

IN THE SUPREME COURT OF CALIFORNIA

No. S230051

---

FACEBOOK, INC., INSTAGRAM, LLC, AND TWITTER, INC.,  
Petitioners,

v.

THE SUPERIOR COURT OF SAN FRANCISCO COUNTY,  
Respondent.

DERRICK D. HUNTER and LEE SULLIVAN,  
Real Parties in Interest.

SUPREME COURT  
**FILED**

JAN 23 2017

Jorge Navarrete Clerk

---

After Published Opinion by the Court of Appeal  
First Appellate District, Division 5, No. A144315

---

Deputy

Superior Court of the State of California  
County of San Francisco  
The Honorable Bruce Chan, Judge Presiding  
Nos. 13035657, 13035658

---

**SUPPLEMENTAL BRIEF FOR THE PETITIONERS**

---

Eric D. Miller, Bar No. 218416  
EMiller@perkinscoie.com  
John R. Tyler (*pro hac vice*)  
RTyler@perkinscoie.com  
Perkins Coie LLP  
1201 Third Avenue, Suite 4900  
Seattle, WA 98101  
Telephone: 206-359-8000  
Facsimile: 206-359-9000

James G. Snell, Bar No. 173070  
JSnell@perkinscoie.com  
Sunita Bali, Bar No. 274108  
SBali@perkinscoie.com  
Perkins Coie LLP  
3150 Porter Drive  
Palo Alto, CA 94304  
Telephone: 650-838-4300  
Facsimile: 650-838-4350

Attorneys for Petitioners  
Facebook, Inc., Instagram, LLC, and  
Twitter, Inc.

IN THE SUPREME COURT OF CALIFORNIA

No. S230051

---

FACEBOOK, INC., INSTAGRAM, LLC, AND TWITTER, INC.,  
Petitioners,

v.

THE SUPERIOR COURT OF SAN FRANCISCO COUNTY,  
Respondent.

DERRICK D. HUNTER and LEE SULLIVAN,  
Real Parties in Interest.

---

After Published Opinion by the Court of Appeal  
First Appellate District, Division 5, No. A144315

Superior Court of the State of California  
County of San Francisco  
The Honorable Bruce Chan, Judge Presiding  
Nos. 13035657, 13035658

---

**SUPPLEMENTAL BRIEF FOR THE PETITIONERS**

---

Eric D. Miller, Bar No. 218416  
EMiller@perkinscoie.com  
John R. Tyler (*pro hac vice*)  
RTyler@perkinscoie.com  
Perkins Coie LLP  
1201 Third Avenue, Suite 4900  
Seattle, WA 98101  
Telephone: 206-359-8000  
Facsimile: 206-359-9000

James G. Snell, Bar No. 173070  
JSnell@perkinscoie.com  
Sunita Bali, Bar No. 274108  
SBali@perkinscoie.com  
Perkins Coie LLP  
3150 Porter Drive  
Palo Alto, CA 94304  
Telephone: 650-838-4300  
Facsimile: 650-838-4350

Attorneys for Petitioners  
Facebook, Inc., Instagram, LLC, and  
Twitter, Inc.

## TABLE OF CONTENTS

	Page
INTRODUCTION.....	1
ARGUMENT .....	2
A.    Most of the content at issue in this case is not public and thus will not be affected by the resolution of the issues identified in the Court’s order.....	2
B.    Section 2702 of the SCA categorically prohibits providers from disclosing user communications .....	4
1.    Sections 2702(a)(1) and (2) prohibit disclosure of public and nonpublic content alike.....	4
2.    As relevant here, the lawful consent exception of section 2702(b)(3) applies only to content that the user seeks to make available to the public at large.....	5
3.    Legislative history and court opinions suggesting that the SCA does not apply to public content refer to the access provisions of section 2701, not the disclosure provisions of section 2702.....	7
a.    The text and legislative history of the SCA confirm that section 2701 is subject to a “public content” exception that does not apply to section 2702 .....	7
b.    Case law suggesting a “public” exception to the SCA also focuses on access, not disclosure .....	9
C.    The consent exception of § 2702 may permit disclosure but does not require it .....	12
1.    The lawful consent exception, like all exceptions of section 2702, is discretionary and does not permit a private litigant to compel disclosure by a provider .....	12
2.    Recognizing provider discretion is necessary to protect privacy because it reduces the likelihood of compelling disclosure of content where an exception may not, in fact, exist .....	16

**TABLE OF CONTENTS**  
(continued)

	<b>Page</b>
3. There is no need to compel a provider to disclose public content, because a litigant can obtain and use it in his or her case without the provider's assistance.....	17
4. A provider bears all the risk and burden associated with disclosure and should not be compelled to assume those risks where a litigant already has access to the communications.....	19
CONCLUSION .....	20

## TABLE OF AUTHORITIES

	Page
<b>CASES</b>	
<i>Crispin v. Christian Audigier, Inc.</i> (C.D.Cal. 2010) 717 F.Supp.2d 965 .....	6, 10, 11
<i>Ehling v. Monmouth-Ocean Hosp. Serv. Corp.</i> (D.N.J. 2013) 961 F.Supp.2d 659 .....	6, 10
<i>Facebook, Inc. v. Superior Court (2015)</i> , 240 Cal.App.4th 203, review granted Dec. 16, 2016, No. S230051 .....	1, 3
<i>Garcia v. City of Laredo, Tex.</i> (5th Cir. 2012) 702 F.3d 788 .....	13
<i>Gilday v. Dubois</i> (1st Cir. 1997) 124 F.3d 277.....	6
<i>Griggs-Ryan v. Smith</i> (1st Cir. 1990) 904 F.2d 112.....	7
<i>In re Facebook</i> (N.D.Cal. 2012) 923 F.Supp.2d 1204.....	13
<i>In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.</i> (2d Cir. 2016) 829 F.3d 197 .....	15, 16
<i>Konop v. Hawaiian Airlines</i> (9th Cir. 2002) 302 F.3d 868 .....	9, 10, 11
<i>Negro v. Superior Court</i> (2014) 230 Cal.App.4th 879 .....	14, 15, 20
<i>O'Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423 .....	14, 20
<i>People v. Bryant</i> (2014) 60 Cal.4th 335 .....	3
<i>People v. Fernandez</i> (1963) 222 Cal.App.2d 760, 768 .....	4

**TABLE OF AUTHORITIES**  
(continued)

	<b>Page</b>
<i>People v. Harris</i> (Crim. Ct. N.Y. 2012) 949 N.Y.S.2d 590.....	9, 11, 12
<i>People v. Smith</i> (1985) 38 Cal.3d 945.....	4
<i>People v. Stanley</i> (1995) 10 Cal.4th 764.....	3
<i>People v. Valdez</i> (2011) 201 Cal.App.4th 1429.....	19
<i>Russello v. United States</i> (1983) 464 U.S. 16 [104 S.Ct. 296, 78 L.Ed.2d 17].....	13
<i>Sams v. Yahoo! Inc.</i> (9th Cir. 2013) 713 F. 3d 1175.....	13
<i>Schweickert v. Hunts Point Ventures, Inc.</i> (W.D.Wash. Dec. 4, 2014) No. 13-cv-675RSM, 2014 WL 6886630.....	13
<i>Snow v. DirecTV, Inc.</i> (11th Cir. 2006) 450 F.3d 1314.....	10, 11
<i>State v. Bray</i> (Or. Ct. App. 2016) 383 P.3d 883.....	13
<i>United States v. Graham</i> (4th Cir. 2016) 824 F. 3d 421.....	13
<i>United States v. Rodgers</i> (1983) 461 U.S. 677 [103 S.Ct. 2132, 76 L.Ed.2d 236].....	12
<i>United States v. Warshak</i> (6th Cir. 2010) 631 F.3d 266.....	14
<i>United States v. Wong Kim Bo</i> (5th Cir. 1972) 472 F.2d 720.....	13
<i>Viacom Int'l Inc. v. YouTube LLC</i> (S.D.N.Y. 2008) 253 F.R.D. 256.....	9, 11

**TABLE OF AUTHORITIES**  
(continued)

**Page**

**STATUTES**

18 U.S.C. § 2511(2)(g)(i).....	8, 10, 17, 18
18 U.S.C. § 2702(a).....	11
18 U.S.C. § 2702(b)(5).....	14
18 U.S.C. § 2703 .....	9, 11, 14
18 U.S.C. § 2703(a).....	15
Evid. Code, § 1410.....	18

## INTRODUCTION

This brief is submitted in response to the Court's December 21, 2016 order directing the parties to address whether sections 2702(a)(1) and (2) of the Stored Communications Act (SCA) should be construed to apply to communications that were, when sent, configured to be public, and hence generally accessible to the public.

Much of the content at issue in this case is not accessible to the public, and thus the treatment of that content will not be affected by the resolution of the issues raised in the supplemental briefing order. To the extent that defendants wish to obtain public content, there is no need for them to obtain it from the Providers—if a communication is public, a litigant can obtain it without the Provider's assistance. Perhaps for that reason, defendants have not argued that the materials they seek are exempt from the disclosure prohibitions of SCA. Rather, as the Court of Appeals observed, “[i]t is undisputed that the materials Defendants seek here are subject to the SCA's protections.” (*Facebook, Inc. v. Superior Court* (2015), 240 Cal.App.4th 203, 213, review granted Dec. 16, 2016, No. S230051.) Because defendants have waived any argument that the materials they seek are not subject to the SCA, the Court should resolve this case without considering such an argument.

If the Court does consider the issues raised in the supplemental briefing order, it should conclude that sections 2702(a)(1) and (2) of the SCA prohibit covered service providers from disclosing the contents of communications irrespective of the privacy setting of the communications. The public availability of a communication is relevant to a provider's ability to disclose that communication only because section 2702(b) contains eight enumerated exceptions, one of which permits a provider to disclose content with the “lawful consent” of the user. When a user chooses to make a communication freely accessible to the public, he or she has necessarily



consented to its disclosure. Although some of the authorities cited in the Court's supplemental briefing order suggest that the SCA may not apply to publicly available communications at all, most of those authorities address the SCA's restrictions on access to stored communications, set out in section 2701, rather than the SCA's prohibition on provider disclosure, set out in section 2702.

Significantly, while the existence of "lawful consent" permits providers to disclose content, it does not require them to do so. Rather, the SCA vests providers with discretion to decide whether to disclose content when an exception may apply. A contrary interpretation that construed the exceptions as compelling disclosure would permit private parties and law enforcement to circumvent the disclosure prohibition of sections 2702(a)(1) and (2) anytime they believed an exception existed. Congress recognized provider discretion as an important means of promoting the SCA's privacy-enhancing purposes, and if the Court chooses to address the issue, it should do so as well.

## ARGUMENT

**A. Most of the content at issue in this case is not public and thus will not be affected by the resolution of the issues identified in the Court's order.**

Defendants' subpoenas sought "any and all public and private content" associated with Facebook and Instagram accounts purportedly belonging to the victim and the percipient witness as well as "any and all public and private" content from Twitter associated with the account purportedly belonging to percipient witness. (1 AE 12-18; 53-56.) As defendants have acknowledged, much of that content is not publicly available. (1 AE 103 [acknowledging that much of the data sought is not available publicly because "privacy settings vary post-by-post" and that the defense also seeks "private messages"].)

Specifically, most, if not all, of the Facebook or Instagram content sought by defendants is not readily accessible to the public, as defendants recognize by stating that they are unable to obtain it by visiting the Facebook and Instagram profiles at issue. (1 AE 103.) Defendants also acknowledge that they are seeking nonpublic Twitter content that is not available to visitors of the Twitter profile at issue. Because that content is not publicly available, the application of the SCA to public content is not directly relevant to deciding the issues on appeal.<sup>1</sup>

The Court's order addresses only a small subset of the information that defendants sought, such as the publicly available Twitter communications from the public Twitter profile associated with the percipient witness. Defendants have not suggested, however, that they do not have access to the public content or that that SCA's disclosure prohibition does not apply to those communications. To the contrary, as the Court of Appeals observed, "[i]t is undisputed that the materials Defendants seek here are subject to the SCA's protections." (*Facebook, supra*, 240 Cal.App.4th at p. 213; accord Defs.' Br. at p. 10.) Accordingly, defendants have waived any argument that the materials they seek are exempt from the disclosure prohibitions of the SCA. (*People v. Bryant* (2014) 60 Cal.4th 335, 363 ["If a party's briefs do not provide legal argument and citation to authority on each point raised, "the court may treat it as waived, and pass it without consideration.""] [quoting *People v. Stanley* (1995) 10 Cal.4th 764, 793].)

Furthermore, because so much of the content that defendants seek is not public, resolving the issues raised in the Court's supplemental briefing order will not allow the Court to avoid the constitutional questions presented

---

<sup>1</sup> As the Providers have explained in the Petition for Writ of Mandate, defendants have already obtained much of the nonpublic content they seek from the People, and they could obtain additional content by issuing subpoenas to the users who were parties to the sought-after communications. (See Facebook, Instagram and Twitter's Petition for Writ of Mandate at 28.)

in this case. The Court should therefore treat those issues as waived and avoid confronting them. Such a course is especially appropriate because, to the extent defendants' subpoenas seek publicly available content, defendants do not need subpoenas to obtain that content. The ready availability of information from other sources is itself a reason to decline to enforce a subpoena compelling the Providers to produce it. (Cf. *People v. Smith* (1985) 38 Cal.3d 945, 958 ["Obviously, the right to subpoena witnesses . . . does not authorize the indiscriminate use of the process of the court to call witnesses whose testimony . . . is grossly cumulative."] [quoting *People v. Fernandez* (1963) 222 Cal.App.2d 760, 768].)

**B. Section 2702 of the SCA categorically prohibits providers from disclosing user communications.**

**1. Sections 2702(a)(1) and (2) prohibit disclosure of public and nonpublic content alike.**

Sections 2702(a)(1) and (2) prohibit a provider of an "electronic communications service" or "remote computing service" from disclosing user communications or records. Subsection 2702(a)(1) broadly restricts "a person or entity providing an electronic communication service" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." Subsection 2702(a)(2) likewise restricts "a person or entity providing a remote computing service to the public" from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." Neither provision excludes publicly available content from its prohibition.

Paragraphs (1) through (8) of section 2702(b) set out eight voluntary exceptions to the disclosure prohibition—that is, circumstances in which a provider "may" disclose content. While none of the exceptions expressly addresses the original privacy setting of a communication, paragraph (b)(3)

permits a provider to disclose communications “with the lawful consent of the originator or an addressee or intended recipient” of the communication. When the originator of a communication has made it available to the public, he or she has necessarily consented to its disclosure. Thus, as applied to communications that are available to the public, the lawful consent exception allows a provider to disclose communications to any member of the public.

The legislative history of the SCA confirms that Congress intended public content to be subject to the general disclosure prohibition of section 2702(a)(1) and (2), as modified by the consent exception of section 2702(b)(3). The House Judiciary Committee observed that a provider may have “lawful consent” under section 2702(b)(3) to choose to disclose content if, among other things, the communication was made in a manner indicating that the user reasonably understood that it would be made freely available to the public. (H. R. Rep. No. 99-647, 2d Sess., p. 66 [noting that “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,” may have given consent for disclosure of that communication].) That statement presupposes that the prohibitions of section 2702(a)(1) and (2) would otherwise apply to that content. If they did not, there would be no need for section 2702(b)(3) to apply.

**2. As relevant here, the lawful consent exception of section 2702(b)(3) applies only to content that the user seeks to make available to the public at large**

Some of the content that defendants seek consists of communications that may have been shared with others but not with the public at large, or communications that were allegedly publicly accessible at one time but are no longer public. (1 AE 103.) The SCA does not permit provider disclosure of such content to the public.

That a user permits content to be viewed by a large number of people does not mean that the content is publicly available or that the provider has “lawful consent” to disclose it to those outside the group for whom it was intended. Other circumstances surrounding the communication also matter. (See H. R. Rep. No. 99-647, *supra*, at p. 66 [noting that “conditions governing disclosure or use” as relayed to the user can form the basis to “imply consent”].) Even if a post is available to a large group of people, if it is not available to the public at large, then the user cannot be said to have consented to public disclosure—instead, the user has consented only to disclosure to those persons for whom the post was intended. Accordingly, a “critical inquiry” is whether “users took steps to limit access” such that the communication is not accessible “to the general public.” (*Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965, 990.) As one federal court has observed, a contrary rule based “on the number of users who can access information” would be unworkable because it “would result in arbitrary line-drawing.” (*Ibid.*) The “[p]rivacy protection provided by the SCA” cannot reasonably be made to “depend on the number of Facebook friends that a user has.” (*Ehling v. Monmouth-Ocean Hosp. Serv. Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 668.)

In addition, because permissible disclosure under section 2702(b)(3) requires user consent, users may revoke consent by taking a once-public post and rendering it private, or deleting the post or their entire account. By doing so, a user has “actively restrict[ed] the public from accessing the information.” (*Ehling, supra*, 961 F.Supp.2d at p. 668.) In that case, the consent exception of section 2702(b)(3) is no longer satisfied because any disclosure to persons that are not currently authorized to access the communication would “exceed[] the boundaries” of the since-revoked consent. (*Gilday v. Dubois* (1st Cir. 1997) 124 F.3d 277, 297 [considering the conceptually related consent exception to the Wiretap Act and holding

that “a reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception exceeded those boundaries”] [quoting *Griggs-Ryan v. Smith* (1st Cir. 1990) 904 F.2d 112, 119].)

Thus, content is “public,” in the operative sense, only if it is unrestricted such that anyone (including defendants) can access it. If it is restricted in any way, such that defendants are not able to access it without the Providers’ involvement, then the content is not public and the lawful consent exception of section 2702(b)(3) would not be satisfied.

**3. Legislative history and court opinions suggesting that the SCA does not apply to public content refer to the access provisions of section 2701, not the disclosure provisions of section 2702.**

The supplemental briefing order refers to several authorities suggesting that the SCA may not apply to publicly available communications. Those authorities primarily refer to section 2701 of the SCA, which criminalizes unauthorized access to stored communications. They say little about the disclosure prohibitions of section 2702(a)(1) or (2), which, as explained above, are not subject to a similar blanket exception for publicly available content.

**a. The text and legislative history of the SCA confirm that section 2701 is subject to a “public content” exception that does not apply to section 2702.**

Section 2701 of the SCA provides for the criminal punishment of anyone who “intentionally accesses without authorization a facility through which an electronic communication service is provided” or “intentionally exceeds an authorization to access that facility” and “thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system[.]” (18 U.S.C. § 2701(a)(1), (2).)

While section 2701 does not contain an exception for publicly available content, the access provisions of the SCA are subject to an

exception contained in the Wiretap Act, which states that “[i]t shall not be unlawful under [the SCA] for any person . . . to intercept or *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.” (18 U.S.C. § 2511(2)(g)(i) [emphasis added].) Thus, while section 2701 prohibits unauthorized access to communications, section 2511(2)(g)(i) makes clear that access is not prohibited if a system is configured to be publicly accessible. Importantly, the exception applies only to access. Section 2511(2)(g)(i) contains no exception for “divulg[ing]” communications, and thus by its terms it does not alter the disclosure prohibition of section 2702(a)(1) or (2).

The legislative history is consistent with this construction. In discussing “New section 2701,” the Senate Judiciary Committee noted that “[t]his provision addresses the growing problem of unauthorized persons deliberately gaining access to ... electronic or wire communications that are not intended to be available to the public.” (Sen. Rep. No. 99–541, 2d Sess., pp. 35–36, reprinted in 1986 U.S.C.C.A.N., p. 3599.) Congress was aware “that some electronic communication services offer specific features, sometimes known as computer ‘electronic bulletin boards,’ through which interested persons may communicate openly with the public to exchange computer programs in the public domain and other types of information that may be distributed without legal constraint,” but it had no “intent to hinder the development or use of ‘electronic bulletin boards’ or other comparable services.” (H. R. Rep. No. 99-647, *supra*, p. 62.) Thus, “[t]o access a communication on such a system should not be a violation of the law.” (*Ibid.*)

Importantly, this language refers to section 2701, not section 2702, because it appears within a section of the legislative history entitled “Proposed section 2701.” (H. R. Rep. No. 99-647, *supra*, p. 62.) The

legislative history of section 2702, which falls under a section entitled “Proposed section 2702,” contains no similar discussion suggesting that section 2702(a)(1) or (2) does not apply to public content. Instead, as discussed above, it says only that the “lawful consent” exception may permit disclosure of content “freely made available to the public” depending on the “conditions governing disclosure and use.” (*Id.* at p. 66.)

**b. Case law suggesting a “public” exception to the SCA also focuses on access, not disclosure.**

Consistent with the SCA’s text and legislative history, case law suggesting a “public content” exception for the SCA does so predominantly within the context of section 2701, not section 2702. That is likewise true of the authorities referenced in the Court’s order for supplemental briefing. Most of those authorities refer to section 2701, while one case (*People v. Harris*) addresses section 2703 and expressly holds that it applies to public content. Only two of the cases address section 2702, and of those, one (*Viacom Int’l. Inc. v. YouTube LLC*) supports Providers’ construction of that provision.

For example, in *Konop v. Hawaiian Airlines* (9th Cir. 2002) 302 F.3d 868, the Ninth Circuit considered an alleged violation of section 2701 based on unauthorized access. The plaintiff in *Konop* was a former employee of Hawaiian Airlines who had set up a password-protected bulletin board on which employees could discuss issues and concerns. The airline circumvented the password on the bulletin board to access the communications, and the plaintiff sued under section 2701, arguing that the airline did not have authorization to access the communications in the bulletin board. The court recognized both that section 2701 was intended to “protect electronic communications that are configured to be private” and that the statute applied to the plaintiff’s password-protected website. (*Id.* at p.



875.) The court did not consider section 2702 because disclosure by a provider was not at issue.

In *Snow v. DirecTV, Inc.* (11th Cir. 2006) 450 F.3d 1314, the Eleventh Circuit considered a similar claim of unauthorized access. In that case, Snow hosted a website critical of DirecTV's anti-piracy efforts. The website purported to "expressly forbid[] access by DIRECTV and its agents." (*Id.* at p. 1316.) After DirecTV employees and its lawyers accessed the website, Snow sued on the theory that they had violated section 2701. The court rejected that claim, emphasizing that "Snow's complaint fails to allege, as the SCA requires, that the website was configured to not be readily accessible by the general public." (*Ibid.*) The court noted that section 2511(2)(g)(i) expressly authorizes interception of or access to publicly accessible communications, and it concluded that providing a warning that purportedly limited access to a website was not sufficient to prohibit access. If such a warning were sufficient, the court reasoned, "the floodgates of litigation would open and the merely curious would be prosecuted." (*Id.* at p. 1321.) As in *Konop*, the court did not address section 2702. (Accord, *Ehling, supra*, 961 F.Supp.2d at p. 666 [considering an alleged violation of section 2701 and holding that where a user takes steps to limit access, a communication is "configured to be private"].)

In both *Konop* and *Snow*, the courts used the terms "SCA" and "ECPA" (the Electronic Communications Privacy Act) as shorthand for section 2701. That practice led to confusion, as later reflected in *Crispin v. Christian Audigier Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965. In that case, the Central District of California determined that section 2702 prohibited the litigants from using a subpoena to compel content from Facebook, but when presented with defendant's argument that some communications may have been available to the public, it concluded that further findings of fact were necessary to determine the privacy settings of those communications. (*Id.* at

pp. 990-91.) In suggesting that the SCA did not apply to publicly available content, the court incorrectly relied on *Konop, Snow*, and the sections of the legislative history addressing section 2701, but it did not appropriately consider the text or legislative history of section 2702 with respect to public content. Thus, to the extent that the court in *Crispin* suggested that section 2702(a) does not apply to content that is readily accessible to the general public, it relied on misapplication of authority analyzing section 2701.

The other case involving section 2702 considered the public nature of a communication in the context of consent. In *Viacom Int'l Inc. v. YouTube LLC* (S.D.N.Y. 2008) 253 F.R.D. 256, the court found “colorable” the plaintiffs’ argument that users who post content such that it is “freely made available to the public” may have consented to disclosure. (*Id.* at p. 265.) It did not hold that public content is exempt from section 2702, and in fact it acknowledged that “[i]t is not clear from this record whether plaintiffs’ interpretation of the ECPA is correct.” (*Ibid.*)

The final case mentioned in the Court’s order is *People v. Harris* (Crim. Ct. N.Y. 2012) 949 N.Y.S.2d 590, in which a New York appellate court considered section 2703 of the SCA. Section 2703 defines the mechanisms through which the government can compel disclosure of information in criminal cases, and the *Harris* court held that section 2703 applies to the government’s efforts to compel Twitter to disclose public tweets. The court did not hold that public content is exempt from the SCA generally, or from section 2703 specifically—to the contrary, the court required the government to comply with the SCA and obtain a search warrant in order to compel Twitter to disclose content that was 180 days old or less as required by section 2703. (*Id.* at pp. 878-79 [holding that “ECS content information less than 180 days old (tweeted on December 31, 2011) may only be disclosed pursuant to a search warrant” and requiring the government to obtain a new search warrant for this content].) Thus, while

*Harris* did not address section 2702, it, too, supports the position that public communications are not excluded from the voluntary disclosure regime of section 2702.

**C. The consent exception of § 2702 may permit disclosure but does not require it.**

As explained above, this case does not require the Court to consider the application of the SCA to publicly available content. To the extent that the Court does reach that issue, however, it should conclude that the SCA leaves the disclosure of such content to the discretion of the provider. A provider is permitted under the SCA to disclose such content, but it is not required to do so.

**1. The lawful consent exception, like all exceptions of section 2702, is discretionary and does not permit a private litigant to compel disclosure by a provider.**

While section 2702(b)(3) authorizes a provider to disclose content with the lawful consent of the originator, it does not compel provider disclosure. Instead, it vests discretion in a provider by stating that a provider “may” disclose content based on “lawful consent.” (18 U.S.C. 2702(b)(3); see *United States v. Rodgers* (1983) 461 U.S. 677, 706 [103 S.Ct. 2132, 76 L.Ed.2d 236] [“The word ‘may,’ when used in a statute, usually implies some degree of discretion.”].) Congress’s use of the word “may” in section 2702(b)(3) is particularly significant when contrasted with other provisions of the statute. Section 2703(c)(1)(C), for example, states that the government can “require” a provider to disclose non-content records or other information when the government “has the consent of the subscriber or customer to such disclosure.” (18 U.S.C. § 2703(c)(1)(C).) No parallel provision authorizes the government, let alone a private party, to require disclosure of *content* based on consent. The structure of the statute thus demonstrates that Congress meant to ensure that providers would retain the discretion to

choose whether to disclose content based on a user's consent. (See *Russello v. United States* (1983) 464 U.S. 16, 23 [104 S.Ct. 296, 78 L.Ed.2d 17] ["Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."] [quoting *United States v. Wong Kim Bo* (5th Cir. 1972) 472 F.2d 720, 722].)

Courts interpreting the SCA have repeatedly confirmed that "while consent may *permit* production by a provider, it may not *require* such a production." (*In re Facebook* (N.D.Cal. 2012) 923 F.Supp.2d 1204, 1206; see also *Schweickert v. Hunts Point Ventures, Inc.* (W.D.Wash. Dec. 4, 2014) No. 13-cv-675RSM, 2014 WL 6886630, at \*13 ["Even if the Court could compel Plaintiff to consent to the disclosure of some [of] her emails under Rule 34, the providers would still only be permitted, but not required, to turn over the contents under 18 U.S.C. § 2702(b)(3)"]; *State v. Bray* (Or. Ct. App. 2016) 383 P.3d 883, 891 [noting that "under [the] plain language of 18 USC § 2702(b), disclosure pursuant to exception is discretionary"].)

That interpretation of section 2702(b)(3) makes sense in light of the overall purpose of the SCA to protect user privacy. (*Sams v. Yahoo! Inc.* (9th Cir. 2013) 713 F. 3d 1175, 1179 [the purpose of the SCA is "to protect[] the privacy of electronic communications"]; *United States v. Graham* (4th Cir. 2016) 824 F. 3d 421, 438 (conc. opn. of Wilkinson) [the SCA "creates a set of Fourth Amendment-like privacy protections by statute"] [quoting *Sams*], cert. granted *sub nom. Graham v. United States* (2016) \_\_ U.S. \_\_; *Garcia v. City of Laredo, Tex.* (5th Cir. 2012) 702 F.3d 788, 791 ["Congress passed the SCA as part of the Electronic Communications Privacy Act to protect potential intrusions on individual privacy . . . ."].) The existence of consent may sometimes be obvious—such as where a user expressly informs the provider that he or she consents to disclosure of content contained in that

account. But in many cases, the presence of lawful consent may not be obvious—such as where the consent is provided to the provider in a form that does not permit the provider to verify that the person providing the consent is the person who created and used the account.

In addition, if the existence or alleged existence of a voluntary exception such as consent under § 2702(b) were sufficient to compel disclosure, then law enforcement could compel disclosure of content based on that exception, even though the SCA does not permit a governmental entity to compel disclosure of content with anything other than a search warrant. (See 18 U.S.C. § 2703(a), (b); *United States v. Warshak* (6th Cir. 2010) 631 F.3d 266, 288 [holding that the government must obtain a warrant to obtain communications content from a provider].) The voluntary nature of the §2702(b) exceptions is further supported by the other exceptions. For example, § 2702(b)(5) creates an exception that allows a provider to disclose content “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.” 18 U.S.C. § 2702(b)(5). If the existence of a § 2702(b) exception were sufficient for a third party to compel disclosure of content, then the government or any private party could compel disclosure by alleging that disclosure would help protect the provider. (See *O’Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1442 [rejecting argument that section 2702(b)(5) authorizes compelled disclosure in response to a subpoena, noting that “effect of such an interpretation would be to permit disclosure whenever someone threatened the service provider with litigation.”].) Such a construction of the SCA would create an end-run around the statute and effectively replace the provisions of § 2703 that limit the circumstances in which the government can obtain stored communications.

The only published, contrary authority interpreting the lawful consent exception is the decision of the Court of Appeal in *Negro v. Superior Court*

(2014) 230 Cal.App.4th 879. In that case, the court held that Google could be compelled to disclose content in response to a subpoena if the user expressly consents to disclosure. Even on its own terms, the decision does not support compelled disclosure here: in *Negro*, the user “expressly consented” to disclosure in a verifiable manner by “send[ing] an e-mail to Google stating that he was the user of a specified address and that he consented to disclosure of messages between himself and 14 named persons or entities over a specified range of dates.” (*Id.* at p. 893.) The court expressed doubt that anything less than such “express” consent could be adequate to compel disclosure. (*Id.* at p. 891 [noting that “implied-in-fact consent” might likewise be insufficient even when combined with a subpoena, and “question[ing] the soundness of such a construction of the Act, at least for purposes of compelling a provider to disclose stored messages”].)

More fundamentally, the court in *Negro* erred in construing the word “may” in section 2702(b)(3) “not as a grant of discretionary power . . . but as a special *exception* to a general *prohibition*.” (*Id.* at p. 902.) The court’s reasoning is flawed 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 and impermissibly broaden federal law. It would thereby conflict with the SCA’s comprehensive scheme of regulating the circumstances under which the disclosure of content is permissible or required. Indeed, the SCA “formal[ly] recogni[z]es” the “special role” of providers “vis-à-vis the content that its customers entrust to it” such that certain information may be simply unavailable from providers in discovery. (*In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* (2d Cir. 2016) 829 F.3d 197, 220 [rejecting the government’s contention that law developed in the subpoena context should control application of section 2703(a)] and holding that the government cannot use an SCA warrant to obtain content stored in another

country].) “In that respect,” Providers are simply unlike “other subpoena recipients who are asked to turn over records in which only they have a protectable privacy interest.” (*Id.* at pp. 220-21.)

**2. Recognizing provider discretion is necessary to protect privacy because it reduces the likelihood of compelling disclosure of content where an exception may not, in fact, exist.**

The SCA covers a wide—and constantly expanding—range of services, including traditional email providers, public and private bulletin boards, blogs, social networks, and new technologies such as virtual reality. Because these services often provide robust features that allow users to customize and change their privacy settings, providers may not easily be able to determine the intended audience of a communication at any given point in time. Many services are not public bulletin boards in which it is clear that every communication is configured to be readily accessible to the general public. Instead, many modern electronic services, whether available by a web browser or application, have granular privacy options, and they are often available on a variety of devices, including mobile devices with small screens.

For example, Facebook allows users to designate different privacy settings for each communication that they make to their accounts. Users can make certain communications available to all Facebook users, to only their Facebook friends, to specific friends only, or to the user alone. Users can also change the privacy setting that they have selected for a given communication at any time, or they can decide to edit or delete a communication. Twitter and Instagram also have settings that allow users to communicate publicly or privately. Given the potential variability in the intended audiences for content associated with a user, it may be difficult for a provider to accurately identify which content can be viewed by the requesting party. Similarly, if a user changes the privacy setting for a communication, a service may not be

able to accurately determine prior privacy settings. By contrast, that determination will be simple for the requesting party because it either will, or will not, have access to the communications consistent with the user's intent.

Users may also inadvertently publish content intended to be private. For example, a person may hit "publish" on a communication intended to be private, only to realize they hit the wrong button as a result of an oversight. That realization might happen right away, or sometime later, and the provider will often lack the facts necessary to determine the user's motivation: did the user intend to revoke consent, or did the user never knowingly consent in the first place? The SCA, which includes a private right of action against providers for violations of the SCA (18 U.S.C. § 2707(a)), implicitly recognizes these potential complications as well as potential liability if a provider makes a mistake by making provider disclosure voluntary. Thus, where a provider cannot reliably determine whether disclosure is authorized, it need not disclose. Of course, the requesting party is not without recourse, given that she will have access to all communications for which she is authorized and can seek disclosure of other communications directly from any person that was a party to the desired communication.

**3. There is no need to compel a provider to disclose public content, because a litigant can obtain and use it in his or her case without the provider's assistance.**

While the sections of the ECPA that restrict unauthorized access to communications (such as section 2511 of the Wiretap Act and section 2701 of the SCA) are subject to a "readily accessible to the general public" exemption, no such exemption is needed for the disclosure provisions of section 2702. This is because in the absence of an exemption for access to publicly available communications, sections 2511 and 2701 would criminalize merely curious behavior by making it unlawful to intercept or



access a communication that was designed to be available to everyone. Congress accordingly included an exemption applicable to each statute in section 2511(2)(g)(i), which exempts the interception or accessing of electronic communications made through an electronic communication system that is configured to be “readily accessible to the general public.” By contrast, no corresponding exemption from potential liability for the provider exists for section 2702 because disclosure is discretionary, and in the case of public content, anyone can access that content without the need for provider assistance.

For example, Twitter accounts are generally public,<sup>2</sup> such that if a litigant visits a user’s profile and sees that Tweets are visible, that litigant has access to the photos or Tweets available on that user’s profile. In this case, defendants obtained all of the Tweets available on the percipient witness’s account when defendants visited her profile page. (1 AE 53-56, 161-174.) Because an account is either fully public or fully private, there were no Tweets “hidden” from view, and there is no need to seek further “public” content from Twitter. Placing the burden on Twitter or any other provider to produce public content available to the Defendants, or anyone else who seeks such content, is unnecessary and improperly shifts the burden from a party to a non-party. After all, Defendants are in a better position than either provider to gather the public information they deem relevant.

To the extent Defendants believe they need the Providers to produce the communications so the records can be authenticated, they are mistaken. California law places no restriction on “the means by which a writing may be authenticated.” (Evid. Code, § 1410.) The “threshold authentication burden

---

<sup>2</sup> Both Twitter and Instagram permit users to designate their accounts as protected or private, in which case all posts are available only to approved users. Twitter and Instagram also permit direct messages, which are communications to specifically-identified users.

for admissibility is not to establish validity or negate falsity in a categorical fashion, but rather to make a showing on which the trier of fact reasonably could conclude the proffered writing is authentic.” (*People v. Valdez* (2011) 201 Cal.App.4th 1429, 1437.) Thus, to the extent the information is available to the public, anyone, such as an investigator or expert, can authenticate the communications. While a defendant may prefer to have a different witness authenticate such content, this preference is insufficient to override a federal statute. (*Id.* at p. 1435 [“The fact [that] conflicting inferences can be drawn regarding authenticity goes to the document’s weight as evidence, not its admissibility.”]). Furthermore, the Providers were not parties to the communications and they can authenticate neither the actual identity of the person who owns the account nor the person who posted a specific communication. Providers cannot do so because they do not in fact know the actual identity of the person who opened an account or who authored a post. They possess only the information provided to them by a user when the user signs up for the account, and such subscriber information is available to defendants via subpoena. (1 AE 22, 59.)

**4. A provider bears all the risk and burden associated with disclosure and should not be compelled to assume those risks where a litigant already has access to the communications.**

Under the SCA, a nonparty provider bears all the risk and burden associated with an allegedly wrongful disclosure. (18 U.S.C. § 2707(a).) Where a litigant already has access to a communication, there is no reason to force a provider to incur that risk. This is especially so because a provider will often lack the context necessary to determine whether a communication was sufficiently public to trigger the “lawful consent” exception, even more so when factoring in the sheer volume of requests that a provider receives and the various privacy settings and options available to users.

One purpose of the SCA was to enhance the use of communications services and protect providers from being embroiled as a nonparty in litigation. (See *O'Grady v. Superior Court* (2006) 139 Cal.App.4th at 1446-47.) But if litigants could use implied-in-fact consent as a basis to compel a provider to disclose public content that could create uncertainties and result in increased litigation where a provider does not have the ability to easily identify or segregate publicly available communications from nonpublic communications. (See *Negro, supra*, 230 Cal.App.4th at p. 891, fn. 2.) Thus not only is provider disclosure of publicly available content unnecessary, but the likely increase in resulting litigation would increase the burden on courts and nonparties.

#### CONCLUSION

The judgment of the Court of Appeal should be affirmed.

DATED: January 23, 2017

PERKINS COIE LLP

By: 

James G. Snell, Bar No. 173070  
JSnell@perkinscoie.com

Attorneys for Petitioners  
Facebook, Inc., Instagram, LLC, and  
Twitter, Inc.

**WORD COUNT CERTIFICATION**

Pursuant to California Rules of Court, Rule 8.520(c), counsel of record hereby certifies that the foregoing Supplemental Brief for the Petitioners consists of 6179 words, including footnotes, as counted by the Microsoft Word program used to prepare this brief.

DATED: January 23, 2017

**PERKINS COIE LLP**

By: 

James G. Spell, Bar No. 173070  
JSnell@perkinscoie.com

Attorneys for Petitioners  
Facebook, Inc., Instagram, LLC, and  
Twitter, Inc.

**PROOF OF SERVICE**

***Facebook, Inc., et al. v. Superior Court of San Francisco***  
**Case No. S230051**

I, Marla J. Heap, declare:

I am a citizen of the United States and employed in the County of Santa Clara, State of California. I am over the age of 18 years and am not a party to the within action. My business address is Perkins Coie LLP, 3150 Porter Drive, Palo Alto, California 94304-1212. I am personally familiar with the business practice of Perkins Coie LLP. On January 23, 2017, I caused the following document(s) to be served on the following parties by the manner specified below:

**SUPPLEMENTAL BRIEF FOR THE PETITIONERS**

XXX (BY U.S. MAIL) On this day, I placed the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at Palo Alto, California addressed as set forth below.

Heather Trevisan  
Ana Maria Gonzalez  
Office of the San Francisco County  
District Attorney  
850 Bryant Street, Room 322  
San Francisco, CA 94103  
[heather.trevisan@sfgov.org](mailto:heather.trevisan@sfgov.org)

*Counsel for The People of the  
State of California*

Janelle Caywood  
3223 Webster Street  
San Francisco, CA 94123  
[janelle.caywood@gmail.com](mailto:janelle.caywood@gmail.com)

*Counsel for Real Party in  
Interest Lee Sullivan  
(Case No. 13035657)*

Susan Kaplan  
214 Duboce Street  
San Francisco, CA 94103  
[sbkapl@yahoo.com](mailto:sbkapl@yahoo.com)

*Counsel for Real Party in  
Interest Lee Sullivan  
(Case No. 13035657)*

Jose Umali  
507 Polk Street, Suite 340  
San Francisco, CA 94102  
[umali-law@att.net](mailto:umali-law@att.net)

*Counsel for Real Party in  
Interest Derrick Hunter  
(Case No. 13035658)*

Superior Court of the City and County  
of San Francisco  
850 Bryant Street  
San Francisco, CA 94103

*Respondent Superior Court of  
the City and County of San  
Francisco*

Clerk of the Court  
Court of Appeal, First District, Div. 5  
350 McAllister Street  
San Francisco, CA 94102

Donald E. Landis, Jr.  
Monterey County Assistant Public  
Defender  
111 W. Alisal Street  
Salinas, CA 93901  
[landside@co.monterey.ca.us](mailto:landside@co.monterey.ca.us)

*Attorneys for Amicus Curiae  
California Attorney for  
Criminal Justice*

John T. Philipsborn  
Law Offices of J.T. Philipsborn  
507 Polk Street, Ste. 350  
San Francisco, CA 94102  
[jphilipsbo@aol.com](mailto:jphilipsbo@aol.com)

*Attorneys for Amicus Curiae  
California Attorneys for  
Criminal Justice*

David M. Porter  
Office of the Federal Public Defenders  
801 I Street, 3rd Floor  
Sacramento, CA 95814  
[David\\_Porter@fd.org](mailto:David_Porter@fd.org)

*Attorneys for Amicus Curiae  
National Association of  
Criminal Defense Lawyers*

Jeff Adachi  
Public Defender  
Dorothy Bischoff  
Deputy Public Defender  
San Francisco Public Defender's Office  
555 Seventh Street  
San Francisco, CA 94103

*Attorneys for Amicus Curiae  
San Francisco Public  
Defender's Office*

Donald M. Falk  
Mayer Brown LLP  
Two Palo Alto Square  
3000 El Camino Real  
Palo Alto, CA 94306  
[dfalk@mayerbrown.com](mailto:dfalk@mayerbrown.com)


*Attorneys for Amicus Curiae  
Google Inc.*

Stephen P. Lipson  
Michael C. McMahon  
800 S. Victoria Avenue  
Ventura, California 93009  
[michael.mcmahon@ventura.org](mailto:michael.mcmahon@ventura.org)

*Attorneys for Amici Curiae  
California Public Defenders  
Association and Public  
Defender of Ventura County*

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on January 23, 2017 at Palo Alto, California.

  
\_\_\_\_\_  
Marla J. Heap