public because a single recipient could share a private communication with the world (and some recipients do). … The ability to share an electronic communication accordingly cannot be the basis for removing privacy protections from content posted with less-than-public privacy settings."

[34] See, e.g., Twitter, Privacy Policy, Information [****60] Collection and Use/Tweets, Following, Lists, Profile, and Other Public Information <http://twitter.com/privacy> (as of May 22, 2018) (the service "broadly and instantly disseminates your public information to a wide range of users, customers, and services, including search engines"); Facebook Help Center, Appearing in Search Engine Results <https://www.facebook.com/help/392235220834308> (as of May 22, 2018); Facebook Help Center, What is public information? <https://www.facebook.com/help/203805466323736?helpref=faq_content> (as of May 22, 2018); Instagram Help Center, Controlling Your Visibility <https://help.instagram.com/116024195217477> (as of May 22, 2018). All Internet citations in this opinion are archived by year, docket number and case name at <http://www.courts.ca.gov/38324.htm>.

media page, a title and a snippet of text.[35] In other words, when, for example, a Facebook user configures a post as public, that communication becomes both (a) available to all two billion registered Facebook users, and (b) again in the words of the House Report, "readily accessible to the general public" via crawling by search engines. (House Rep., *supra*, at p. 62.) The result is that, as counsel for providers conceded at oral argument, a public communication is available to "everyone in the world"—even to those who are not registered Facebook users, but who have open access to the Internet.

Providers' FAQs warn that even communications configured as restricted still might be shared by an authorized recipient with anyone else.[36] At the [*1281] same time, nothing of [**749] which we are aware in any of providers' policies or answers to FAQs suggests that users would have any reason to expect that, having configured a communication to be available not to the public but [***105] instead to a restricted group of friends or followers, the user nevertheless has made a *public* communication—and hence has impliedly consented to disclosure by a service provider, just as if the configuration had been public.

**(6)** For all of these reasons we reject defendants' proposed broad interpretation of the lawful consent

---

[35] See, e.g., Google Search, How Search organizes information <https://www.google.com/insidesearch/howsearchworks/crawling-indexing.html> (as of May 22, 2018); Google Search Console Help, Create good titles and snippets in Search Results <https://support.google.com/webmasters/answer/35624?hl=en> (as of May 22, 2018). Regarding Twitter's firehose stream, see, e.g., Financial Times Lexicon, Definition of Twitter fire hose <http://lexicon.ft.com/Term?term=Twitter-fire-hose> (as of May 22, 2018).

In addition, the three largest search engines—Google, Bing, and Yahoo!—also display in their results a link to a cached version of the social media user's page. (See, e.g., Google, Search Help, View webpages cached in Google Search Results <https://support.google.com/websearch/answer/1687222?hl=en> [as of May 22, 2018].) Google explains that "[c]ached links show you what a web page looked like the last time Google visited it" and that "Google takes a snapshot of each web page as a backup in case the current page isn't available. … If you click on a link that says 'Cached,' you'll see the version of the site that Google stored." (*Ibid*.)

[36] Even with regard to communications that a user configures—either initially when sent, or subsequently as reconfigured—to be available to only a defined group (such as followers or friends), any such restriction operates only within the confines of the service and the licensing agreements under which other entities interact with the provider. Providers are generally careful to avoid describing the effect of privacy configuration more broadly. (See, e.g., Facebook Help Center, When someone re-shares something I posted, who can see it? <https://www.facebook.com/help/569567333138410> [as of May 22, 2018] ["When someone clicks Share below your post, they aren't able to share your photos, videos or status updates *through Facebook* with *people who weren't in the audience you originally selected to share with*" (italics added, boldface omitted)].)

Accordingly, when a user configures a post to be available to only specifically listed persons, the provider will be able to honor that user's choice only *within the service*—by disabling those recipients from, in turn, sharing that communication with others within the system through the system's sharing tools. Moreover, all three providers warn users that such configuration protection within each system does not prevent any authorized recipient from employing mechanisms outside the system to copy any post (by, for example, downloading or creating a screenshot) and then sharing the communication with anyone on the Internet. (See, e.g., Twitter, About public and protected Tweets/Who can see my Tweets? <https://support.twitter.com/articles/14016> [as of May 22, 2018] ["Keep in mind that when you choose to share content on Twitter with others, this content may be downloaded or shared"].) Indeed, as Twitter advises, even when a user protects communications by restricting them to specific persons, that user's communications might nevertheless be shared by any such person with anyone else. (Twitter Help Center, Twitter Privacy Policy/Information Collection and Use/Direct Messages and Non-Public Communications <https://twitter.com/privacy?lang=en> [as of May 22, 2018] ["When you use features like Direct Messages to communicate privately, please remember that recipients may copy, store, and re-share the contents of your communications"]; see also Facebook, Data Policy/How is this information shared?/Sharing our Services/People you share and communicate with <https://www.facebook.com/policy.php> [as of May 22, 2018] ["people you share and communicate with may download or re-share this content with others on and off our Services"]; Instagram, Privacy Policy/3. Sharing of your information/Parties with whom you may choose to share your User Content <https://help.instagram.com/155833707900388> [as of May 22, 2018] ["Once you have shared User Content or made it public, that User Content may be re-shared by others. … [¶] If you remove information that you posted to the Service, copies may remain viewable in cached and archived pages of the Service, or if other Users or third parties using the Instagram API [application programming interface] have copied or saved that information."].)

exception. We hold that implied consent to disclosure by a provider is not established merely because a communication was configured by the user to be accessible to a "large group" of friends or followers.[37] [*1282]

C. *Providers' Argument That Section 2702 Affords a Provider Discretion To Decline To Comply with a Valid State Subpoena*

Providers contend [****61] that to the extent section 2702(b)(3)'s lawful consent exception [***106] applies to any of the communications at issue here, that provision simply *authorizes* them to comply with the subpoenas, but does not by itself *compel* them to comply with the subpoenas. They further assert that section 2702(b) affords providers who are authorized to disclose, the "discretion" to refuse to do [**750] so—even in the face of an otherwise proper subpoena lawfully issued under state law. We agree with the first proposition, [****62] but not with the second.

**(7)** As observed earlier, section 2702(a) sets out a general prohibition against disclosure of communications by a service provider; and section 2702(b) lists exceptions under which a provider "may" disclose such communications—including, in subsection (3), communications regarding which a user has lawfully consented to disclosure. As the parties have conceded, such consent is applicable when a user posts a communication configured to be public. Plainly, section 2702(b) merely permits a provider to disclose, and it does not by itself impose a duty or obligation to disclose. Yet providers maintain that by use of the word "may," the section also operates to "ensure that providers would retain the discretion to choose whether to disclose content based on a user's consent"—even in the face of a lawful subpoena. In support, they rely on language in an order by a federal magistrate judge, in In re Facebook, Inc. (N.D.Cal. 2012) 923 F.Supp.2d 1204, 1206, stating that although "consent may *permit* production by a provider, it may not *require* such a production." (Original italics, boldface omitted.) Providers also rely on United States v. Rodgers (1983) 461 U.S. 677, 706 [76 L. Ed. 2d 236, 103 S. Ct. 2132], cited in footnote 7 of the order, for the general proposition that "[t]he word 'may,' when used in a statute, usually implies some degree of discretion."

As explained [****63] below, a California Court of Appeal decision, Negro v. Superior Court (2014) 230 Cal.App.4th 879 [179 Cal. Rptr. 3d 215] (*Negro*), has thoroughly considered and rejected providers' argument. In that litigation, the plaintiff sued multiple defendants concerning business transactions. Prior to trial, the plaintiff subpoenaed defendant Negro's e-mail service provider, Google, seeking e-mail communications between him, his codefendants, and others. Defendant Negro eventually expressly consented to disclosure by Google of e-mails between himself and specific persons and entities covering a defined range of dates. But despite its user's express consent, Google refused to comply with the civil subpoena. On review, the Court of Appeal considered and applied section 2702(b)(3)'s lawful consent exception, ultimately finding that the defendant had given his express and enforceable [*1283] written consent to service provider Google's disclosure of his e-mails. (Negro, at pp. 893–899.) Having found the lawful consent exception satisfied, the appellate court further concluded that the subpoena was itself enforceable and that Google was required to comply with it. In the process, the court carefully considered and rejected the contention that providers raise now—that the statute empowers providers to defy subpoenas [****64] seeking communications that are exempted from section 2702's prohibition on disclosure under the section's lawful consent exception. (Negro, at pp. 899–904.) Because

---

[37] At the same time, we do not endorse the view, expressed by counsel for providers at oral argument, that if it were *possible* for a registered Facebook user to restrict a communication to "only" all of the other *two billion* Facebook users, such a communication would not qualify as public under the Act. To our knowledge, no case has endorsed that view and on its face the claim seems rather questionable, particularly inasmuch as Facebook does not generally limit who may join its social media platform. In this regard, we note that what is public under the SCA is not defined by what a social media provider labels as "public."

Nor are we aware of any prior case involving a user who has placed minimal restrictions on a communication within a large social media service (as another hypothetical example, a user who might disseminate a communication to all two billion Facebook users except for one or two people). Although we hold that limiting a communication to a "large group" does not render a post public, and acknowledge that on remand the trial court might find that the public configurations at issue in this case render the resulting communications public under the SCA, we also observe that neither the hypothetical discussed at oral argument nor this additional hypothetical involving minimal restrictions is presented in this case. Therefore, we need not and do not resolve whether such communications would be sufficiently public to imply consent to disclosure under section 2702(b)(3).

we find the *Negro* court's reasoning persuasive, we quote that decision's analysis at some length.

As an initial matter, the court in *Negro, supra, 230 Cal.App.4th 879*, rejected the claim that the SCA confers "a blanket exemption or immunity [***107] on service providers against compulsory civil discovery process." (*Negro, at p. 899*.) The court acknowledged that the SCA does not, on its face, contain any exception for or mention of civil (or for that matter criminal) discovery subpoenas. But the court explained that the Act's failure to expressly include such subpoenas does not "suggest that it rendered" the normal state law "discovery process impotent in all circumstances." (*Negro, at p. 899*.)[38]

[**751] Turning to the same argument reprised by providers here, the court in *Negro* addressed Google's assertion "that the language of the Act makes the consent exception 'permissive' and the provider's disclosure under it 'voluntary' … so that 'Google may not be compelled by an order issued in a civil proceeding to disclose content, even with the user's consent.'" (*Negro, supra, 230 Cal.App.4th at p. 900*.) The appellate court observed that [****65] Google relied on *section 2702(b)*'s "use of the word 'may' to frame the exception for disclosure based on a user's consent," and on the passage quoted above from the federal magistrate's order in *In re Facebook, Inc., supra, 923 F.Supp.2d at page 1206*. (*Negro, at p. 900*.) The court determined that the magistrate's reasoning "places much more weight on a very small word than it is designed to bear. It is certainly true that 'may' generally conveys permission, and that when used in contradistinction to 'shall' it implies a discretionary power or privilege, as distinguished from a mandatory duty. [Citations.]" (*Id., at p. 901*.) But, the court reasoned, "The subdivision where 'may' appears is framed not as a grant of discretionary power or as the imposition of a [*1284] mandatory duty but as a special exception to a general prohibition. In such a context all 'may' means is that the actor is excused from the duty, liability, or disability otherwise imposed by the prohibition. Stating that the actor 'may' engage in the otherwise proscribed conduct is a natural way—indeed the most natural way—to express such an exception." (*Id., at p. 902*, Original italics.)

The appellate court in *Negro* continued: "Another federal magistrate judge has observed that 'there should be a clear expression of congressional [****66] intent before relevant information essential to the fair resolution of a lawsuit will be deemed absolutely and categorically exempt from discovery and not subject to the powers of the court under [rules governing disclosure].' [Citation.] Congress's use of the word 'may' to frame an exception to the Act's general prohibition on disclosure is not such a 'clear expression of … intent' as will justify a reading of the Act that categorically immunizes service providers against compulsory civil process where the disclosure sought is excepted on other grounds from the protections afforded by the Act." (*Negro, supra, 230 Cal.App.4th at p. 902*.)

[***108] Finally, the appellate court concluded: "In sum, we find no sound basis for the proposition that the Act empowers service providers to defy civil subpoenas seeking discovery of materials that are excepted from the Act's prohibitions on disclosure. Insofar as the Act permits a given disclosure, it permits a court to compel that disclosure under state law." (*Negro, supra, 230 Cal.App.4th at p. 904*.) Accordingly, the court held that in light of the fact that the user/defendant had consented to disclosure by the service provider, "the Act does not prevent enforcement of a subpoena seeking materials in conformity with the consent [****67] given." (*Ibid*.)

Providers do not directly address the logic or substance of the *Negro* court's analysis quoted above. Instead, they assert, first, that the appellate court's decision is distinguishable because the underlying lawful consent in that case was express, whereas the present case concerns implied consent. This attempt to avoid *Negro*'s analysis ignores the legislative history described *ante*, part II.C., disclosing that Congress specifically contemplated that *implied* lawful consent would satisfy the lawful consent exception. It also is in tension with providers' own concession that implied lawful consent is effective with regard to communications configured by a registered user to be public. (See *ante*, pt. III.A.)

---

[38] The court continued: "Nor do we … perceive anything in the language of the Act suggesting that Congress intended to grant service providers a blanket immunity from obligations imposed by discovery laws. The Act does not declare civil subpoenas unenforceable; *it does not mention them at all*. As we have said, it preempts state discovery laws insofar as they would otherwise compel a service provider to violate the Act. It is this preemption that excuses service providers from complying with process seeking disclosures forbidden by the Act. But nothing in the Act suggests that service providers remain shielded from state discovery laws when the disclosures sought are not forbidden by the Act." (*Negro, supra, 230 Cal.App.4th at p. 900*, fn. omitted, first italics added, subsequent in original.)

Alternatively, providers suggest that the SCA should be interpreted to bar the enforcement of any state subpoena that directs service providers to divulge public communications *that the Act permits but does not require them to disclose*. They assert that *Negro*'s contrary analysis and conclusion must be [*1285] wrong because "it would permit a state subpoena to compel disclosure of content where the SCA itself does not. Such an expansion would weaken the protections of the SCA [****68] and impermissibly broaden federal law. It would thereby conflict with the SCA's comprehensive scheme of regulating the circumstances [**752] under which the disclosure of content is permissible or required."

**(8)** In this respect providers implicitly rely on the fact that section 2703 lists circumstances in which a provider is compelled to disclose to governmental entities—and yet, as the *Negro* court observed, the Act, although preempting state discovery laws that would compel a provider to violate the federal statute, "does not mention" civil (or criminal) subpoenas issued by nongovernmental entities in that section or indeed at all. (*Negro, supra, 230 Cal.App.4th at p. 900*; see *ante*, fn. 38.) Consistently with *Negro*'s analysis, we believe that if Congress intended to preclude a state from enforcing a nongovernmental entity's civil or criminal subpoena that is lawful under state law (and as to which the federal statute does not preclude disclosure), such a prohibition would have been made clear in the Act. We find no intent by Congress to preempt state law in this setting. [39]

D. *Additional Issues Raised in the Supplemental Briefs, Some of Which Should Be Explored and Resolved on Remand to the Trial Court*

Having addressed the legal issues that [****69] can be decided on the present record, we turn to other matters raised in providers' briefs that cannot be resolved at this stage—and some of which must await exploration on remand.

[***109] 1. *Providers' assertion that most of the communications at issue are private and hence the lawful consent exception will not assist defendants*

As observed earlier, the subpoenas in this case broadly seek "[a]ny and all public and private content." Providers in their supplemental briefs assert variously that "much" or "most" (or all except a "small subset") of the communications sought by the subpoenas were configured by the users to be private or restricted, not public, and hence the lawful consent exception generally will not assist defendants in this case. Because the parties did not acknowledge the relevance and applicability of the lawful consent exception in the trial court, no reliable record was made concerning either registered [*1286] user's configuration of the social media communications at issue here.[40]

---

[39] To the extent dictum in *Johnson, supra, 538 S.W.3d 32*, is inconsistent (see *ante*, fn. 30), we disagree with its approach and analysis.

[40] At the time relevant in this case, it appears that each provider's default setting for registered users was public, meaning that unless the user configured communications to be private, they were public. (Regarding Twitter, see Twitter Privacy Policy/Information Collection and Use/Tweets, Following, Lists, Profile, and other Public Information <*http://twitter.com/privacy*> [as of May 22, 2018]; regarding Facebook, see Electronic Frontier Foundation, *Facebook's Eroding Privacy Policy: A Timeline* (Apr. 28, 2010) <*https://www.eff.org/deeplinks/2010/04/facebook-timeline*> [as of May 22, 2018] [observing that in Nov. 2009, Facebook reset user privacy default settings to public]; see also Facebook Newsroom, *Making It Easier to Share With Who You Want* (May 22, 2014) <*http://newsroom.fb.com/news/2014/05/making-it-easier-to-share-with-who-you-want/*> [as of May 22, 2018] [noting that in mid-2014—well after most of the communications at issue in this litigation were sent—Facebook again changed its privacy policy default, reverting, for new users, from public to friends, and giving existing users new tools to help ensure that they post publicly only when they intend to do so]; regarding Instagram, see Instagram Help Center, Controlling Your Visibility/Setting Your Photos and Videos to Private <*https://help.instagram.com/116024195217477*> [as of May 22, 2018].)

From what we can glean from the record, it appears that Renesha Lee may not have changed the default on one of her Twitter accounts and made her tweets and/or any replies private. (See *ante*, pt. I.D. and related discussion.) The record does not address the configuration of Renesha Lee's Facebook communications. Finally, regarding Instagram, the record suggests that Renesha may have configured one Instagram account to be private. In addition, the record suggests that she may have had, and deleted, multiple additional accounts with some or all of the social media providers. The configurations of these additional accounts are unknown. (See *ante*, fn. 5.) Regarding victim Rice, the limited record suggests that he had accounts, perhaps multiple, and of unknown configuration, with Facebook and Instagram—and that some if not all of those accounts (including at least one relied upon by the prosecution's gang expert) have been

Moreover, as noted earlier, it is not apparent that the trial court had sufficient information to fully assess defendants' need for discovery when it denied providers' motions to quash and allowed defendants [****70] discovery on a novel constitutional theory.

[**753] 2. *Providers' assertion that lawful consent to disclosure is revoked by a user's reconfiguration of a communication from public to restricted or by a user's deletion of a public communication*

As noted, providers concede that they may, pursuant to the lawful consent exception set forth in 2702(b)(3), disclose a post configured by the user to be public. They maintain, however, that the fact a user may have *initially* configured a post for public distribution should not necessarily resolve the question of the applicability of the lawful consent exception. Specifically, providers observe that a communication originally configured to be public subsequently can be reconfigured by the user to [***110] be restricted, can be deleted by the user, or the user can close the account.[41] They argue that when such a [*1287] change occurs before a provider is served with a subpoena, the reconfiguration [****71] or deletion should be understood as a revocation of lawful consent for purposes of section 2702(b)(3)—with the result that the provider would be prohibited by section 2702(a) from complying with a subpoena regarding any such communication.[42]

Defendants, by contrast, insist that once a registered social media user configures a communication as public and posts it, triggering section 2702(b)(3)'s lawful consent exception and presumptively allowing disclosure by a provider, the user cannot subsequently revoke that implied consent to disclosure, even if the user promptly reconfigures any post as restricted or deletes the post or closes the account. In support, defendants assert that "any reasonable user knows once you make information publicly available on social media it will be '… broadly and instantly disseminate[d]' … 'to a wide range of [****72] users, customers, and services, including search engines, developers, and publishers …' just as Twitter advises in its terms of service."[43] Defendants assert that after a public communication has been made so widely available, "[r]evoking consent is as possible as un-ringing a bell." [*1288]

The parties have cited no decision explicitly addressing whether reconfiguration, deletion or account closure operates to revoke consent for purposes of section 2702(b)(3), nor have we found any such [***111] case. It appears that providers' revocation claim poses a question of first impression.

---

closed. (*Ibid*.)

[41] In this regard Facebook tells users: "If you accidentally share a post with the wrong audience, you can always change it." (Facebook, Privacy Basics/Manage Your Privacy <https://www.facebook.com/about/basics/manage-your-privacy/posts#6> [as of May 22, 2018]; see also Facebook Help Center, How can I adjust my privacy settings? <https://www.facebook.com/help/193677450678703?helpref=related> [as of May 22, 2018] ["You can view and adjust your privacy settings at any time"].) Twitter allows an account to be changed from unprotected to protected and vice versa, and states: "If you at one time had public Tweets (before protecting your Tweets), those Tweets will no longer be public on Twitter, or appear in public Twitter search results [within the provider's system]. Instead, your Tweets will only be viewable and searchable on Twitter by you and your followers." (Twitter Help Center, About public and protected Tweets/What happens when I change my Tweets from public to protected? <https://support.twitter.com/articles/14016#> [as of May 22, 2018].) At the same time, Twitter explains, the opposite also occurs: "If you later change your account settings to no longer protect your Tweets, Tweets that were previously protected will become public and may be indexed by third-party search engines." (Twitter Help Center, Why are my Tweets appearing on Google after deleting or protecting them?/Protected Tweets <https://support.twitter.com/articles/15349#> [as of May 22, 2018].) Finally, Instagram also allows an account to be changed from the default (public) to private, and vice versa. (Instagram Help Center, Privacy Settings & Information/Privacy settings/How do I set my photos and videos to private so that only approved followers can see them? <https://help.instagram.com/196883487377501/?helpref=hc_fnav> [as of May 22, 2018].)

[42] Amicus curiae Google hypothesizes that any given communication originally configured as public, or any subsequent reverse reconfiguration of a communication from restricted to public, might conceivably be undertaken *not* by a registered user him—or herself, but by a person or entity who uses or hacks the user's account. Any such action, Google argues, should be viewed as not constituting implied consent to disclosure by a provider. We agree, and observe that the trial court on remand will be in a position to permit providers to attempt to establish, as a preliminary matter, that a given communication was configured, reconfigured, or deleted, by someone *other than* the registered account owner without authority of the owner.

[43] See *ante*, footnote 34.

[**754] Providers may be understood to invoke Congress's intent to protect users' privacy (as described *ante*, pt. II.A.), and to suggest that their proposed interpretation—under which a provider would be required to honor a user's reconfiguration or deletion so long as it was undertaken by the time a subpoena is issued—would afford greater protection to that privacy interest.[44] Defendants, on the other hand, question whether a social media user's reconfiguration or deletion of a public post can in reality effectuate a revocation of consent to disclosure[45]—and whether Congress intended to [*1289] ensure revocability of consent in this context. Because the [****73] record does not indicate whether, in fact, any public communication sought by defendants was subsequently reconfigured or deleted before the relevant underlying subpoena was issued, we express no opinion on the revocation of consent issue—and leave it to be explored, if necessary, by the trial court on remand.

[***112] 3. *Technical difficulties that providers may face in determining the applicable privacy configuration and retrieving deleted communications—and protecting providers from excessive burdens*

Providers assert that in light of a registered user's ability to reconfigure communications, "providers may not easily be able to determine the intended audience of a communication at any given point in time" and "it may be difficult for a provider to accurately identify" whether a given communication when posted was public or restricted. Likewise, [****74] speaking on providers' behalf, amicus curiae Google avers: "Providers do not routinely maintain records of past privacy settings for each post or message. Lacking such records, it would be *impossible* to determine the privacy configuration that applied when a communication was posted or sent." (Italics added.) Providers also assert that "if a user changes the privacy setting for a communication, a service may not be able to accurately [**755] determine prior privacy settings." In addition, providers assert it would be difficult for them to retrieve deleted communications. As noted by the trial court, however, a subpoena recipient has a general obligation to undertake reasonable efforts to locate responsive materials. Again, any technical difficulties a given

---

[44] In support providers cite *Van Patten v. Vertical Fitness Group, LLC (9th Cir. 2017) 847 F.3d 1037, 1047*, which notes the "common law principle that consent is revocable." (Accord, *Neder v. United States (1999) 527 U.S. 1, 21 [144 L. Ed. 2d 35, 119 S. Ct. 1827]* ["'"[W]here Congress uses terms that have accumulated settled meaning under … the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms"'"]; *Osorio v. State Farm Bank, F.S.B. (11th Cir. 2014) 746 F.3d 1242, 1253* [quoting a dictionary for the proposition that "'[u]nder the common law understanding of consent, the basic premise of consent is that it is "given voluntarily,"'" and quoting *Rest.2d Torts, § 892* for the proposition that "'"Consent is a willingness in fact for conduct to occur"'" and that "'"[C]onsent is terminated when the actor knows or has reason to know that the other is no longer willing for him to continue the particular conduct"'"]; see also *State v. Brown (2010) 348 Ore. 293 [232 P.3d 962, 967]* ["[A] person who places an item in plain view has relinquished any constitutionally protected privacy interest in the item. That person, however, may renew the privacy interest simply by removing the item from plain view."].)

[45] In this regard, providers warn users, the acts of reconfiguration or deletion (or even account closure) do not reach outside the provider's system and prevent third parties that may have indexed and cached any communication from continuing to make a given communication available in its prior form to anyone on the Internet. For example, Facebook notes that in that situation it has no "control over content that has already been indexed and cached in search engines" and it offers the same advice as do Instagram and Twitter to their own registered users: In order to "request the immediate removal of [a particular] search listing, you will have to contact the specific search engine's support team." (Facebook Help Center, Appearing in Search Engine Results/I'm showing up in the results of other search engines even though I've chosen not to <*https://www.facebook.com/help/392235220834308/?helpref=hc_fnav*> [as of May 22, 2018].) And yet even if a user identifies each search engine that displays the communication and seeks expedited recognition of any reconfiguration or deletion, providers indicate that the most that can be said is that any given search engine will "eventually index updated … information" to reflect any reconfiguration protection or post deletion. (Twitter Help Center, Why are my Tweets appearing on Google after deleting or protecting them?/How and when to send Google a request to remove information <*https://support.twitter.com/articles/15349#*> [as of May 22, 2018].) Indeed, Instagram observes that there is no such thing as immediate reconfiguration or deletion of a public communication that has become available on a search engine; instead, "[i]t may take some time for these [other third party search engine] sites and Google to re-index and remove" a given communication "even if you delete your account." (Instagram Help Center, Controlling Your Visibility/Instagram Privacy on the Web/How can I remove my images from Google search <*https://help.instagram.com/116024195217477*> [as of May 22, 2018].)

provider may face in determining the relevant history of a particular communication, or retrieving any deleted communication, are matters to be explored at the anticipated hearing on remand.

Providers similarly urge that they should be protected from excessive burdens. As observed *ante*, part II.A., Congress articulated its main purposes in enacting the SCA: affording privacy protections to users while accommodating the legitimate needs of [****75] law enforcement. It also articulated a tertiary goal: to avoid discouraging the use and development of new technologies. Providers' briefs characterize this additional purpose as one of "enhanc[ing] the use of communications services and protect[ing] providers from being embroiled as a nonparty in litigation." Amicus curiae on providers' behalf, Google, characterizes this additional purpose even more specifically as "protecting providers from an otherwise limitless burden of responding to requests to disclose their users' communications." Providers rely on dictum in [*1290] *O'Grady, supra, 139 Cal.App.4th 1423*, in which the court voiced concern about the prospect of such subpoenas to providers in routine civil cases. (*Id., at pp. 1445–1447*.)[46]

**(9)** In light of the statutory scheme, it appears that Congress sought to limit burdens placed on service providers by various means—most obviously, by establishing broad prohibitions and specific exceptions regarding access and disclosure under *sections 2701* and *2702*, along with rules and procedures pursuant to which the government may compel disclosure under *section 2703*. With regard to burdens related to disclosure in particular, Congress significantly limited the potential onus on providers by establishing a scheme under which a provider is effectively [****76] prohibited from complying with a subpoena issued by a nongovernmental [***113] entity—*except* in specified circumstances. But when any one of the exceptions does apply, there is no indication that Congress intended that providers would be categorically relieved from the burden of compliance with an otherwise lawful civil or criminal subpoena. Hence, as the court held in *Negro, supra, 230 Cal.App.4th 879*, a provider may properly be subject to the burden of compliance with a subpoena, even with respect to communications configured by the registered user to be *private*, when a user expressly consents to disclosure by his or her service provider. Likewise, a provider may properly be subject to the burden of compliance with a subpoena when a user implicitly consents to disclosure by configuring a social media communication as *public*.

Of course, any third party or entity—including a social media provider—may defend against a criminal subpoena by establishing that, for example, the proponents can obtain the same information by other means, or that the burden on the third party is not justified under the circumstances. (*City of Alhambra v. Superior Court (1988) 205 Cal.App.3d 1118, 1134 [252 Cal. Rptr. 789]*; cf. *Kling v. Superior Court (2010) 50 Cal.4th 1068, 1074–1075, 1078 [116 Cal. Rptr. 3d 217, 239 P.3d 670]*.) Indeed, the Act itself specifically contemplates that providers may raise such issues in the context of [****77] compelled disclosure to a governmental entity under *section 2703(d)* (a court "may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider"), and the same principles would apply in the present setting.

As noted, providers advanced similar arguments regarding the burden of compliance with the subpoenas in the earlier trial court proceeding. (*Ante*, [*1291] pt. I.E.) In response, the [**756] trial court ruled that absent additional factual information demonstrating impossibility or the extent of burdens, it could not engage in any such balancing of production versus burden. Providers' current claim of undue burden can properly be addressed by the trial court on remand.[47]

---

[46] In a related vein, providers observe that they stand in jeopardy of incurring civil liability under *section 2707* of the Act if they knowingly or intentionally violate the SCA. But that section by its terms contemplates liability only for a provider that violates the Act "with a knowing or intentional state of mind." (*§ 2707(a)*.) Moreover, the statute provides a safe harbor for a provider that, in "good faith," relies on "a court … order." (*§ 2707(e)(1)*.)

[47] The trial court on remand might also consider two additional and somewhat related legal issues that have been only generally alluded to in the briefing to date in this case, but which are highlighted in our January 17, 2018 order granting review in the related matter of *Facebook, Inc., v. Superior Court (2017) 15 Cal.App.5th 729 [223 Cal. Rptr. 3d 660]*, review granted January 17, 2018, S245203. That order directs the parties to address, among other things (1) whether a trial court may compel a witness to consent [****78] to disclosure by a provider, subject to in camera review and any appropriate protective or limiting conditions; and (2) whether a trial court may compel the prosecution to issue a search warrant under the Act, on behalf of a defendant.

[***114] **IV. CONCLUSION** [****79] **AND DISPOSITION**

We vacate the Court of Appeal's decision and direct that court to remand the matter to the trial court for proceedings consistent with this opinion.

Chin, J., Corrigan, J., Liu, J., Cuéllar, J., Kruger, J., and Yegan, J.,* concurred.

---

End of Document

---

Finally, yet another matter, not discussed in the parties' briefs, may require consideration on remand. As alluded to *ante*, part I.F., after the trial court confirmed its production ruling, counsel for defendant Sullivan asked that providers be ordered to preserve all data at issue in this case. The court stated that it would not immediately issue an oral preservation order because it wanted the parties to first work out among themselves language addressing providers' preservation obligations, and stated: "You will have to draft something and submit it, and see if you can reach an agreement. And if you get competing orders, we will have to have another hearing about that." The record before us, however, contains no preservation order; no mention of such an order appears in the briefs; and the superior court docket for each case, as to which we have taken judicial notice, reflects no such order. (See, e.g., *Williams v. Russ (2008) 167 Cal.App.4th 1215, 1223 [84 Cal. Rptr. 3d 813]* [addressing a party's "failure to preserve evidence for another's use in pending or future litigation" and corresponding sanctions].)

* Associate Justice of the Court of Appeal, Second Appellate District, Division Six, assigned by Chief Justice pursuant to *article VI, section 6 of the California Constitution*.

# *Juror Number One v. Superior Court*

Court of Appeal of California, Third Appellate District

May 31, 2012, Opinion Filed

C067309

**Reporter**
206 Cal. App. 4th 854 *; 142 Cal. Rptr. 3d 151 **; 2012 Cal. App. LEXIS 642 ***; 95 A.L.R.6th 749; 2012 WL 1950184

JUROR NUMBER ONE, Petitioner, v. THE SUPERIOR COURT OF SACRAMENTO COUNTY, Respondent; DEMETRIUS ROYSTER et al., Real Parties in Interest.

**Subsequent History:** Stay granted by *Juror Number One v. S.C. (Royster), 2012 Cal. LEXIS 6827 (Cal., July 2, 2012)*

Review denied by, Stay dissolved by *Juror Number One v. S.C. (Royster), 2012 Cal. LEXIS 8208 (Cal., Aug. 22, 2012)*

**Prior History:** [***1] Petition for Writ of Prohibition, Superior Court of Sacramento County, No. 08F09791, Michael P. Kenny, Judge.

*Juror Number One v. S.C. (Royster), 2011 Cal. LEXIS 3367 (Cal., Mar. 30, 2011)*

**Disposition:** Petition denied, stay vacated.

## Case Summary

**Procedural Posture**
Respondent, the Sacramento County Superior Court, California, learned that a trial juror had posted items on his Facebook account concerning the trial while it was in progress. The trial court entered an order pursuant to the Stored Communications Act (SCA) requiring the juror to execute a consent form authorizing Facebook to release for in camera review all items he posted during the trial. The juror filed a petition for a writ of prohibition.

**Overview**
The court concluded that the SCA was not applicable to the order at issue, and that the juror failed to establish a violation of his constitutional or privacy rights. The juror provided the court with nothing as to the general nature or specific operations of Facebook. Without such facts, the court was unable to determine whether or to what extent the SCA was applicable to the information at issue. But even assuming the juror's posts were protected by the SCA, that protection would apply only as to attempts to compel Facebook to disclose the requested information. The question was not whether the trial court could compel Facebook to disclose the contents of the juror's posts but whether it could compel the juror to do so. If the trial court could compel the juror to produce the information, it could likewise compel him to consent to the disclosure by Facebook. Even if the juror had a privacy interest in his posts, that interest was not absolute. It had to be balanced against the rights of real parties in interest to a fair trial. The juror failed to establish the trial court exceeded its power to inquire into alleged juror misconduct.

**Outcome**
The juror's petition for a writ of prohibition was denied.

**Counsel:** The Rosenfeld Law Firm and Kenneth Rosenfeld for Petitioner.

No appearance for Respondent.

John K. Cotter, Michael Wise and Keith J. Staten for Real Parties in Interest.

**Judges:** Opinion by Hull, J., with Raye, P. J., concurring. Concurring opinion by Mauro, J.

**Opinion by:** Hull

## Opinion

[**153] **HULL, J.**—Following the conviction of real parties in interest for various offenses stemming from an assault, respondent court learned that one of the trial jurors, fictitiously named Juror Number One, had posted one or more items on his Facebook account concerning the trial while it was in progress, in violation of an admonition by the court. The court conducted a hearing at which Juror Number One and several other jurors were examined about this and other claimed instances of misconduct. Following the hearing, the court entered an order requiring Juror Number One to execute a consent form [*858] pursuant to the Stored Communications Act (SCA) (*18 U.S.C. § 2701 et seq.*) authorizing Facebook to release to the court for in camera review all items he posted during the trial.

Juror Number One [***2] filed a petition for writ of prohibition with this court seeking to bar respondent court from enforcing its order. He contends the order violates the SCA, the *Fourth* and *Fifth Amendments to the United States Constitution*, and his state and federal privacy rights.

**(1)** We conclude the SCA is not applicable to the order at issue here and Juror Number One has otherwise failed to establish a violation of constitutional or privacy rights. We therefore deny the petition.

FACTS AND PROCEEDINGS

Juror Number One was a juror in the trial of *People v. Christian*, Sacramento County Superior Court case No. 08F09791 (the criminal trial) in which the defendants, real parties in interest in this writ proceeding, were convicted of various offenses stemming from the beating of a young man on Halloween night in 2008.

[**154] The criminal trial commenced in April 2010, and the jury reached its verdicts approximately two months later, on June 25. On August 10, 2010, one of the trial jurors (Juror No. 5) submitted a declaration in which she stated, among other things, that, on or about May 18, 2010, Juror Number One had "posted comments about the evidence as it was being presented during the trial on his 'Facebook [***3] Wall,' inviting his 'friends' who have access to his 'Facebook' page to respond."

On September 17, 2010, respondent court conducted a hearing on this and other allegations of juror misconduct. Four jurors were examined, including Juror Number One and Juror No. 5. Juror No. 5 testified that she did not learn about the Facebook postings until after the trial. Juror Number One had invited her to be a Facebook "friend" and this gave her access to his postings on Facebook, including those during the trial. This is when she saw the post mentioned in her declaration. According to Juror No. 5, one person had responded to the post that he or she liked what Juror Number One had said.

Juror Number One admitted that he posted items on his Facebook account about the trial while it was in progress. However, he indicated those posts contained nothing about the case or the evidence but were merely indications that he was still on jury duty. Juror Number One acknowledged that on one occasion he posted that the case had been boring that day and he almost fell asleep. According to Juror Number One, this was the day they were going [*859] through phone records and he posted that he was listening to piles and piles [***4] of "Metro PCS records." Juror Number One testified that he posted something every other day on his Facebook account and later tried to delete some of his posts. He denied reading any responses he received from his "friends" to these postings.

The other two jurors who were examined by the court had nothing to contribute on this issue.

At the conclusion of the hearing, respondent court indicated there had been clear misconduct by Juror Number One, but the degree of such misconduct was

still at issue.

On October 7, 2010, counsel for real party in interest Demetrius Royster issued a subpoena to Facebook to produce "[a]ll postings for [Juror Number One] dated 3/01/2010 to 10/06/2010." Attached was an order from respondent court compelling Facebook to "release any and all information, including postings and comments for Facebook member [Juror Number One]."

Facebook moved to quash the subpoena, asserting disclosure of the requested information would violate the SCA. In its memorandum in support of the motion to quash, Facebook asserted the requested information can be obtained from Juror Number One himself inasmuch as he "owns and has access to his own Facebook account, and can disclose his Facebook postings [***5] without limitation."

On January 28, 2011, counsel for real party in interest Royster issued a subpoena to Juror Number One to produce "[a]ny and all documents provided to [him] by Facebook" and "[a]ny and all posts, comments, emails or other electronic communication sent or received via Facebook during the time [he was] a juror in the above-referenced matter."

On February 3, 2011, Juror Number One moved to quash the subpoena.

The following day, respondent court granted Juror Number One's motion to quash the subpoena based on overbreadth. However, the court also issued an order requiring Juror Number One to turn over [**155] to the court for in camera review all of his Facebook postings made during trial.

Juror Number One filed a petition with this court seeking to bar respondent court from enforcing its February 4, 2011, order. We summarily denied the petition. However, on March 30, 2011, the California Supreme Court granted review and transferred the matter back to us for further consideration. The high court also issued a temporary stay of respondent court's order.
[*860]

On April 5, 2011, we vacated our prior order denying the petition, issued an order to show cause to respondent court and ordered [***6] that the temporary stay remain in effect.

## DISCUSSION

**(2)** Congress passed the SCA as part of the Electronic Communications Privacy Act of 1986 (*Pub.L. No. 99-508 (Oct. 21, 1986) 100 Stat. 1848*) to fill a gap in the protections afforded by the *Fourth Amendment*. As one commentator observed: "The *Fourth Amendment* offers strong privacy protections for our homes in the physical world. Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime. When we use a computer network such as the Internet, however, a user does not have a physical 'home,' nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a 'virtual home,' in fact that 'home' is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private [***7] third parties and held far away on remote network servers." (Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It* (2004) *72 Geo. Wash. L.Rev. 1208, 1209–1210*, fns. omitted (Kerr).) The *Fourth Amendment* provides no protection for information voluntarily disclosed to a third party, such as an Internet service provider (ISP). (See *Smith v. Maryland (1979) 442 U.S. 735, 743–744 [61 L.Ed.2d 220, 229, 99 S. Ct. 2577]*; *United States v. Miller (1976) 425 U.S. 435, 443 [48 L.Ed.2d 71, 79, 96 S. Ct. 1619]*.)

**(3)** To remedy this situation, the SCA creates a set of *Fourth Amendment*-like protections that limit both the government's ability to compel ISP's to disclose customer information and the ISP's ability to voluntarily disclose it. (*Kerr, supra, 72 Geo. Wash. L.Rev. at pp. 1212–1213*.) "The [SCA] reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, [citation], the [SCA] protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." [***8] (*Thoefel v. Farey-Jones (9th Cir. 2003) 359 F.3d 1066, 1072–1073*.)

**(4)** The SCA addresses two classes of service providers, those providing electronic communication service (ECS) and those providing remote computing service (RCS). An ECS is "any service which provides

to users thereof [*861] the ability to send or receive wire or electronic communications." (18 U.S.C. § 2510(15); see 18 U.S.C. § 2711(1).) An RCS provides "computer storage or processing services by means of an electronic communications [**156] system." (18 U.S.C. § 2711(2).) Subject to certain conditions and exceptions, the SCA prohibits ECS's from knowingly divulging to any person or entity the contents of a communication while in "electronic storage" (18 U.S.C. § 2702(a)(1)) and prohibits RCS's from knowingly divulging the contents of any communication "which is carried or maintained on that service" (*id.*, § 2702(a)(2)). One exception is recognized where the customer or subscriber has given consent to the disclosure. (*Id.*, § 2702(b)(3).)

Any analysis of the SCA must be informed by the state of the technology that existed when the SCA was enacted. (Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications [***9] Act* (2010) 98 Geo. L.J. 1195, 1204 (Note).) "[C]omputer networking was in its infancy in 1986. Specifically, at the time Congress passed the SCA in the mid-1980s, 'personal users [had begun] subscribing to self-contained networks, such as Prodigy, CompuServe, and America Online,' and 'typically paid based on the amount of time they were connected to the network; unlike today's Internet users, few could afford to spend hours casually exploring the provider's network. After connecting to the network via a modem, users could download or send e-mail, post messages on a "bulletin board" service, or access information.' [Citation.] Notably, the SCA was enacted before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994." (*Crispin v. Christian Audigier, Inc. (C.D.Cal. 2010) 717 F.Supp.2d 965, 971, fn. 15* (*Crispin*), quoting Note, *supra, 98 Geo. L.J. at p. 1198*.) In light of rapid changes in computing technology since the enactment of the SCA, "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfactory results." (*Konop v. Hawaiian Airlines, Inc. (9th Cir. 2002) 302 F.3d 868, 874*.)

**(5)** Under [***10] the SCA, an ECS is prohibited from divulging "the contents of a communication while in electronic storage by that service." (18 U.S.C. § 2702(a)(1).) However, the term "electronic storage" has a limited definition under the SCA. It covers "(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." (18 U.S.C. § 2510(17).) Thus, only copies of electronic communications held by the ECS pending initial delivery to the addressee or held thereafter for backup purposes are protected. (*Thoefel v. Farey-Jones, supra, 359 F.3d at pp. 1075–1076*.)

**(6)** An RCS is prohibited from divulging the content of any electronic transmission that is carried or maintained on its service "solely for the [*862] 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." (18 U.S.C. § 2702(a)(2)(B).) Thus, if the service *is* [***11] authorized to access the customer's information for other purposes, such as to provide targeted advertising, SCA protection may be lost. (See *Note, supra, 98 Geo. L.J. at pp. 1212–1214*.)

In addition to protecting traditional electronic mail services and remote processing services, the courts have indicated the SCA was intended by Congress to protect electronic bulletin boards as well. " 'Computer bulletin boards generally offer both private electronic mail service and newsgroups. The latter is essentially [**157] email directed to the community at large, rather than a private recipient.' [Citation.] The term 'computer bulletin board' evokes the traditional cork-and-pin bulletin board on which people post messages, advertisements, or community news. [Citation.] Court precedent and legislative history establish that the SCA's definition of an ECS provider was intended to reach a private [bulletin board system]. [Citations.]" (*Crispin, supra, 717 F.Supp.2d at pp. 980–981*.) A private bulletin board system is essentially one with restricted access rather than one open to the public at large.

**(7)** In its order compelling consent to the release of Juror Number One's Facebook postings, respondent court cited *Moreno v. Hanford Sentinel, Inc. (2009) 172 Cal.App.4th 1125, 1130 [91 Cal. Rptr. 3d 858]*, [***12] for the proposition that the information covered by the order "was posted so that others might read it and that it was not private in any sense that relates to this inquiry." However, the MySpace posting at issue in *Moreno* was open to the public at large, not a select group of Facebook "friends" like the postings at issue here. A party does not forfeit SCA protection by making his communications available to a closed group, i.e., a private bulletin board. (*Crispin, supra, 717 F.Supp.2d at pp. 980–981*, fn. omitted.) Thus, respondent court's

rationale does not withstand scrutiny.

Juror Number One contends Facebook has been recognized as an ECS within the meaning of the SCA, citing *Crispin, supra, 717 F.Supp.2d 965*. In *Crispin*, the federal district court concluded Facebook and MySpace qualify as both ECS's and RCS's. The court provided the following description of those sites: "'Facebook and MySpace, Inc., are companies which provide social networking websites that allow users to send and receive messages, through posting on user-created "profile pages" or through private messaging services.' … Facebook's user-created profile page is known as [***13] the Facebook 'wall,' 'a space on each user's profile page that allows friends to post messages for the user to see.' These messages … 'can be viewed by anyone [*863] with access to the user's profile page, and are stored by Facebook so that they can be displayed on the Facebook website, not as an incident to their transmission to another place.' Similarly … MySpace has a profile page with a 'comments' feature that is identical to the Facebook wall." (*Id. at pp. 976–977*, fns. omitted.)

The court in *Crispin* concluded that, because Facebook and MySpace provide limited access to messages posted by users on the Facebook "wall" or the MySpace "comments" feature, there is no basis for distinguishing those features from a restricted access electronic bulletin board. There is also no basis for distinguishing the private messaging services provided by those companies from traditional Web-based e-mail. Hence, the court concluded Facebook and MySpace qualified as ECS's. (*Crispin, supra, 717 F.Supp.2d at pp. 981–982*.)

The court next considered whether messages posted on the Facebook wall are in "electronic storage" within the meaning of the SCA. As noted above, this requires either that the message [***14] is in temporary, intermediate storage awaiting delivery, or is in backup storage. Regarding the former, the court noted that messages posted to the Facebook wall are not in intermediate storage awaiting delivery to the recipient, because the wall itself is the recipient or final destination for the messages. (*Crispin, supra, 717 F.Supp.2d at pp. 988–989*.) Nevertheless, the court found the messages, once posted, are held for backup purposes. (*Id. at p. 989*.) In the alternative, [**158] the court concluded Facebook qualifies as an RCS with respect to posted messages held on the wall. (*Id. at p. 990*.)

Assuming *Crispin* was correctly decided, that case did not establish *as a matter of law* that Facebook is either an ECS or an RCS or that the postings to that service are protected by the SCA. The findings in *Crispin* were based on the stipulations and evidence presented by the parties in that case. The court noted that the parties "provided only minimal facts regarding the three third-party entities that were subpoenaed." (*Crispin, supra, 717 F.Supp.2d at p. 976*.) The parties cited the companies' home pages and Wikipedia as authority. (*Ibid.*)

Juror Number One has provided this court with nothing, either [***15] by way of the petition or the supporting documentation, as to the general nature or specific operations of Facebook. Without such facts, we are unable to determine whether or to what extent the SCA is applicable to the information at issue in this case. For example, we have no information as to the terms of any agreement between Facebook and Juror Number One that might provide for a waiver of privacy rights in exchange for free social networking services. Nor do we have any information about how widely Juror Number One's posts are available to the public.
[*864]

But even assuming Juror Number One's Facebook postings are protected by the SCA, that protection applies only as to attempts by the court or real parties in interest to compel Facebook to disclose the requested information. Here, the compulsion is on Juror Number One, not Facebook.

In *Flagg v. City of Detroit (E.D.Mich. 2008) 252 F.R.D. 346* (*Flagg*), the plaintiff issued subpoenas for text messages held by SkyTel, Inc., a text messaging service that had contracted with the city to provide such services until 2004 and had maintained the messages thereafter. The city moved to quash the subpoena, arguing the messages were protected by the [***16] SCA. (*252 F.R.D. at pp. 347–348*.) The federal district court held that, because the messages remained in the constructive control of the city, they were subject to discovery under the federal rules, notwithstanding the SCA. (*252 F.R.D. at pp. 352–357*.) However, the proper procedure would be to seek the information by a document request to the city rather than a third party subpoena. (*Id. at p. 366*.) To the extent consent of the city is required by the SCA, the city has an obligation under the discovery rules to provide that consent to the service provider. (*252 F.R.D. at p. 359*.)

**(8)** In effect, the court in *Flagg* equated the situation presented to that where the materials sought to be

discovered were in the actual possession of the party. The court explained: "[A] party has an obligation under [*Federal Rules of Civil Procedure,] Rule 34* to produce materials within its control, and this obligation carries with it the attendant duty to take the steps necessary to exercise this control and retrieve the requested documents. … [A] party's disinclination to exercise this control is immaterial, just as it is immaterial whether a party might prefer not to produce documents in its possession or custody." (*Flagg, supra, 252 F.R.D. at p. 363*.) [***17] The court continued: "It is a necessary and routine incident of the rules of discovery that a court may order disclosures that a party would prefer not to make. … [T]his power of compulsion encompasses such measures as are necessary to secure a party's compliance with its discovery obligations. In this case, the particular device that the SCA calls for is 'consent,' and [the defendant] has not cited any authority for the proposition that a court lacks the power to ensure that this necessary authorization [**159] is forthcoming from a party with the means to provide it. Were it otherwise, a party could readily avoid its discovery obligations by warehousing its documents with a third party under strict instructions to release them only with the party's 'consent.' " (*Ibid.*; see *O'Grady v. Superior Court (2006) 139 Cal.App.4th 1423, 1446 [44 Cal. Rptr. 3d 72]* ["Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions."].)

Thus, the question here is not whether respondent court can compel Facebook to disclose the contents of Juror Number One's wall postings but [*865] whether the court can compel [***18] Juror Number One to do so. If the court can compel Juror Number One to produce the information, it can likewise compel Juror Number One to consent to the disclosure by Facebook. The SCA has no bearing on this issue.

**(9)** Juror Number One contends disclosure of the requested information violates the *Fourth Amendment* "in that [he] has a legitimate expectation of privacy in the records." However, beyond merely asserting this to be so, Juror Number One provides no argument or citation to authority. As noted earlier, Juror Number One has provided no specifics as to the operation of Facebook or the nature of his contractual relationship with the Web site. Obviously, the extent of Juror Number One's "legitimate expectation of privacy" under the *Fourth Amendment* would depend on the extent to which his wall postings are disseminated to others or are available to Facebook or others for targeted advertising. Where a point is raised in an appellate brief without argument or legal support, "it is deemed to be without foundation and requires no discussion by the reviewing court." (*Atchley v. City of Fresno (1984) 151 Cal.App.3d 635, 647 [199 Cal. Rptr. 72]*.)

Likewise with Juror Number One's *Fifth Amendment* claim. Juror Number [***19] One asserts he may not be compelled to give evidence against himself. Juror Number One again provides no further argument or citation to authority. But, more significantly, at this point in the litigation and on this record, his *Fifth Amendment* claim is, at best, speculative. Should Juror Number One's rights under the *Fifth Amendment* in fact come into play as this litigation proceeds, the court will be able to consider and resolve them at that time.

Juror Number One argues he nevertheless has a privacy right not to disclose his Facebook posts. He cites as support *Code of Civil Procedure sections 206* and *237*, which protect jurors against involuntary disclosure of personal identifying information. Juror Number One argues these provisions demonstrate a strong public policy to protect jurors from being compelled to discuss their deliberations. However, as noted above, Juror Number One has failed to demonstrate any expectation of privacy in his Facebook posts. At any rate, protection against disclosure of personal identifying information that might be used by a convicted defendant to contact or harass a juror is not the same thing as protection of a juror's communications, which themselves [***20] are misconduct.

But even if Juror Number One has a privacy interest in his Facebook posts, that interest is not absolute. It must be balanced against the rights of real parties in interest to a fair trial, which rights may be implicated by juror misconduct. Thus, the question becomes whether respondent court had the authority to order Juror Number One to disclose the messages he posted to [*866] Facebook during the criminal [**160] trial as part of its inherent power to control the proceedings before it and to assure real parties in interest a fair trial.

**(10)** "A trial court has inherent as well as statutory discretion to control the proceedings to ensure the efficacious administration of justice." (*People v. Cox (1991) 53 Cal.3d 618, 700 [280 Cal. Rptr. 692, 809 P.2d 351]*, disapproved on other grounds in *People v. Doolin (2009) 45 Cal.4th 390, 421, fn. 22 [87 Cal. Rptr. 3d 209, 198 P.3d 11]*.) "Criminal defendants have a right to trial by an impartial jury. (*U.S. Const., 6th Amend.*) '[T]here

exists a “strong public interest in the ascertainment of the truth in judicial proceedings, including jury deliberations.” [Citation.] … Lifting the veil of postverdict secrecy to expose juror misconduct serves an important public purpose. “ ‘[T]o hear such proof would have a tendency [***21] to diminish such practices and to purify the jury room, by rendering such improprieties capable and probable of exposure, and consequently deterring jurors from resorting to them.’ ” [Citation.]’ [Citation.]” (*People v. Tuggles (2009) 179 Cal.App.4th 339, 379–380 [100 Cal. Rptr. 3d 820]*.) “When a trial court is aware of *possible* juror misconduct, the court ‘must “make whatever inquiry is reasonably necessary” ’ to resolve the matter.” (*People v. Hayes (1999) 21 Cal.4th 1211, 1255 [91 Cal. Rptr. 2d 211, 989 P.2d 645]*.)

Juror Number One contends the trial court had no authority to compel production of the Facebook posts, because it had completed its investigation of juror misconduct. He repeatedly asserts the trial court conducted a hearing, examined the jurors, and found the jurors testified truthfully. Implicitly, Juror Number One questions the need for any further investigation of the matter, inasmuch as he testified he posted nothing of substance on Facebook. According to Juror Number One, once he informed the court under oath that he did not post anything of substance to Facebook, the court has no power to inquire further. Juror Number One argues the order at issue here is not really part of the court's continued inquiry into misconduct but [***22] an effort to enforce the failed attempts by real parties in interest to subpoena the Facebook records.

Juror Number One's assertion that the trial court accepted Juror Number One's claim that he posted nothing substantive to Facebook is apparently based on the following comment by the court during discussions about whether to bring in additional jurors to testify: “It seems to me that all four jurors who spoke were credible. It seems to me that all four jurors were doing their best to be open and honest, and to convey what they recall with regard to the deliberations. I did not get an impression from any one of the four jurors that there was an effort to hide anything.”

But assuming the court believed Juror Number One had made no effort to hide anything, that does not also mean it believed he testified accurately. [*867] Juror Number One may well not have remembered posting anything of substance on Facebook, yet the evidence may show otherwise. When asked how many times he recalled posting about the case during trial, Juror Number One initially responded: “I probably posted about ‘Day 22’ or ‘Day 24.’ That's about it. Not really posting every day something negative or anything at all.” Later, [***23] Juror Number One acknowledged he “posted something every other day.” He also testified that he would go onto Facebook to see what others had posted to his account, but claimed he did not look at items posted in response to his own postings about the trial.

In light of Juror Number One's equivocation about how often and what he posted [**161] to Facebook, and the court's express finding that there had been misconduct, with the degree of misconduct still at issue, it can hardly be said respondent court concluded its investigation of the matter. The court may have completed its examination of the jurors, but there was still some question about the content of the Facebook posts themselves. In this regard, it must be remembered that those posts are not just potential evidence of misconduct. They *are* the misconduct.

Juror Number One also contends respondent court's order “necessarily encompass[es] not only [his] privacy, but that of other individuals who were *not* jurors, merely because they are [his] Facebook ‘friends’ and may have posted to his Facebook site during the trial.” But the order at issue here does not encompass posts by Juror Number One's “friends.” The court ordered only that Juror Number [***24] One consent to the release of posts made by him during trial. In any event, to the extent others have posted to Juror Number One's Facebook wall, they have given up any privacy right in those posts as to Juror Number One. It would be as if the “friend” had sent Juror Number One a letter which was still in the juror's possession. If the juror's papers are subject to search, then the letter from the “friend” would also be subject to search.

Juror Number One argues several of his Facebook posts were presented to the trial court during the misconduct hearing and none revealed any prejudice to real parties in interest. However, this puts the cart before the horse. If a juror were to acknowledge having consulted with an attorney during trial but refused to say what was discussed, there would be no way to determine from this alone if the communications were potentially prejudicial. By Juror Number One's theory, the court could inquire no further.

The trial in this matter lasted approximately two months. Juror Number One admitted posting something every other day during trial. Thus, there were potentially 30 posts. Juror Number One acknowledged deleting some

of his posts, although there is no [***25] explanation as to why.
[*868]

The present matter no longer involves a claim of potential misconduct. Misconduct has been established without question. The only remaining issue is whether the misconduct was prejudicial. This cannot be determined without looking at the Facebook posts. Yet Juror Number One would bar the trial court from examining the posts to determine if there was prejudice because there has been no showing of prejudice.

In summary, in the present matter, Juror Number One does not claim respondent court exceeded its inherent authority to inquire into juror misconduct. Just as the court may examine jurors under oath (*People v. Hedgecock (1990) 51 Cal.3d 395, 417–418 [272 Cal. Rptr. 803, 795 P.2d 1260]*), it may also examine other evidence of misconduct. In this instance, the court seeks to review in camera the very items—the Facebook posts—that constitute the misconduct. Juror Number One contends such disclosure violates the SCA, but it does not. Even assuming the Facebook posts are protected by the SCA, the SCA protects against disclosure by third parties, not the posting party. Juror Number One also contends the order is not authorized, because the court has completed its investigation of misconduct. But such [***26] investigation obviously has not been completed. Juror Number One also contends the compelled disclosure violates his *Fourth* and *Fifth Amendment* rights. However, beyond asserting this to be so, he provides no argument or citation to authority. Thus, those arguments are forfeited. Finally, Juror Number One argues [**162] forced disclosure of his Facebook posts violates his privacy rights. However, Juror Number One has not shown he has any expectation of privacy in the posts and, in any event, those privacy rights do not trump real parties in interest's right to a fair trial free from juror misconduct. The trial court has the power and the duty to inquire into whether the confirmed misconduct was prejudicial.

In the absence of further argument or authority, we conclude Juror Number One has failed to establish respondent court's order exceeded its power to inquire into alleged juror misconduct. The petition for writ of prohibition must be denied.

DISPOSITION

The petition for writ of prohibition is denied. Upon this decision becoming final, the stay previously ordered in this matter is vacated.

Raye, P. J., concurred.

**Concur by:** Mauro

## Concur

**MAURO, J.,** Concurring.—The majority opinion states that "even assuming Juror Number One's [***27] Facebook postings are protected by the [Stored Communications Act (SCA) (*18 U.S.C. § 2701 et seq.*)], that protection applies only [*869] as to attempts by the court or real parties in interest to compel Facebook to disclose the requested information. Here, the compulsion is on Juror Number One, not Facebook." (Maj. opn., *ante*, at p. 864.)

It is true the compulsion is on Juror Number One to "consent" to the production of documents. But the trial court is seeking the documents from Facebook, not from Juror Number One. The trial court crafted its order to take advantage of the consent exception in the SCA (Stored Communications Act). (*18 U.S.C. § 2702(b)(3)*.) It ordered Juror Number One to "execute a consent form sufficient to satisfy the exception stated in Title *18, U.S.C. section 2702(b)* allowing Facebook to supply the postings made by [Juror Number One] during trial." In essence, the trial court's order is an effort to compel indirectly (through Juror Number One) what the trial court might not be able to compel directly from Facebook. This is arguably inconsistent with the spirit and intent of the protections in the SCA. Compelled consent is not consent at all. (See, e.g., *Schneckloth v. Bustamonte (1973) 412 U.S. 218, 228, 233 [36 L.Ed.2d 854, 863, 866, 93 S. Ct. 2041]* [***28] [coerced consent is merely a pretext for unjustified intrusion].)

The majority opinion explains that "[i]f the court can compel Juror Number One to produce the information, it can likewise compel Juror Number One to consent to the disclosure by Facebook." (Maj. opn., *ante*, at p. 865.) This may ultimately be true, but here the trial court bypassed a determination as to whether it could compel Juror Number One to produce the documents. Defendant Demetrius Royster had issued subpoenas to both Facebook and Juror Number One directing them to produce Juror Number One's postings. Facebook and Juror Number One both moved to quash the

subpoenas. The trial court continued the hearing on Facebook's motion to quash and granted Juror Number One's motion to quash, ruling that the subpoena against Juror Number One was overbroad. The trial court then concluded it was "unnecessary" to determine whether it could directly compel Facebook or Juror Number One to produce the documents in their possession.[1] Thus, the trial court compelled consent even though other statutory [**163] procedures to directly compel production of the documents were still available and had not yet been exhausted.

Nonetheless, Juror Number One does not assert these specific concerns as contentions in his petition for writ of prohibition, perhaps recognizing that raising such procedural matters would merely delay resolution of the ultimate issues in the case. Instead, he argues the trial court's order violated his rights under constitutional and federal law. He also asserts that the order was an unreasonable intrusion because there is no evidence the Facebook posts were [*870] prejudicial. This final contention encompasses the appropriate balance between Juror Number One's privacy concerns and defendants' right to a fair trial, and it warrants further discussion.

Juror Number One's Facebook posts violated the trial court's instructions to the jury. (*Pen. Code, § 1122, subd. (a)(1)*; *CALCRIM No. 101*.) This was serious misconduct giving rise to a presumption of prejudice. (*In re Hitchings (1993) 6 Cal.4th 97, 118 [24 Cal. Rptr. 2d 74, 860 P.2d 466]*; accord, *People v. Wilson (2008) 44 Cal.4th 758, 838 [80 Cal. Rptr. 3d 211, 187 P.3d 1041]* (*Wilson*).)

"The disapproval of juror conversations with nonjurors derives largely from the risk the juror will gain information about the case that [***30] was not presented at trial." (*People v. Polk (2010) 190 Cal.App.4th 1183, 1201 [118 Cal. Rptr. 3d 876]*.) Nonetheless, the presumption of prejudice that arises from discussing the case with nonjurors "is rebutted … if the entire record in the particular case, including the nature of the misconduct or other event, and the surrounding circumstances, indicates there is no reasonable probability of prejudice, i.e., no *substantial likelihood* that one or more jurors were actually biased against the defendant." (*In re Hamilton (1999) 20 Cal.4th 273, 296 [84 Cal. Rptr. 2d 403, 975 P.2d 600]*, original italics (*Hamilton*); accord, *In re Lucas (2004) 33 Cal.4th 682, 697 [16 Cal. Rptr. 3d 331, 94 P.3d 477]*.)

As the California Supreme Court explained in *Hamilton*, "The standard is a pragmatic one, mindful of the 'day-to-day realities of courtroom life' [citation] and of society's strong competing interest in the stability of criminal verdicts [citations]. It is 'virtually impossible to shield jurors from every contact or influence that might theoretically affect their vote.' [Citation.] Moreover, the jury is a 'fundamentally human' institution; the unavoidable fact that jurors bring diverse backgrounds, philosophies, and personalities into the jury room is both the strength and the weakness [***31] of the institution. [Citation.] '[T]he criminal justice system must not be rendered impotent in quest of an ever-elusive perfection. … [Jurors] are imbued with human frailties as well as virtues. If the system is to function at all, we must tolerate a certain amount of imperfection short of actual bias.' [Citation.]" (*Hamilton, supra, 20 Cal.4th at p. 296*.)

Accordingly, juror conversations involving peripheral matters, rather than the issues to be resolved at trial, are generally regarded as nonprejudicial. (*Wilson, supra, 44 Cal.4th at pp. 839–840* ["trivial" comments to a fellow juror were not prejudicial where not meant to persuade]; *People v. Page (2008) 44 Cal.4th 1, 58–59 [79 Cal. Rptr. 3d 4, 186 P.3d 395]* [circulation of a cartoon in the jury room that did not bear on guilt was not misconduct]; *People v. Avila (2006) 38 Cal.4th 491, 605 [43 Cal. Rptr. 3d 1, 133 P.3d 1076]* [*871] [juror statements disparaging counsel and the court were not material because they had no bearing on guilt]; *People v. Stewart (2004) 33 Cal.4th 425, 509–510 [15 Cal. Rptr. 3d [**164] 656, 93 P.3d 271]* [a juror who complimented the appearance of the defendant's former girlfriend committed nonprejudicial misconduct of a " 'trifling nature' "]; *People v. Majors (1998) 18 Cal.4th 385, 423–425 [75 Cal. Rptr. 2d 684, 956 P.2d 1137]* [general comments by jurors that [***32] did not address the evidence were not prejudicial]; *People v. Loot (1998) 63 Cal.App.4th 694, 698–699 [74 Cal. Rptr. 2d 324]* [a juror who asked a public defender whether the prosecutor was " 'available' " committed "technical," but nonprejudicial, misconduct].)

In determining whether communications are prejudicial or if the presumption of prejudice has been rebutted, the court must consider the " ' "nature and seriousness of the misconduct, and the probability that actual prejudice may have ensued." ' [Citation.]" (*Wilson, supra, 44*

[1] Counsel for Juror Number One admitted during [***29] oral argument in this court that Facebook sent him the posts sought by the trial court.

*Cal.4th at p. 839*, italics omitted; see *People v. Polk, supra, 190 Cal.App.4th at pp. 1201–1202*.)

Four jurors testified under oath at the posttrial hearing. Juror No. 5 testified that she had access to Juror Number One's Facebook postings when she became a Facebook friend of his after the jury was discharged. She said she did not receive any Facebook communications regarding the trial during trial or deliberations. After the jury was discharged, Juror No. 5 found at least one Facebook posting by Juror Number One that he made during the trial, but she did not remember any others. She did not notice any comments in response to Juror Number One's post. When presented in the posttrial hearing [***33] with a copy of five pages from Juror Number One's Facebook wall—exhibit D, pages 19 through 23 in the record—Juror No. 5 said they appeared to be the Facebook pages that she had previously seen. Juror No. 5 recognized on those five pages the Facebook posting on May 18, at 7:36 a.m. from Juror Number One that she had seen. Juror No. 5 testified that there was nothing missing on the copy of the five Facebook pages from what she remembered seeing. She is still a Facebook friend with Juror Number One, and other jurors had been "friended" by Juror Number One, too. Juror No. 5 did not talk to the other juror Facebook friends about what Juror Number One had posted.

Exhibit D, the copy of Facebook postings, includes the following relevant entries (with original ellipsis points):

"May 17 at 3:09pm via Facebook for iPhone": "Week 5 of jury duty … [.]" Below that post was the following comment from a Facebook friend later that afternoon: "[W]ow … never been on jury duty that long … ." And below that, another friend posted a comment later that evening, saying "5 weeks, difil [*sic*] de creer, pues que hicieron para estar en un caso tan largo" which [*872] could be understood to mean "5 [***34] weeks, hard to believe, but what did they do in order to be in a case so long."

"May 18 at 7:36am": "Back to jury duty can it get any more BORING than going over piles and piles of metro pcs phone records … .uuuggghhhhhh." Below the post, a Facebook friend indicated that he or she "like[d]" that comment.

"May 24 at 12:28am": "Jury duty week six … [.]" The copy indicates there were four comments from friends, but only two are visible on the copy. One comment that evening says, "did they convict [S]acramento for pretending to have a pro basketball team?" The other comment that evening says, "You still doing that shit? Sorry to hear holmes!"

"June 27 at 11:21pm via Facebook for iPhone": "Great to have my life back to normal … . NO MORE JURY DUTY … ." The copy indicates that the [**165] post was made after the jury had been discharged, and that there were five comments to the post.

Juror Number One testified next. He admitted posting Facebook entries sporadically about the trial even though the trial judge had instructed the jurors not to talk about the case with anyone. He authenticated exhibit D as depicting him on Facebook. He testified that he did not recall posting anything other [***35] than that he was on jury duty, counting down the days, and in one posting he said the piles and piles of Metro PCS phone record evidence was boring and that he almost fell asleep. He said if they had access to his Facebook that day, he did not think they would still find the postings he made during the trial, because he tries to delete a lot of things. But he said he had no idea prior to the hearing why he had been called in for the hearing.

Juror Number One testified that he never had verbal discussions with people about the case. He said he never talked to other jurors about the Facebook postings, and they did not know about them during the trial.

Juror No. 8 testified that Juror Number One never mentioned Facebook to her, she does not use Facebook, and she does not know anything about it. Juror No. 5 told her, as they were waiting in the hall prior to the posttrial hearing, that Juror Number One had posted on Facebook, but Juror No. 8 did not have any personal knowledge about that.

Juror No. 3 testified that he was not aware that any juror might have been doing anything with Facebook, and he had no Facebook communications with other jurors.
[*873]

The evidence presented at the posttrial [***36] hearing indicated that the Facebook posts involved peripheral matters and did not involve issues to be resolved at trial. Although Juror Number One admitted deleting Facebook posts, he testified that the only things he ever posted regarding the trial were comments about the number of weeks he was on jury duty, counting down the days, and in one post mentioning that the phone record evidence was boring. Juror No. 5 and Juror Number One both testified that exhibit D accurately reflected the type of Facebook posts made by Juror

Number One about the trial. There was no evidence that Juror Number One deleted Facebook posts in anticipation of the posttrial hearing. Juror No. 5 said in her declaration that the alleged inappropriate conduct did not influence her decision in the case, and the other jurors did not have access to the posts during the trial and did not talk about them during the trial. After the hearing, the trial court said the testifying jurors were credible and seemed to be doing their very best to be open and honest. The trial court added, "I did not get an impression from any one of the four jurors that there was an effort to hide anything."

The question is whether this evidentiary [***37] record rebuts the presumption of prejudice. Juror Number One says it does. The majority opinion says this record cannot rebut the presumption until all of the Facebook posts are reviewed by the trial court, noting that "Juror Number One would bar the trial court from examining the posts to determine if there was prejudice because there has been no showing of prejudice." (Maj. opn., *ante*, at p. 868.)

The majority opinion is correct that there has been no showing of prejudice on this record. Moreover, the evidence elicited at the posttrial hearing could be construed to negate the possibility of prejudice, even in the deleted posts. Thus, it is possible to conclude, as Juror Number One urges, that the record does not establish a substantial [**166] likelihood that one or more jurors were actually biased against defendants. (*Hamilton, supra, 20 Cal.4th at p. 296*.)

That might have been the end of the analysis if the trial court had made such findings and declined to continue the investigation. But here, the trial court—which was in the best position to evaluate the evidence—determined that it needed to see the deleted Facebook posts in order to rule out prejudice. At the same time, the trial court sought [***38] to balance Juror Number One's privacy concerns by ordering in camera review of the posts.

Although a trial court must avoid a " 'fishing expedition' " when considering allegations of alleged misconduct (*People v. Hedgecock (1990) 51 Cal.3d 395, 419 [272 Cal. Rptr. 803, 795 P.2d 1260]*), I am unaware of any authority preventing a trial court from taking steps to rule out prejudice once juror misconduct has been established. Because prejudice is presumed based on Juror Number One's misconduct in posting about the trial on Facebook, and [*874] because we do not have all of Juror Number One's Facebook posts regarding the case, I cannot say there is "no substantial likelihood" Juror Number One was biased against defendants. (*Hamilton, supra, 20 Cal.4th at p. 296*, italics omitted.) Under these circumstances, the balance between Juror Number One's privacy concerns and defendants' right to a fair trial tips in favor of defendants.

Accordingly, I concur in the disposition.

A petition for a rehearing was denied June 21, 2012, and petitioner's petition for review by the Supreme Court was denied August 22, 2012, S203713.

---

**End of Document**

Up^ Add To My Favorites

**PROBATE CODE - PROB**

**DIVISION 2. GENERAL PROVISIONS [100 - 890]** *( Division 2 enacted by Stats. 1990, Ch. 79. )*

**PART 20. Revised Uniform Fiduciary Access to Digital Assets Act [870 - 884]** *( Part 20 added by Stats. 2016, Ch. 551, Sec. 1. )*

**870.** This part shall be known, and may be cited, as the Revised Uniform Fiduciary Access to Digital Assets Act.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**871.** As used in this part, the following terms shall have the following meanings:

(a) "Account" means an arrangement under a terms-of-service agreement in which the custodian carries, maintains, processes, receives, or stores a digital asset of the user or provides goods or services to the user.

(b) "Carries" means engages in the transmission of electronic communications.

(c) "Catalogue of electronic communications" means information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person.

(d) "Content of an electronic communication" means information concerning the substance or meaning of the communication, which meets all of the following requirements:

(1) Has been sent or received by a user.

(2) Is in electronic storage by a custodian providing an electronic communication service to the public or is carried or maintained by a custodian providing a remote-computing service to the public.

(3) Is not readily accessible to the public.

(e) "Court" means the superior court presiding over the judicial proceedings which have been initiated under this code to administer the estate of the deceased user, or, if none, the superior court sitting in the exercise of jurisdiction under this code in the county of the user's domicile, and the court, as defined in this section, shall have exclusive jurisdiction over proceedings brought under this part.

(f) "Custodian" means a person that carries, maintains, processes, receives, or stores a digital asset of a user.

(g) "Designated recipient" means a person chosen by a user using an online tool to administer digital assets of the user.

(h) "Digital asset" means an electronic record in which an individual has a right or interest. The term "digital asset" does not include an underlying asset or liability, unless the asset or liability is itself an electronic record.

(i) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(j) "Electronic communication" has the same meaning as the definition in Section 2510(12) of Title 18 of the United States Code.

(k) "Electronic communication service" means a custodian that provides to a user the ability to send or receive an electronic communication.

(l) "Fiduciary" means an original, additional, or successor personal representative or trustee.

(m) "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or other items with like characteristics.

(n) "Online tool" means an electronic service provided by a custodian that allows the user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or

nondisclosure of digital assets to a third person.

(o) "Person" means an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

(p) "Personal representative" means an executor, administrator, special administrator, or person that performs substantially the same function under any other law.

(q) "Power of attorney" means a record that grants an agent authority to act in the place of the principal.

(r) "Record  means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.

(s) "Remote-computing service" means a custodian that provides to a user computer processing services or the storage of digital assets by means of an electronic communications system, as defined in Section 2510(14) of Title 18 of the United States Code.

(t) "Terms-of-service agreement" means an agreement that controls the relationship between a user and a custodian.

(u) "Trustee" means a fiduciary with legal title to property under an agreement or declaration that creates a beneficial interest in another. The term includes a successor trustee.

(v) "User" means a person that has an account with a custodian.

(w) "Will" includes a codicil, a testamentary instrument that only appoints an executor, or an instrument that revokes or revises a testamentary instrument.

*(Added by Stats  2016, Ch  551, Sec  1  (AB 691) Effective January 1, 2017 )*

**872.** (a) This part shall apply to any of the following:

(1) A fiduciary acting under a will executed before, on, or after January 1, 2017.

(2) A personal representative acting for a decedent who died before, on, or after January 1, 2017.

(3) A trustee acting under a trust created before, on, or after January 1, 2017.

(4) A custodian of digital assets for a user if the user resides in this state or resided in this state at the time of the user's death.

(b) This part shall not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business.

*(Added by Stats  2016, Ch  551, Sec  1  (AB 691) Effective January 1, 2017 )*

**873.** (a) A user may use an online tool to direct the custodian to disclose to a designated recipient or not disclose some or all of the user's digital assets, including the content of electronic communications. If the online tool allows the user to modify or delete a direction at all times, a direction regarding disclosure using an online tool overrides a contrary direction by the user in a will, trust, power of attorney, or other record.

(b) If a user has not used an online tool to give direction under subdivision (a) or if a custodian has not provided an online tool, a user may allow or prohibit in a will, trust, power of attorney, or other record the disclosure to a fiduciary of some or all of the user's digital assets, including the contents of electronic communications sent or received by the user.

(c) A user's direction under subdivision (a) or (b) overrides a contrary provision in a terms-of-service agreement.

*(Added by Stats  2016, Ch  551, Sec  1  (AB 691) Effective January 1, 2017 )*

**874.** (a) This part does not change or impair a right of a custodian or a user under a terms-of-service agreement to access and use digital assets of a user.

(b) This part does not give a fiduciary or designated recipient any new or expanded rights other than those held by the user for whom, or for whose estate or trust, the fiduciary or designated recipient acts or represents.

(c) A fiduciary's or designated recipient's access to digital assets may be modified or eliminated by a user, by federal law, or by a terms-of-service agreement when the user has not provided any direction that is recognized in Section 873.

*(Added by Stats  2016, Ch  551, Sec  1  (AB 691) Effective January 1, 2017 )*

**875.** (a) When disclosing the digital assets of a user under this part, the custodian may, in its sole discretion, do any of the following:

(1) Grant the fiduciary or designated recipient full access to the user's account.

(2) Grant the fiduciary or designated recipient partial access to the user's account sufficient to perform the tasks with which the fiduciary or designated recipient is charged.

(3) Provide the fiduciary or designated recipient with a copy in a record of any digital asset that, on the date the custodian received the request for disclosure, the user could have accessed if the user were alive and had full capacity and access to the account.

(b) A custodian may assess a reasonable administrative charge for the cost of disclosing digital assets under this part.

(c) A custodian need not disclose under this part a digital asset deleted by a user.

(d) If a user directs or a fiduciary or designated recipient requests a custodian to disclose under this part some, but not all, of the user's digital assets, the custodian need not disclose the assets if segregation of the assets would impose an undue burden on the custodian. If the custodian believes the direction or request imposes an undue burden, the custodian, fiduciary, or designated recipient may petition the court for an order to do any of the following:

(1) Disclose a subset limited by date of the user's digital assets.

(2) Disclose all of the user's digital assets to the fiduciary or designated recipient.

(3) Disclose none of the user's digital assets.

(4) Disclose all of the user's digital assets to the court for review in camera.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**876.** If a deceased user consented to or a court directs disclosure of the content of electronic communications of the user, the custodian shall disclose to the personal representative of the estate of the user the content of an electronic communication sent or received by the user if the personal representative gives to the custodian all of the following:

(a) A written request for disclosure in physical or electronic form.

(b) A certified copy of the death certificate of the user.

(c) A certified copy of the letter of appointment of the representative, a small-estate affidavit under Section 13101, or court order.

(d) Unless the user provided direction using an online tool, a copy of the user's will, trust, power of attorney, or other record evidencing the user's consent to disclosure of the content of electronic communications.

(e) If requested by the custodian, any of the following:

(1) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account.

(2) Evidence linking the account to the user.

(3) An order of the court finding any of the following:

(A) That the user had a specific account with the custodian, identifiable by the information specified in paragraph (1).

(B) That disclosure of the content of the user's electronic communications would not violate Chapter 121 (commencing with Section 2701) of Part 1 of Title 18 of, and Section 222 of Title 47 of, the United States Code, or other applicable law.

(C) Unless the user provided direction using an online tool, that the user consented to disclosure of the content of electronic communications.

(D) That disclosure of the content of electronic communications of a user is reasonably necessary for estate administration.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**877.** Unless the user prohibited disclosure of digital assets or the court directs otherwise, a custodian shall disclose to the personal representative of the estate of a deceased user a catalogue of electronic communications sent or received by the user and digital assets, other than the content of electronic communications, of the user, if the personal representative gives to the custodian all of the following:

(a) A written request for disclosure in physical or electronic form.

(b) A certified copy of the death certificate of the user.

(c) A certified copy of the letter of appointment of the representative, a small-estate affidavit under Section 13101, or court order.

(d) If requested by the custodian, any of the following:

(1) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account.

(2) Evidence linking the account to the user.

(3) An affidavit stating that disclosure of the user's digital assets is reasonably necessary for estate administration.

(4) An order of the court finding either of the following:

(A) That the user had a specific account with the custodian, identifiable by the information specified in paragraph (1).

(B) That disclosure of the user's digital assets is reasonably necessary for estate administration.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**878.** Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose to a trustee that is not an original user of an account the content of an electronic communication sent or received by an original or successor user and carried, maintained, processed, received, or stored by the custodian in the account of the trust if the trustee gives to the custodian all of the following:

(a) A written request for disclosure in physical or electronic form.

(b) A certified copy of the death certificate of the settlor.

(c) A certified copy of the trust instrument, or a certification of trust under Section 18100.5, evidencing the settlor's consent to disclosure of the content of electronic communications to the trustee.

(d) A certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust.

(e) If requested by the custodian, any of the following:

(1) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account.

(2) Evidence linking the account to the trust.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**879.** Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose, to a trustee that is not an original user of an account, the catalogue of electronic communications sent or received by an original or successor user and stored, carried, or maintained by the custodian in an account of the trust and any digital assets, other than the content of electronic communications, in which the trust has a right or interest if the settlor of the trust is deceased and the trustee gives the custodian all of the following:

(a) A written request for disclosure in physical or electronic form.

(b) A certified copy of the death certificate of the settlor.

(c) A certified copy of the trust instrument or a certification of trust under Section 18100.5.

(d) A certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust.

(e) If requested by the custodian, any of the following:

(1) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account.

(2) Evidence linking the account to the trust.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**880.** (a) The legal duties imposed on a fiduciary charged with managing tangible property apply to the management of digital assets, including all of the following:

(1) The duty of care.

(2) The duty of loyalty.

(3) The duty of confidentiality.

(b) All of the following shall apply to a fiduciary's or designated recipient's authority with respect to a digital asset of a user:

(1) Except as otherwise provided in Section 873, a fiduciary's or designated recipient's authority is subject to the applicable terms-of-service agreement.

(2) A fiduciary's or designated recipient's authority is subject to other applicable law, including copyright law.

(3) In the case of a fiduciary, a fiduciary's authority is limited by the scope of the fiduciary's duties.

(4) A fiduciary's or designated recipient's authority may not be used to impersonate the user.

(c) A fiduciary with authority over the property of a decedent or settlor has the right of access to any digital asset in which the decedent or settlor had a right or interest and that is not held by a custodian or subject to a terms-of-service agreement. Nothing in this subdivision requires a custodian to share passwords or decrypt protected devices.

(d) A fiduciary acting within the scope of the fiduciary's duties is an authorized user of the property of the decedent or settlor for the purpose of applicable computer-fraud and unauthorized-computer-access laws.

(e) The following shall apply to a fiduciary with authority over the tangible, personal property of a decedent or settlor:

(1) The fiduciary has the right to access the property and any digital asset stored in it. Nothing in this subdivision requires a custodian to share passwords or decrypt protected devices.

(2) The fiduciary is an authorized user for purposes of any applicable computer-fraud and unauthorized-computer-access laws.

(f) A custodian may disclose information in an account to a fiduciary of the decedent or settlor when the information is required to terminate an account used to access digital assets licensed to the user.

(g) A fiduciary of a decedent or settlor may request a custodian to terminate the user's account. A request for termination shall be in writing, in either physical or electronic form, and accompanied by all of the following:

(1) If the user is deceased, a certified copy of the death certificate of the user.

(2) A certified copy of the letter of appointment of the representative, a small-estate affidavit under Section 13101, a court order, a certified copy of the trust instrument, or a certification of the trust under Section 18100.5 giving the fiduciary authority over the account.

(3) If requested by the custodian, any of the following:

(A) A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account.

(B) Evidence linking the account to the user.

(C) A finding by the court that the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A).

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**881.** (a) Not later than 60 days after receipt of the information required under Sections 876 to 879, inclusive, a custodian shall comply with a request under this part from a fiduciary or designated recipient to disclose digital assets or terminate an account. If the custodian fails to comply with a request, the fiduciary or designated recipient may apply to the court for an order directing compliance.

(b) An order under subdivision (a) directing compliance shall contain a finding that compliance is not in violation of Section 2702 of Title 18 of the United States Code.

(c) A custodian may notify a user that a request for disclosure of digital assets or to terminate an account was made pursuant to this part.

(d) A custodian may deny a request under this part from a fiduciary or designated recipient for disclosure of digital assets or to terminate an account if the custodian is aware of any lawful access to the account following the date of death of the user.

(e) This part does not limit a custodian's ability to obtain or to require a fiduciary or designated recipient requesting disclosure or account termination under this part to obtain a court order that makes all of the following findings:

(1) The account belongs to the decedent, principal, or trustee.

(2) There is sufficient consent from the decedent, principal, or settlor to support the requested disclosure.

(3) Any specific factual finding required by any other applicable law in effect at that time, including, but not limited to, a finding that disclosure is not in violation of Section 2702 of Title 18 of the United States Code.

(f) (1) A custodian and its officers, employees, and agents are immune from liability for an act or omission done in good faith and in compliance with this part.

(2) The protections specified in paragraph (1) shall not apply in a case of gross negligence or willful or wanton misconduct of the custodian or its officers, employees, or agents.

*(Amended (as added by Stats 2016, Ch 551) by Stats 2016, Ch 585, Sec 2 (SB 873) Effective January 1, 2017 )*

**882.** This part modifies, limits, or supersedes the federal Electronic Signatures in Global and National Commerce Act (15 U.S.C. Sec. 7001 et seq.), but does not modify, limit, or supersede Section 101(c) of that act (15 U.S.C. Sec. 7001(c)) or authorize electronic delivery of any of the notices described in Section 103(b) of that act (15 U.S.C. Sec. 7003(b)).

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**883.** Disclosure of the contents of the deceased user's or settlor's account to a fiduciary of the deceased user or settlor is subject to the same license, restrictions, terms of service, and legal obligations, including copyright law, that applied to the deceased user or settlor.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*

**884.** If any provision of this part or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this part that can be given effect without the invalid provision or application, and, to this end, the provisions of this part are severable.

*(Added by Stats 2016, Ch 551, Sec 1 (AB 691) Effective January 1, 2017 )*