

No. S245203

**IN THE SUPREME COURT OF  
THE STATE OF CALIFORNIA**

**SUPREME COURT  
FILED**

MAR 19 2018

**FACEBOOK, INC.,**  
*Petitioner,*

Jorge Navarrete Clerk

v.

Deputy

**THE SUPERIOR COURT OF SAN DIEGO COUNTY,**  
*Respondent;*

**LANCE TOUCHSTONE,**  
*Real Party in Interest.*

After Published Opinion by the Court of Appeal, Fourth Appellate  
District, Division One, No. D072171; Superior Court of San Diego  
County, No. SCD268262, Hon. Kenneth So, Presiding Judge

**ANSWERING BRIEF ON THE MERITS**

**PERKINS COIE LLP**  
JAMES G. SNELL, SBN 173070  
jsnell@perkinscoie.com  
CHRISTIAN LEE, SBN 301671  
clee@perkinscoie.com  
3150 Porter Drive  
Palo Alto, CA 94304  
tel: 650.838.4300, fax: 650.838.4350

**GIBSON, DUNN & CRUTCHER LLP**  
\*JOSHUA S. LIPSHUTZ, SBN 242557  
jlipshutz@gibsondunn.com  
555 Mission Street  
San Francisco, CA 94105  
tel: 415.393.8200, fax: 415.393.8306

MICHAEL J. HOLECEK, SBN 281034  
mholecek@gibsondunn.com  
333 South Grand Avenue  
Los Angeles, CA 90071  
tel: 213.229.7000, fax: 213.229.7520

*Attorneys for Petitioner Facebook, Inc.*

No. S245203

**IN THE SUPREME COURT OF  
THE STATE OF CALIFORNIA**

---

**FACEBOOK, INC.,**  
*Petitioner,*

v.

**THE SUPERIOR COURT OF SAN DIEGO COUNTY,**  
*Respondent;*

**LANCE TOUCHSTONE,**  
*Real Party in Interest.*

---

After Published Opinion by the Court of Appeal, Fourth Appellate District, Division One, No. DO72171; Superior Court of San Diego County, No. SCD268262, Hon. Kenneth So, Presiding Judge

---

**ANSWERING BRIEF ON THE MERITS**

---

**PERKINS COIE LLP**  
JAMES G. SNELL, SBN 173070  
jsnell@perkinscoie.com  
CHRISTIAN LEE, SBN 301671  
clee@perkinscoie.com  
3150 Porter Drive  
Palo Alto, CA 94304  
tel: 650.838.4300, fax: 650.838.4350

**GIBSON, DUNN & CRUTCHER LLP**  
\*JOSHUA S. LIPSHUTZ, SBN 242557  
jlipshutz@gibsondunn.com  
555 Mission Street  
San Francisco, CA 94105  
tel: 415.393.8200, fax: 415.393.8306

MICHAEL J. HOLECEK, SBN 281034  
mholecek@gibsondunn.com  
333 South Grand Avenue  
Los Angeles, CA 90071  
tel: 213.229.7000, fax: 213.229.7520

*Attorneys for Petitioner Facebook, Inc.*

## TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	9
STATEMENT OF THE CASE.....	11
I.    The Stored Communications Act.....	11
II.   The California Electronic Privacy Act.....	14
III.  Facebook and the Nature of Electronic Communications.....	15
IV.  Procedural History.....	16
ARGUMENT .....	18
I.    Defendant Has Several Ways To Obtain the Materials He Seeks Without Requiring Facebook To Violate Federal Law.....	18
A.  Defendant can obtain a witness’s communications by issuing a subpoena to the witness himself.....	19
1.  Criminal defendants may issue subpoenas and courts may enforce them, including by ordering the witness to consent to disclosure.....	20
2.  Defendant has not exhausted attempts to subpoena witnesses for the records he seeks.....	21
3.  Defendant cannot challenge the SCA based on speculation that subpoenaing the victim will be ineffective.....	24
4.  If Defendant’s efforts to obtain records from the victim and recipients fail, there are other remedies to assure him a fair trial.....	27
B.  A trial court can enforce a criminal defendant’s subpoena to a witness consistent with the SCA.....	30
1.  A court order directed to a witness does not implicate the SCA.....	31

TABLE OF CONTENTS (continued)

	<u>Page</u>
2. A court order directing a witness to consent to the disclosure by the provider is valid under the SCA, but providers retain discretion to disclose.....	31
C. Defendant can issue trial subpoenas to the victim and other witnesses. ....	34
D. The SCA applies to court orders both before and during trial. ....	35
E. A trial court can force the prosecution to choose between issuing a search warrant and dismissing charges for lack of critical evidence. ....	35
II. The SCA’s Prohibition on Provider Disclosure Does Not Violate Criminal Defendants’ Constitutional Rights .....	37
A. There is no constitutional right to pretrial discovery. ....	38
B. Any right to compel evidence from third parties—before or during trial—is subject to reasonable restrictions like the SCA. ....	39
C. The prosecution’s ability to obtain records by search warrant does not make the SCA unconstitutional. ....	42
D. The SCA does not provide an exception for in camera review, nor is one constitutionally required. ....	43
CONCLUSION .....	45

TABLE OF AUTHORITIES

Page(s)

Cases

*Al Noaimi v. Zaid*  
(D.Kan. Oct. 5, 2012, No. 11-1156), 2012 WL 4758048 .....21

*Alvarado v. Superior Court*  
(2000) 23 Cal.4th 1121 .....38

*Brady v. Maryland*  
(1963) 373 U.S. 83 .....37

*City of L.A. v. Superior Court*  
(2002) 29 Cal.4th 1 .....37, 40

*Crispin v. Christian Audigier, Inc.*  
(C.D.Cal. 2010) 717 F.Supp.2d 965 .....15

*Dell M. v. Superior Court*  
(1977) 70 Cal.App.3d 782 .....29

*Doe v. U.S.*  
(1988) 487 U.S. 201 .....26, 27

*Dunbar v. Google, Inc.*  
(N.D.Cal. Jan. 8, 2013, No. 12-3305) 2013 WL 12331501 .....32

*Ehling v. Monmouth-Ocean Hosp. Service Corp.*  
(D.N.J. 2013) 961 F.Supp.2d 659 .....16

*Evans v. Superior Court*  
(1974) 11 Cal.3d 617 .....36, 43

*In re Facebook*  
(N.D.Cal. 2012) 923 F.Supp.2d 1204 .....32

*Fisher v. U.S.*  
(1976) 425 U.S. 391 .....26

*General Dynamics Corp. v. U.S.*  
(2011) 131 S.Ct. 1900 .....30

*Glazer v. Fireman’s Fund Ins. Co.*  
(S.D.N.Y. Apr. 5, 2012, No. 11-CIV-4374), 2012 WL 1197167 .....21

*In re Grand Jury Subpoena, Dated Apr. 18, 2003*  
(9th Cir. 2004) 383 F.3d 905 .....26

*In re Irish Bank Res. Corp. Ltd.*  
(Bankr.D.Del. 2016) 559 B.R. 627 .....21

*Jencks v. U.S.*  
(1957) 353 U.S. 657 .....30

**TABLE OF AUTHORITIES** *(continued)*

	<u>Page(s)</u>
<i>Juror No. One v. Super. Ct.</i> (2012) 206 Cal.App.4th 854 .....	20, 31, 36
<i>Kling v. Super. Ct.</i> (2010) 50 Cal.4th 1068 .....	20, 30, 36, 44
<i>Lucas v. Superior Court</i> (1988) 203 Cal.App.3d 733 .....	40
<i>Montana v. Egelhoff</i> (1996) 518 U.S. 37.....	40
<i>Negro v. Super. Ct.</i> (2014) 230 Cal.App.4th 879 .....	20, 21, 32, 33
<i>Nucci v. Target Corp.</i> (Fla.App. 4 Dist. 2015) 162 So.3d 146 .....	31
<i>O'Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423 .....	10, 12, 14, 20, 26, 31, 41
<i>People v. Anderson</i> (2001) 25 Cal.4th 543 .....	38
<i>People v. Brophy</i> (1992) 5 Cal.App.4th 932 .....	29
<i>People v. Clark</i> (2011) 52 Cal.4th 856 .....	38
<i>People v. Cromer</i> (2001) 24 Cal.4th 889 .....	22
<i>People v. Goliday</i> (1973) 8 Cal.3d 771 .....	22, 36
<i>People v. Gurule</i> (2002) 28 Cal.4th 557 .....	38, 39, 40
<i>People v. Hammon</i> (1997) 15 Cal.4th 1117 .....	38, 39
<i>People v. Johnson</i> (1989) 47 Cal.3d 1194 .....	41
<i>People v. Loveless</i> (App.Ct.Ill. 1980) 80 Ill.App.3d 1052 .....	28
<i>People v. Maciel</i> (2013) 57 Cal.4th 482 .....	38

TABLE OF AUTHORITIES (continued)

	<u>Page(s)</u>
<i>People v. Martinez</i> (2009) 47 Cal.4th 399 .....	38
<i>People v. Navarro</i> (2007) 40 Cal.4th 668 .....	18, 37
<i>People v. Prince</i> (2007) 40 Cal.4th 1179 .....	38
<i>People v. Riegler</i> (1984) 159 Cal.App.3d 1061 .....	28
<i>People v. Sanders</i> (1995) 11 Cal.4th 475 .....	22
<i>People v. Valdez</i> (2012) 55 Cal.4th 82 .....	38
<i>People v. Walton</i> (1996) 42 Cal.App.4th 1004 .....	22
<i>PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.</i> (W.D.Pa. 2017) 273 F.Supp.3d 558.....	32, 33
<i>Riley v. California</i> (2014) 134 S.Ct. 2473 .....	42
<i>Russello v. U.S.</i> (1983) 464 U.S. 16.....	33
<i>Sallah v. Worldwide Clearing LLC</i> (S.D.Fla. 2012) 855 F.Supp.2d 1364 .....	26
<i>Schweickert v. Hunts Point Ventures, Inc.</i> (W.D.Wash. Dec. 4, 2014, No. 13-675), 2014 WL 6886630 .....	32
<i>State v. Bray</i> (Or.Ct.App. 2016) 383 P.3d 883.....	32, 42
<i>In re Subpoena Duces Tecum to AOL, LLC</i> (E.D.Va. 2008) 550 F.Supp.2d 606 .....	21
<i>U.S. v. Bright</i> (9th Cir. 2010) 596 F.3d 683 .....	26
<i>U.S. v. Hubbell</i> (2000) 530 U.S. 27.....	26
<i>U.S. v. Norwood</i> (8th Cir. 2005) 420 F.3d 888 .....	26

**TABLE OF AUTHORITIES** *(continued)*

	<u>Page(s)</u>
<i>U.S. v. Pierce</i> (2d Cir. 2015) 785 F.3d 832.....	24, 27, 37, 42
<i>U.S. v. Warshak</i> (6th Cir. 2010) 631 F.3d 266 .....	13, 42
<i>United States v. Scheffer</i> (1998) 523 U.S. 303.....	40
<i>United States v. Tucker</i> (S.D.N.Y. 2008) 249 F.R.D. 58 .....	42
<i>Wardius v. Oregon</i> (1973) 412 U.S. 470.....	43
<i>Weatherford v. Bursey</i> (1977) 429 U.S. 545.....	38
<i>Williams v. Florida</i> (1970) 399 U.S. 78.....	23

**Statutes**

18 U.S.C. § 2511(2)(g)(i).....	13
18 U.S.C. § 2701(a)(1).....	13
18 U.S.C. § 2702.....	13
18 U.S.C. § 2702(a) .....	31, 35
18 U.S.C. § 2702(a)(1)–(2).....	13
18 U.S.C. § 2702(b)(1)–(8).....	13
18 U.S.C § 2702(b)(3) .....	13, 21, 32
18 U.S.C. § 2703.....	13
18 U.S.C. §2703(a)–(b).....	13
18 U.S.C. § 2703(c)(1)(C) .....	33
18 U.S.C. § 2707(a)–(c).....	14
Pen. Code, § 632 .....	40
Pen. Code, § 633 .....	40
Pen. Code, § 1054.1, subd. (c).....	36, 43
Pen. Code, § 1054.5, subd. (b).....	20



TABLE OF AUTHORITIES (continued)

	<u>Page(s)</u>
Pen. Code, § 1326, subds. (a)(1)–(4) .....	20
Pen. Code, § 1331 .....	20, 34
Pen. Code, § 1546 et seq.....	14
Pen. Code, § 1546, subd. (d).....	14
Pen. Code, § 1546.1 .....	14
Pen. Code, §1546.1, subd. (a).....	14, 42
Pen. Code, §1546.1, subd. (b).....	14, 42
Pen. Code, § 1546.2 .....	14
Pub. L. No. 99-508, 100 Stat. 1860 (Oct. 21, 1986).....	11

**Other Authorities**

<i>Discovering Facebook: Social Network Subpoenas and the Stored Communications Act</i> (2011) 24 Harv. J.L. & Tech. 563 .....	15
H.R.Rep. No. 99–647, p. 19 (1986).....	12
McPeak, <i>Social Media, Smartphones, and Proportional Privacy in Civil Discovery</i> (2015) 64 U. Kan. L.Rev 235 .....	15, 16
Sen.Rep. No. 99–541, p. 3559 (1986).....	12

## INTRODUCTION

Congress enacted the Stored Communications Act (“SCA”) to protect privacy in emails and other electronic communications, and to encourage the growth of those technologies. One of the SCA’s key provisions restricts service providers like Facebook from disclosing account holders’ electronic communications to third parties. Congress worried that if members of the public could obtain people’s private information from service providers—who maintain such records as part of their role in transmitting and storing data—then people would not trust the privacy of electronic communications, providers would become inundated with third-party requests, and innovations in communications technology would cease. The SCA thus promotes the privacy of electronic communications by strictly limiting the circumstances under which providers may divulge them. Under the SCA, electronic communications have flourished, new and important technologies have developed, and billions of people now rely on email, instant messages, and social media to communicate personally and professionally, participate in important social movements around the world, and share and preserve some of their most private information.

Defendant Lance Touchstone asks this Court to invalidate the SCA’s disclosure restriction as unconstitutional because it prevents him from obtaining social media records and other electronic communications directly from Facebook. But no court has ever held that a criminal defendant has a constitutional right to third-party discovery *at all*, let alone a constitutional right to obtain evidence from a particular source—even the most convenient source. In fact, the United States Supreme Court and this Court have repeatedly held that a defendant does *not* have an absolute right to third-party evidence, and that reasonable restrictions may be imposed on evidence gathering and use.

The SCA is a reasonable restriction because a defendant has many other ways to obtain the same records. The SCA is not a complete bar to accessing electronic records; rather, it limits only one way that a defendant can obtain communications—from providers. Defendants remain free to obtain those records the same way people have sought communications for hundreds of years: from senders, recipients, and public sources. As the Court of Appeal noted in *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1447, the SCA leaves defendants “no worse off” than they were with non-electronic communications.

In any event, this case is a particularly poor vehicle for addressing the SCA’s constitutionality. Defendant has not exhausted *any* of the other ways to obtain the records he seeks. He has made little effort to subpoena the victim for his records. He claims he made two attempts to serve the victim, but he has not asked the prosecution to assist in serving the subpoena, nor has he asked the trial court to compel the prosecution to serve the subpoena. And he has not attempted to obtain records from any message recipient—including his own sister, who is in a relationship with the victim.

Defendant speculates that subpoenaing the victim will be ineffectual because the victim may spoliage or refuse to produce evidence. But that is a risk with any discovery, and it does not create a constitutional violation. Further, even if Defendant ultimately cannot obtain certain social media records from lawful sources, the trial court can fashion narrowly tailored remedies to ensure Defendant gets a fair trial. For example, the trial court can preclude the victim from testifying, condition the victim’s testimony on his pretrial production of complete records, or provide the jury with adverse instructions regarding any failure to disclose records. The trial court also can put the prosecution to the choice of obtaining full records from its key witness (by search warrant, if necessary) or having its case dismissed. Defendant has not sought any of those remedies.

The fact that the SCA did not carve out an exception for criminal defendants was not an “oversight,” as Defendant claims. The statute is part of the federal Criminal Code, repeatedly addresses criminal procedure, and has proven effective in protecting privacy in both civil and criminal matters, including this case. Here, Defendant wants to obtain a crime victim’s private records to try to portray the victim as a violent, domestic-abusive drug user—without giving the victim any opportunity to object to the release of those records. That is exactly why the SCA’s protections are so critical.

Although Congress passed the SCA before the advent of the Internet, in many ways it has proven to be a prescient piece of legislation, foreseeing and encouraging the growth in electronic communications and the ways in which such technology would challenge traditional notions of privacy and Fourth Amendment protections. Instead of scaling back the SCA’s protections, courts have repeatedly maintained and strengthened them, recognizing that email, social media and other electronic communications can contain some of our most sensitive, deeply personal information. Indeed, in 2015, the California Legislature enacted the California Electronic Communications Privacy Act, which imposes further restrictions on the government and is even more privacy-protective than the SCA. While California and the rest of the world are moving toward greater privacy of electronic communications, Defendant asks this Court to move in the opposite direction and erode these important safeguards. The Court should decline that invitation and affirm the Court of Appeal.

## **STATEMENT OF THE CASE**

### **I. The Stored Communications Act**

In 1986, Congress passed the SCA as part of the Electronic Communications Privacy Act. (Pub. L. No. 99-508, 100 Stat. 1860 (Oct. 21, 1986).) The purposes of the Act were to protect individuals’ privacy rights

in stored communications and encourage the development of technology. (*O'Grady, supra*, 139 Cal.App.4th at p. 1445.) Specifically, Congress was concerned that the public and businesses would resist using electronic communications because of “legal uncertainty” over the confidentiality of communications routed through and stored on third-party servers. (*Ibid.*; see also Sen.Rep. No. 99–541, p. 3559 (1986).)

“The [SCA] reflects Congress’s judgment that electronic communications, including those routed through and stored by providers, should receive protections similar to those enjoyed by analog methods of communications.” (H.R.Rep. No. 99–647, p. 19 (1986).) Congress observed that while mail and telephone communications had long enjoyed a variety of legal protections, there were no “comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology . . . even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.” (Sen.Rep. No. 99–541, p. 3559 (1986).)

Congress thus sought not only to shield private electronic communications from government intrusion but also to encourage “‘innovative forms’ of communication by granting them protection against unwanted disclosure *to anyone*.” (*O'Grady, supra*, 139 Cal.App.4th at p. 1445 [original italics].) “In the absence of a degree of privacy at least roughly comparable to that accompanying more traditional modes of communication, potential users might be deterred from using the new forms merely out of a feared inability to communicate in confidence.” (*Ibid.*)

The SCA was codified in the federal Criminal Code and addresses two distinct privacy concerns: (1) the public’s ability to *access* stored communications maintained by a communications provider, and (2) a service

provider's ability to *disclose* stored communications. (18 U.S.C. §§ 2702, 2703.)

In the access provisions, Congress made it a crime to “intentionally access[] without authorization a facility through which an electronic communication service is provided.” (18 U.S.C. § 2701(a)(1).) But it is not a crime for a person to “access an electronic communication . . . [that] is readily accessible to the general public.” (*Id.*, § 2511(2)(g)(i).) Here, that means that any party, including the People and Defendant, may lawfully access all publicly available social media records.

In the disclosure provisions, Congress extended privacy protections to electronic records by restricting service providers's authority to disclose a person's communications and other records. A service provider “shall not knowingly divulge to any person or entity the contents of a [stored] communication.” (18 U.S.C. § 2702(a)(1)–(2).) The disclosure prohibitions do not distinguish between public and private content, but they do not apply to account owners—message senders and receivers—who remain free to disclose their own communications.

The SCA contains eight exceptions to the disclosure prohibition under which providers may disclose stored communications. (18 U.S.C. § 2702(b)(1)–(8).) Most relevant here, a provider “may” divulge the contents of a communication with “the lawful consent” of an addressee or intended recipient of such communication. (*Id.* § 2702(b)(3).)

Congress also recognized that law enforcement officials may have a legitimate need to obtain information from providers. It therefore created a three-tiered system requiring the government to use a subpoena, court order, or search warrant to compel different types of information from providers. (18 U.S.C. § 2703.) As to contents of communications, the government must obtain a search warrant issued upon a finding of probable cause. (*Id.* § 2703(a)–(b); see also, e.g., *U.S. v. Warshak* (6th Cir. 2010) 631 F.3d 266,

288 [search warrant required for the production of contents of communications].)

To add teeth to the prohibition against disclosing stored communications, the SCA provides that any person “aggrieved” by a violation of the statute may recover actual and statutory damages from the person or entity that committed the violation. (18 U.S.C. § 2707(a)–(c).) As a result, a provider may face liability if it improperly discloses information in response to legal process. (See *O’Grady, supra*, 139 Cal.App.4th at p. 1442 [holding that a service provider would violate the SCA by disclosing the content of a person’s communications without consent, even if required to do so by a court order].)

## **II. The California Electronic Privacy Act**

In 2015, the California Legislature enacted the California Electronic Communications Privacy Act (CalECPA), Penal Code section 1546 et seq., to reinforce and enhance the SCA’s privacy protections. CalECPA broadly prohibits California governmental entities in criminal matters from obtaining any “electronic communications information” from a provider except with a warrant or wiretap order based on probable cause. (Pen. Code, § 1546.1, subs. (a), (b).) Under CalECPA, “electronic communications information” is defined more broadly than any of the categories of information under the SCA—it includes all content, all records or other information, and even some basic subscriber information (such as IP logs or billing information). (Pen. Code, § 1546, subd. (d).) Like the SCA, CalECPA prohibits providers from disclosing a person’s communications in response to a subpoena. (See *id.*, at §§ 1546.1, 1546.2.) In other words, the California Legislature has responded to advances in communications technology by enacting a law that is broader and more privacy-protective than the SCA.

### III. Facebook and the Nature of Electronic Communications

There are more than two billion Facebook account holders worldwide. Facebook has become a platform not only for sharing communications with a person's Facebook friends or the Facebook community at large, but also for sensitive private communications among account holders. (See Facebook's Appendix of Exhibits to the Court of Appeal ("App'x") 128.) For many younger people in particular, Facebook and other social media sites have become predominant platforms for substantive electronic communications, replacing email (not to mention the U.S. Postal Service). (Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act* (2011) 24 Harv. J.L. & Tech. 563, 563–564).

Facebook offers people robust privacy options and settings allowing them to specifically tailor the audience of their communications on a message-by-message and post-by-post basis. For instance, a person can choose to communicate with Facebook Messenger, a chat functionality allowing for one-to-one or small group conversations. (See App'x 128.) These messages are similar to traditional email in that they are not available to any person except the direct participants in the communication. (*Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965, 987.) As such, Facebook messages may contain the type of sensitive information that in the past would have been conveyed by mail or email.

Even when a person chooses to "post" something to his or her Facebook page, the person controls who may view that post. For instance, an individual post can be set as available to the general public, available only to the person's Facebook "friends," or available to only members of a specific network (such as a school or an employer). (McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery* (2015) 64 U. Kan. L.Rev 235, 239–240.) A person can even restrict access to posts on a person-by-person basis, allowing some, but not all, friends to view a post.



(See *Ehling v. Monmouth-Ocean Hosp. Service Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 662.) These settings cannot be overridden by others; if a post is set to be viewable only by a certain audience, it may not then be shared or forwarded through the Facebook platform to someone outside that audience. (See McPeak, *supra*, at pp. 239–240.) Additionally, posts and their privacy settings can be edited, allowing people to revise their communications’ chosen audience as they see fit. (See *ibid.*) People can—and do—employ these privacy settings with the expectation that they can tailor their online presence to disclose exactly what they want to disclose and to whom. (See *ibid.*)

#### **IV. Procedural History**

Defendant Lance Touchstone was charged with the attempted murder of his sister’s boyfriend, Jeffrey R. Seven months later, Touchstone served a broad subpoena *duces tecum* on Facebook seeking “all records” associated with the victim’s Facebook account, including all “timeline posts, messages, phone calls, photos, videos, location information, and user-input information from account inception to present date.” (App’x 85.)

Facebook met and conferred with Defendant’s counsel, who conceded that, before serving the subpoena, they had not attempted to subpoena the records directly from the victim nor attempted to work with the People to obtain information by search warrant. (App’x 17.) Facebook moved to quash Defendant’s subpoena because the SCA prohibits Facebook from disclosing the contents of the subpoenaed communications. (App’x 4.)

In opposing Facebook’s motion to quash, Defendant admitted that the victim’s Facebook account “is in part visible to [the] public” and attached screenshots of several of the victim’s public Facebook posts. (App’x 77.) Defendant argues that these public posts—which Defendant already has in his possession—discuss “killing” Defendant’s sister and “clearly reflect [the victim’s] malevolence towards Touchstone, violence toward[s] Rebecca, unlawful handling of firearms, and regular use of illegal drugs.” (Def’s

Opening Brief (“OB”) 28.) Defendant concedes it is “*unknown* whether additional relevant posts” exists. (App’x 78, italics added.) Nonetheless, defense counsel speculated that the unknown content “may contain additional information that provides exonerating, exculpatory evidence for Mr. Touchstone.” (App’x 79.)

Defense counsel described minimal efforts to obtain records from the victim himself. Counsel stated that its investigator tried to contact the victim “on two separate occasions in March 2017,” but did nothing more than “leav[e] her business card” each time. (App’x 80.) Defense counsel did not identify any efforts to enlist the assistance of Defendant’s sister in locating the victim. As late as April 27, 2017, Defendant’s sister was “in and out of a relationship with [the victim].” (App’x 129–130.)

Further, although the record shows that the prosecution had repeated contact with the victim (App’x 95, 99), defense counsel never asked the prosecution for assistance in serving a subpoena on the victim. Rather, defense counsel pressed for an in-person “interview” with the victim, even though the prosecution explained that would be difficult because the victim was “terrified for his safety.” (App’x 95.)

Defense counsel also failed to describe any efforts to obtain the victim’s private communications from recipients. For example, the record includes no evidence that defense counsel tried to subpoena Defendant’s sister for any communications she received from the victim.

On April 27, 2017, the presiding judge, the Honorable Kenneth K. So, denied Facebook’s motion to quash and ordered Facebook to produce the victim’s account contents for in camera review. (App’x 134.)

Facebook petitioned for a writ of mandate from the Court of Appeal, which stayed the order compelling production (Pet’n for Review, Ex. A, at p. 5), and later issued a writ ordering the trial court to vacate its order denying Facebook’s motion to quash and enter a new order granting Facebook’s

motion. (*Id.* at p. 2.) The Court of Appeal held that (1) the SCA expressly prohibits service providers like Facebook from disclosing stored communications in response to a subpoena, thus the trial court had no authority to order an in camera review, (2) Touchstone's constitutional challenges to the SCA were meritless, and (3) Touchstone failed to exhaust his efforts to obtain records from the victim, the prosecution, or any recipients of the victim's private communications.

This Court granted Defendant's petition for review and directed the parties to answer five questions in their briefs. Those questions concern (1) the trial court's authority to compel a witness to comply with a subpoena or consent to disclosure by a provider; (2) whether court orders to the witness may form the basis for lawful consent under the SCA; (3) the trial court's authority to issue and enforce discovery orders pretrial and at trial; (4) whether compelled consent is lawful consent under the SCA; and (5) whether a court may order the prosecution to issue a search warrant.

## ARGUMENT

### **I. Defendant Has Several Ways To Obtain the Materials He Seeks Without Requiring Facebook To Violate Federal Law**

Defendant does not dispute that the SCA forbids Facebook from disclosing victim Jeffrey R.'s Facebook communications without his consent: under 18 U.S.C. § 2702(a), Facebook must "not knowingly divulge to any person or entity the contents" of communications it stores, and it faces civil liability if it violates that prohibition. (*Id.* § 2707(a).)

Defendant argues that the SCA violates his constitutional rights as a criminal defendant, but this Court should not consider his constitutional challenge because it is premature; as the Court of Appeal held, Defendant has not exhausted the other ways available to him to obtain the content he seeks. Under the doctrine of constitutional avoidance, courts should avoid reaching constitutional questions unnecessarily. (*People v. Navarro* (2007)

40 Cal.4th 668, 675.) Defendant's constitutional challenge is easily avoided because it incorrectly presumes that Facebook is the only source for the information he seeks.

This Court's questions to the parties highlight some of Defendant's alternatives, which include seeking content from the Facebook account holder, from any of the people with whom that account holder communicated, or from the prosecution. And if Defendant fails to obtain the evidence he seeks from those sources, the trial court has various tools it can employ, if necessary, to protect Defendant's right to a fair trial without violating the SCA. Defendant comes before this Court without having exhausted any of those options.

**A. Defendant can obtain a witness's communications by issuing a subpoena to the witness himself.**

This Court's Question 1 asks:

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

In response, Facebook states its view that a trial court may order the victim or another witness to comply with subpoenas issued by Defendant, including by ordering the victim or witnesses to consent to disclosure by Facebook. But Defendant has made little effort to obtain any records by subpoena.

**1. Criminal defendants may issue subpoenas and courts may enforce them, including by ordering the witness to consent to disclosure.**

The Penal Code authorizes criminal defendants to issue subpoenas to non-parties, and trial courts have authority to enforce compliance. (Pen. Code, § 1326, subds. (a)(1)–(4).)

If a subpoena recipient fails to comply with a valid subpoena without good cause, the court may enforce compliance by holding the recipient in contempt of court. (Pen. Code, § 1331.) The court may also penalize the recipient by requiring him or her to pay the defendant a fee. (*Ibid.*) If those sanctions prove inadequate, the court may fashion alternative remedies to ensure defendants a fair trial, including sanctioning the prosecution, issuing limiting instructions, prohibiting certain areas of testimony, striking witnesses, and even dismissing charges. (See *Kling v. Super. Ct.* (2010) 50 Cal.4th 1068, 1078 [“[A] third party’s refusal to produce documents requested by the defense can potentially result in sanctions being applied against the People.”]; see also Pen. Code, § 1054.5, subd. (b) [orders may include “immediate disclosure, contempt proceedings, delaying or prohibiting the testimony of a witness or the presentation of real evidence, continuance of the matter, or any other lawful order”].)

In the context at issue here, there is no question that the trial court may order a person to obtain and disclose her own social-media records. Those records are within a person’s custody and control, as numerous courts have held. (See *Negro v. Super. Ct.* (2014) 230 Cal.App.4th 879, 897–898 [reviewing cases].) Alternatively, some courts have ordered the account holder to consent to *the provider’s* production of his records. (See, e.g., *O’Grady, supra*, 139 Cal.App.4th at p. 1446; *Juror No. One v. Super. Ct.* (2012) 206 Cal.App.4th 854, 865 [“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.”).<sup>1</sup> The downside of that approach, however, is that it may not be clear to the provider whether the account holder has actually consented to the release of her records. (See *Negro, supra*, 230 Cal.App.4th at p. 898 [disclosure requires an account holder’s “actual” express consent, as opposed to consent “imputed” by the court].) Further, there could be ambiguity over the scope of the consent and which records it covers. An order requiring a person to acquire and produce her own records eliminates that problem.

A subpoena may also issue to the recipient of an electronic communication. Recipients of communications, like senders, are not subject to any disclosure prohibition under the SCA. Thus, the court may also enforce subpoenas served on recipients of electronic communications. (18 U.S.C § 2702(b)(3).)

**2. Defendant has not exhausted attempts to subpoena witnesses for the records he seeks.**

Although Defendant can obtain email and social media records by subpoenaing the senders and recipients of those communications, he has made little attempt to do so.

Defendant has not subpoenaed the victim because he claims he cannot locate him. But the Court of Appeal was “not persuaded that Touchstone exhausted his efforts to locate the victim,” and rightfully so. (Pet’n for Review, Ex. A, at p. 24.) Indeed, defense counsel’s entire attempt to locate the victim consisted of leaving business cards at two of the victim’s known addresses. (*Ibid.*) That is not sufficient.

---

<sup>1</sup> (See also *In re Irish Bank Res. Corp. Ltd.* (Bankr.D.Del. 2016) 559 B.R. 627, 649; *Al Noaimi v. Zaid* (D.Kan. Oct. 5, 2012, No. 11-1156), 2012 WL 4758048, at \*3; *In re Subpoena Duces Tecum to AOL, LLC* (E.D.Va. 2008) 550 F.Supp.2d 606, 614 fn. 5; *Glazer v. Fireman’s Fund Ins. Co.* (S.D.N.Y. Apr. 5, 2012, No. 11-CIV-4374), 2012 WL 1197167, at \*3.)

In *People v. Cromer* (2001) 24 Cal.4th 889, 904, this Court held that “due diligence” in locating a witness “connotes persevering application, untiring efforts in good earnest, efforts of a substantial character.” Because the prosecution in *Cromer* made only “five or six” attempts to locate the witness over a one-month period, the Court held that the prosecution had failed to exercise diligence in searching for the witness. (*Ibid*; see also *People v. Sanders* (1995) 11 Cal.4th 475, 524–525 [defense counsel was “insufficiently diligent” in locating witness because its efforts “were minimal, consisting of a single phone call to [the witness’] former work number and several visits to her former address” and “no relatives, friends, or coworkers appear to have been contacted”]; *People v. Walton* (1996) 42 Cal.App.4th 1004, 1010 [defense counsel’s efforts to locate witness were insufficient because he did not “check local hospitals; check local jails; obtain [witness’] high school records; ask the district attorney for a current address”], disapproved of on standard-of-review grounds in *Cromer, supra*.)

Defendant’s lack of diligence in locating the victim is even more inexplicable given that Defendant’s sister and the victim have been “in and out” of a relationship that persisted well past Defendant’s arrest. (App’x 129–130; OB 9–10.) The record does not include a single mention of Defendant asking his own sister (or anyone else) for help locating the victim.

Nor did Defendant seek the prosecution’s help in locating the victim. (See *People v. Goliday* (1973) 8 Cal.3d 771, 778 [prosecution must “undertake reasonable efforts in good faith to locate [a witness] so that either party or the court itself . . . could, if it so desired, subpoena him as a witness”] [citation omitted].) Not only is it “reasonable to infer that the prosecution will be in contact with [the victim]”—as the Court of Appeal observed (Pet’n for Review, Ex. A, at p. 24)—but defense counsel actually knew that the prosecution was in contact with the victim. (App’x 95, 99.) Yet, there is no

record evidence of defense counsel asking the prosecution for assistance in serving a subpoena. Rather, defense counsel repeatedly pressed for an in-person “interview” with the victim, despite being told that this would be difficult to arrange due to the attempted-murder victim’s fear of the Defendant. (App’x 95, 97.)<sup>2</sup>

Defendant also did not seek the trial court’s assistance in serving a subpoena on the victim. (Pet’n for Review, Ex. A, at p. 24 [“It does not appear that Touchstone has sought a court order directing the People to assist in serving the subpoena”].) Even if the prosecution failed to assist Defendant in serving a subpoena on the victim—and nothing in the record suggests that Defendant even made that request—Defendant’s first recourse should have been to the trial court.

Defendant has also made no attempt to seek records from the recipients of the victim’s communications. As the Court of Appeal held, “the records Touchstone seeks are also available by subpoena to any addressee or intended recipient of the private communications. Touchstone made no showing that he contacted any of the victim’s Facebook ‘friends’ who were recipients of the private communications to obtain the desired information.” (Pet’n for Review, Ex. A, at p. 25 [citation omitted].)

Defendant could have initiated a search for recipient communications by seeking documents from his own sister, who, as the victim’s girlfriend, presumably would have received at least some of the victim’s Facebook posts

---

<sup>2</sup> There is also nothing improper or unusual about expecting defense counsel to work with the prosecution to locate witnesses. (See *Williams v. Florida* (1970) 399 U.S. 78 [“The adversary system of trial is hardly an end in itself; it is not yet a poker game in which players enjoy an absolute right always to conceal their cards until played. We find ample room in that system, at least as far as ‘due process’ is concerned, for . . . [rules] designed to enhance the search for truth in the criminal trial by insuring both the defendant and the State ample opportunity to investigate certain facts crucial to the determination of guilt or innocence.”].)



and other communications and can provide Defendant any communication he desires. And if Defendant did not want to subpoena his sister, he could have subpoenaed any other potential recipient of the victim's private messages. Defendant has never stated that he is unaware of the victim's circle of friends and contacts, but even if he is unaware, he could have learned about the victim's circle of contacts from the public materials Defendant downloaded from the victim's Facebook page. But Defendant made none of those efforts.

Despite making virtually no attempt to locate records from the many sources that the SCA permits, Defendant is asking this Court to invalidate an act of Congress because of his alleged inability to obtain the victim's email and social media records. His appeal fails for this reason alone. (See *U.S. v. Pierce* (2d Cir. 2015) 785 F.3d 832, 842 [affirming order granting Facebook's motion to quash subpoena in part because defendant "failed to subpoena" the Facebook account holder].)

**3. Defendant cannot challenge the SCA based on speculation that subpoenaing the victim will be ineffective.**

Unable to defend his failure to seek records from the victim, Defendant offers a slew of excuses for why any subpoena might be ineffectual. Each excuse fails.

First, as explained above, the victim is not the only source of the private social media communications that Defendant seeks. Defendant could also subpoena recipients (*ante* p. 22), and he offers no reason why that would be ineffective.

Second, Defendant speculates that the victim could spoliage or fail to produce all relevant records. (OB 22–24.) But that is a risk with any third-party discovery, and such a risk cannot convert every discovery abuse into a constitutional violation. As the Court of Appeal observed, there is nothing

new or novel about uncooperative witnesses: the concern applies “equally to paper documents and [is] not unique to electronic documents stored by third party providers.” (Pet’n for Review, Ex. A, at p. 24.) The mere potential for third-party spoliation does not permit a defendant to obtain evidence in ways that violate federal law. For example, if a defendant fears that a third-party witness will throw away a piece of mail critical to his defense, that does not entitle the defendant to search through the witness’s mailbox or home to obtain the letter.

Third, Defendant speculates that even if the victim complies with a subpoena, the records he can access are “different” from what Facebook can access. (OB 22.) But Defendant offers no record support for that theory, and there is none. As Facebook explained to Defendant, account holders can obtain all content stored in their accounts by using the Download Your Information Tool, or by logging into their accounts and downloading responsive information. (App’x 28.) Defendant complains that Facebook requires an account holder to click in “four separate locations,” but never explains why this means an account holder cannot download his “complete record.” (OB 22.)

Fourth, Defendant speculates that the victim has “deactivated” his Facebook account, and that deactivation “destroy[s] all information that was previously available.” (OB 23.) Again, Defendant offers no record support for this claim. Defense counsel apparently tried to access the victim’s Facebook page and received a message stating: “[n]o permission to access this profile.” (*Ibid.*) But Defendant never explains why this means that any content has been “destroy[ed].”<sup>3</sup> (*Ibid.*)

---

<sup>3</sup> Further, if the content is “destroyed,” as Defendant claims, then Facebook would likely have no greater ability to access it than Defendant or any other party. This would leave Defendant in the same position as a destroyed analog communication; if a witness were to burn a letter, a criminal defendant

Fifth, Defendant claims that the victim may refuse to produce documents by invoking the Fifth Amendment. This is more speculation, as Defendant has not even subpoenaed the victim, let alone provided him an opportunity to comply with that subpoena.

In any event, the Fifth Amendment does not permit witnesses to refuse to produce documents like the ones at issue here. A witness may invoke the Fifth Amendment only if the act of producing the documents reveals something *new* about the documents' existence or location. (*U.S. v. Hubbell* (2000) 530 U.S. 27, 44–45; *In re Grand Jury Subpoena, Dated Apr. 18, 2003* (9th Cir. 2004) 383 F.3d 905, 910.) Where the existence and location of the subpoenaed documents are a “foregone conclusion” and the witness “adds little or nothing” by conceding he has the documents, there is no Fifth Amendment privilege against production because the production becomes a “question . . . not of testimony but of surrender.” (*Fisher v. U.S.* (1976) 425 U.S. 391, 411.) Courts regularly compel production of account documents when the existence of the account is already known. (See, e.g., *Doe v. U.S.* (1988) 487 U.S. 201, 215–217 [requiring defendant to agree to production of bank-account documents]; *U.S. v. Bright* (9th Cir. 2010) 596 F.3d 683, 692–693 [request for credit-card account histories did not implicate the Fifth Amendment because prosecution was already aware of account existence]; *U.S. v. Norwood* (8th Cir. 2005) 420 F.3d 888, 895–896 [same]; *Sallah v. Worldwide Clearing LLC* (S.D.Fla. 2012) 855 F.Supp.2d 1364, 1372 [subpoena requesting account histories did not require defendant to employ the “contents of [her] mind”].)

---

would be similarly unable to gain access to its contents. (See *O’Grady, supra*, at p. 1445 [“Traditional communications rarely afforded any comparable possibility of discovery [to electronic communications]. After a letter was delivered, all tangible evidence . . . remained in the sole possession and control of the recipient . . .”].)

Here, there is no dispute that the victim has a Facebook account, and thus compelling production of that account history cannot violate the Fifth Amendment. (See, e.g., OB 34 [describing the “Facebook records that are currently known to the parties and the court”]; *Doe, supra*, 487 U.S. at pp. 215–217.)

In sum, Defendant’s assertions that the victim may refuse to cooperate with a subpoena are both speculative and meritless.

**4. If Defendant’s efforts to obtain records from the victim and recipients fail, there are other remedies to assure him a fair trial.**

Even if Defendant ultimately fails to obtain records from the victim and any recipients, he should first seek case-specific remedies that do not require providers to violate federal law. The trial court has ample authority to assure Defendant a fair trial, but he has yet to seek any of the available remedies.

As an initial matter, Defendant has not shown that he *needs* any of the allegedly missing social media records for a fair trial. Defendant admits he already has exculpatory evidence from the victim’s public Facebook page, including statements about “killing” Defendant’s sister and communications that “clearly reflect [the victim’s] malevolence towards Touchstone, violence toward[s] Rebecca, unlawful handling of firearms, and regular use of illegal drugs.” (OB 9–10, 28.) Defendant has never explained why he believes the victim’s private messages include additional, non-cumulative evidence. For example, Defendant has not submitted a declaration from his sister, or any other witness who has seen victim’s private posts, describing their content. Rather, Defendant admits it is “unknown” whether the private posts contain relevant material, and this alone dooms his constitutional challenge. (See *Pierce, supra*, 785 F.3d at p. 842 [quashing social media subpoena in part because the defendant’s “suggestion that there could have been additional

relevant exculpatory material in the [account at issue] is purely speculative”].)<sup>4</sup>

But even assuming Defendant could identify private communications that he needs for a fair trial, *and* could show he has exhausted efforts to obtain them, the trial court has numerous ways to ensure a fair trial without ordering Facebook to violate federal law.

For example, the trial court could condition the victim’s trial testimony on his pretrial production of records or preclude the victim from testifying at trial at all. Defendant claims that this particular remedy is insufficient because, whether or not the victim testifies, Defendant still needs evidence to pursue his affirmative defense. (OB 24.) But even if the People could prosecute Defendant without the testimony of the victim—who Defendant describes as the “key witness” (App’x 79)—the trial court has other remedies to assure Defendant a fair trial, including, without limitation: (1) shifting the burden of proof on Defendant’s affirmative defense; (2) instructing the jury that the unproduced social media records would have been favorable to Defendant; (3) forcing the People to address the issue by, for example, choosing between issuing a search warrant on Facebook or

---

<sup>4</sup> There is also no need for Facebook to produce “public” posts, as Defendant concedes he already has them. In any event, the SCA’s disclosure prohibition makes no exception for public content, and the Court should not read one into the SCA. Doing so would create an unreasonable burden on providers, who should not be required to package public information for litigants simply because the litigants prefer not to download the records themselves. Moreover, although designating content as public may be indicative of consent to disclose under the SCA, it is far from a perfect proxy for actual consent—especially since Facebook account holders can and do change their privacy settings frequently. (See *People v. Riegler* (1984) 159 Cal.App.3d 1061, 1066–1067 [resealing an open package creates a new expectation of privacy]; *People v. Loveless* (App.Ct.Ill. 1980) 80 Ill.App.3d 1052, 1055 [an individual loses an expectation of privacy by leaving her coat in a public place, but regains it by reclaiming the coat].)

dismissing the prosecution; or (4) dismissing the charges. Defendant has not sought any of those well-established remedies.

For instance, in *Dell M. v. Superior Court* (1977) 70 Cal.App.3d 782, the Court of Appeal instructed the trial court to issue evidentiary orders because of the defendant's inability to obtain records necessary to his defense. The defendant was charged with, among other things, unlawfully resisting police officers. In discovery, he sought police records to determine whether the officers had a history of using excessive force, supporting a claim of self-defense. (*Id.* at p. 784.) The police department refused to produce records on privilege grounds. The Court of Appeal held that, in light of the unobtainable evidence, the trial court should ensure a fair trial by "suppressing all evidence relating to any skirmish" between defendant and the arresting officer "or to any physical resistance offered by [defendant] at the time of his detention." (*Id.* at p. 788.)

In *People v. Brophy* (1992) 5 Cal.App.4th 932, the Court of Appeal similarly fashioned a remedy to address unproduced evidence. There, the defendant subpoenaed the post office for records in aid of his motion to suppress evidence obtained from an unlawful search. (*Id.* at p. 936.) The post office refused to produce the records. (*Ibid.*) The Court of Appeal explained that it would be "unfair" to require the defendant to meet his burden of proof on the suppression motion given the missing evidence and thus held that the trial court should "shift[] the burden to the prosecution to show a lawful search had occurred." (*Id.* at pp. 937–938.)

In extreme cases, such as when the subpoena recipient "chooses to suffer the consequences of a contempt citation rather than disclose" and the unavailable records are necessary for a fair trial, the court may consider more severe sanctions, including dismissal of "the charges to which the material sought to be discovered pertain[]." (*Dell M.*, *supra*, 70 Cal.App.3d at p. 786; see also *Brophy*, *supra*, 5 Cal.App.4th at p. 937 ["Dismissal is proper as a

sanction for refusing to comply with a discovery order when the effect of such refusal is to deny defendant's right to due process."].)

In *General Dynamics Corp. v. U.S.* (2011) 131 S.Ct. 1900, 1905–1906, for example, the U.S. Supreme Court held that if a prosecution depends on information that cannot be disclosed because it would violate federal law protecting state secrets, the prosecution “must be dismissed.” (See also *Jencks v. U.S.* (1957) 353 U.S. 657, 672 [“We hold that the criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce . . . relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at the trial.”].)

Another option is to require the prosecution to choose between helping the defendant obtain necessary evidence (including by issuing a search warrant, if necessary) and dismissing charges. (See *Kling, supra*, 50 Cal.4th at p. 1078 [“a third party's refusal to produce documents requested by the defense can potentially result in sanctions being applied against the People”].) This option is discussed in more detail below, in response to the Court's Question #5.

Here, Defendant has not shown that he is unable to obtain the victim's Facebook communications from other sources, including the victim, other witnesses, and the prosecution. Even if he ultimately makes that showing, the appropriate remedy would be to adjust the trial parameters or limit the prosecution appropriately, rather than ordering Facebook to violate federal law by disclosing private communications without the account holder's consent.

**B. A trial court can enforce a criminal defendant's subpoena to a witness consistent with the SCA.**

This Court's Question 2 asks:

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

The answer is yes. A court order requiring a Facebook account holder to produce his or her own Facebook communications poses no SCA concerns. The SCA also does not prohibit a court from ordering a Facebook account holder to consent to production.

**1. A court order directed to a witness does not implicate the SCA.**

A court order directing a person to disclose his or her stored communications does not implicate the SCA. The SCA’s prohibitions on disclosure of stored communications apply only to a provider of “electronic communication service[s]” or “remote computing service[s].” (18 U.S.C. § 2702(a); *Juror No. One*, *supra*, 206 Cal.App.4th at p. 864 [SCA “protection applies only as to attempts by the court or real parties in interest to compel Facebook to disclose the requested information”].) The SCA’s disclosure restrictions do not apply to individual account holders. (*O’Grady*, *supra*, 139 Cal.App.4th at pp. 1446–1447; *Nucci v. Target Corp.* (Fla.App. 4 Dist. 2015) 162 So.3d 146, 155 [“The [SCA] does not apply to individuals who use the communications services provided.”].)

**2. A court order directing a witness to consent to the disclosure by the provider is valid under the SCA, but providers retain discretion to disclose.**

As explained above, courts have repeatedly held that a trial court may order an account holder to consent to the provider’s disclosure of his or her stored communications under 18 U.S.C. § 2702(b)(3). (See *ante* pp. 21–22.)

Defendant complains that an account holder’s consent does not *require* disclosure by providers, and so Facebook might still refuse to produce records. (OB 19–20.) This issue is not before the Court, because



no account holder has provided Facebook with consent to disclose. Indeed, as explained above, Defendant has made little attempt to obtain consent from the victim or any other witness. (*Ante* pp. 22–25.) Any suggestion that Facebook would refuse to produce records with an account holder’s consent is thus speculative and unsupported. Facebook, however, addresses the issue of provider discretion to clear any confusion.

The SCA states that providers “may”—as opposed to “must”—divulge communications with lawful consent. (18 U.S.C. § 2702(b)(3).) Courts have confirmed this straightforward interpretation of the SCA. (See *PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.* (W.D.Pa. 2017) 273 F.Supp.3d 558, 561 [denying motion to compel Google, Microsoft and Yahoo to comply with subpoenas based on purported consent, because “according to the language of the SCA, it is within the providers’ discretion whether to disclose e-mails even in cases where there is lawful consent.”]; *State v. Bray* (Or.Ct.App. 2016) 383 P.3d 883, 891 [“under [the] plain language of 18 U.S.C. § 2702(b), disclosure pursuant to exception is discretionary”].)<sup>5</sup>

The *Negro* court incorrectly noted that a provider could be compelled to disclose content in response to a subpoena if the account holder expressly consented. (*Negro, supra*, 230 Cal.App. at p. 900.) That error flowed from

---

<sup>5</sup> (See also, e.g., *Schweickert v. Hunts Point Ventures, Inc.* (W.D.Wash. Dec. 4, 2014, No. 13-675), 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)”]; *Dunbar v. Google, Inc.* (N.D.Cal. Jan. 8, 2013, No. 12–3305) 2013 WL 12331501, at \*1 [“Google may not be compelled to produce the emails and associated metadata that it maintains in electronic storage subject to the Stored Communications Act.”]; *In re Facebook* (N.D.Cal. 2012) 923 F.Supp.2d 1204, 1206 [holding that “while consent may permit production by a provider, it may not require such a production.”].)

misconstruing 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 overall structure of the SCA shows that “Congress knew how to draft a provision of the SCA requiring disclosure yet [it] chose not to make disclosure mandatory in cases with lawful consent.” (*PPG, supra*, 273 F.Supp.3d at p. 561.) For example, section 2703 provides that the government “may *require*” a provider to disclose non-content records, if the government “has the consent of the subscriber or customer to such disclosure.” (18 U.S.C. § 2703(c)(1)(C) [italics added].) No parallel provision allows the government, or anyone else, to compel a provider to produce content based on consent, demonstrating that Congress intended to give providers discretion to disclose content with consent. (See *Russello v. U.S.* (1983) 464 U.S. 16, 23 [“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.”].)

Providers are also afforded discretion because they bear the risk of a mistaken disclosure under 18 U.S.C. § 2707(a), and the type of consent that may work for one provider may not work for another. It is, therefore, important that providers retain discretion to evaluate consent depending on the facts of any given case. The risk of error and potential liability that justifies discretion is not hypothetical. For example, in *PPG*, a plaintiff issued subpoenas to various providers seeking content purportedly owned by a person who died in June 2015, arguing that his personal representative had consented to disclosure. (*PPG, supra*, 273 F.Supp.3d at p. 560–561.) Two of the providers, however, noticed that the accounts listed in the subpoena remained active long after the person’s death, calling into question whether the plaintiff had identified the correct accounts. (*Id.* at p. 561.) Because electronic services often allow people to create accounts with nothing more

than an e-mail address or phone number, provider verification of ownership is often difficult. For this reason, among others, many providers, including Facebook, have developed tools that allow people to obtain their own communications directly. (App'x 28.) These tools not only provide people with easy access to their information, but obviate the need for provider assistance in disclosing stored communications in many instances. (*Ante* p. 26.)

Ultimately, though, Defendant's concern that Facebook might not produce records even with an account holder's consent is speculative and premature. Further, as discussed above, account holders can download their own social media records without any assistance from Facebook. Defendant has not yet asked the victim to download his own records, or asked the trial court for any assistance in compelling him to do so.

**C. Defendant can issue trial subpoenas to the victim and other witnesses.**

This Court's Question 3 asks:

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

Yes. As discussed above, there is no reason why Defendant cannot seek records *before trial* by issuing enforceable subpoenas to the victim and any recipients of his private communications. If, however, Defendant's pretrial efforts fail, he can issue enforceable subpoenas *at trial*. (Pen. Code, § 1331.) Section 1331's grant of authority does not distinguish between pretrial and trial, and thus Defendant can use it to compel production or testimony at trial. Indeed, the Court of Appeal recognized that Touchstone could "wait until trial to seek the victim's private Facebook records. At that time, [if and] when the victim's private Facebook communications become relevant to the

defense,” the trial court can order the account holder to produce them. (Pet’n for Review, Ex. A, at p. 25.)

**D. The SCA applies to court orders both before and during trial.**

This Court’s Question 4 asks:

Would a court order contemplated under (3) be proper under the Stored Communications Act, 18 U.S.C. § 2702(b)(3)?

Yes, so long as the court order is directed at the account holder or other witnesses, and not at the provider. The SCA makes no distinction between pretrial and trial; it is a federal statute of general applicability that applies regardless of the stage of a court proceeding, and even when there is no court proceeding at all. (See 18 U.S.C. § 2702(a).) Unless one of the enumerated exceptions applies, the SCA prohibits a provider from disclosing electronic records. But nothing in the SCA would prohibit a trial subpoena to an account holder or other witness to produce his or her stored communications.

**E. A trial court can force the prosecution to choose between issuing a search warrant and dismissing charges for lack of critical evidence.**

This Court’s Question 5 asks:

As an alternative to options (1) or (3) set forth above, may the trial court, acting pursuant to statutory and/or inherent authority to control the litigation before it and to insure fair proceedings, and consistently with 18 U.S.C. § 2702(b)(3), order the prosecution to issue a search warrant under 18 U.S.C. § 2703 regarding the sought communications? (Cf. *State v. Bray* (Or.App. 2016) 383 P.3d 883, pets. for rev. accepted June 15, 2017, 397 P.3d 30 [S064843, the state’s pet.]; 397 P.3d 37 [S064846, the defendant’s pet.].) In this regard, what is the effect, if any, of California Constitution, art. I, §§ 15 and 24?

Facebook does not take a position on whether, and under what authority, a trial court may order the prosecution to issue a search warrant. Certainly, Facebook will comply with any lawful search warrant it receives. But Facebook notes that a trial court has numerous tools at its disposal to ensure the prosecution helps the defendant obtain necessary evidence, and the trial court can dismiss charges if the prosecution fails to comply. (See Penal Code, § 1054.1, subd. (c).) Defendant has yet to explore these options with the trial court, making his constitutional challenge to the SCA premature.

“A trial court has inherent as well as statutory discretion to control the proceedings to ensure the efficacious administration of justice.” (*Juror No. One, supra*, 206 Cal.App.4th at p. 866.) That authority includes holding the prosecution to its duty to help defendants obtain necessary evidence. For example, the trial court can force the prosecution to assist the defense in locating witnesses. (*Goliday, supra*, 8 Cal.3d at pp. 779–782.) The trial court can also compel the prosecution to order a pretrial lineup if a defendant needs one to pursue his false-identification defense. (*Evans v. Superior Court* (1974) 11 Cal.3d 617, 625.) As this Court held, “the People cannot escape a responsibility to disclose merely by passive conduct or the failure to acquire precise knowledge sought by but unavailable to an accused.” (*Ibid.*)

The trial court can also incentivize the prosecution to assist a defendant in obtaining discovery, rendering it unnecessary for the trial court to order the prosecution to issue a search warrant. As this Court explained in *Kling*, the trial court can impose sanctions against the prosecution if third parties fail to produce critical evidence. (*Kling, supra*, 50 Cal.4th at p. 1078.) Here, the trial court may exclude the victim’s testimony, shift the burden of proof, issue a jury instruction, or even dismiss charges if certain evidence is not made available to the defense. (*Ante* pp. 21, 29–31.) That may put the

prosecution to the choice of issuing a search warrant or facing one or more of these potential sanctions.

Defendant notes that he already unsuccessfully moved to compel the People to issue a search warrant. But Defendant moved on the theory that the prosecution had “constructive possession” of *all* social media records, and thus an obligation to turn them over under *Brady v. Maryland* (1963) 373 U.S. 83. Defendant could have taken (and still can take) a far less extreme approach: ask the prosecution for assistance in serving a subpoena on the victim; if the prosecution refuses, or if the victim fails to comply with the subpoena, then ask the trial court to order evidentiary, issue, or terminating sanctions to remedy the absence of any critical evidence. The prosecution can then choose between accepting those sanctions or issuing a search warrant. Defendant should invoke these traditional, well-established, and proven methods for obtaining a fair trial instead of asking for an order requiring Facebook to violate federal law by disclosing a third party’s private information.

## **II. The SCA’s Prohibition on Provider Disclosure Does Not Violate Criminal Defendants’ Constitutional Rights**

Because Defendant has many ways to obtain the content he seeks, his constitutional challenge to the SCA fails. (See *Navarro, supra*, 40 Cal.4th at p. 675 [doctrine of constitutional avoidance]; *Pierce, supra*, 785 F.3d at p. 842 [rejecting constitutional challenge to SCA because defendant did not exhaust other ways to obtain communications].) If this Court considers Defendant’s constitutional arguments, however, it should reject them. Defendant faces a “heavy burden” to invalidate an act of Congress, and he has not carried that burden. (*City of L.A. v. Superior Court* (2002) 29 Cal.4th 1, 16 [“courts will presume a statute is constitutional unless its unconstitutionality clearly, positively, and unmistakably appears; all presumptions and intendments favor its validity”] [citation omitted].)

**A. There is no constitutional right to pretrial discovery.**

This Court held in *People v. Hammon* (1997) 15 Cal.4th 1117, 1125–1127, that there is no constitutional right to pretrial discovery. (See also *Weatherford v. Bursey* (1977) 429 U.S. 545, 559 [“There is no general constitutional right to discovery in a criminal case”].)

As the Court of Appeal observed, this Court has reaffirmed *Hammon* “in varying contexts, for the proposition that a criminal defendant is not entitled to pretrial discovery.” (Pet’n for Review, Ex. A, at p. 14.) For example, in *People v. Clark* (2011) 52 Cal.4th 856, 983, this Court held that a defendant has no pretrial right to discover a prosecution witness’s criminal history, even when it leads to “a significant impairment of [a defendant’s] ability to investigate and cross-examine a witness.” In *People v. Prince* (2007) 40 Cal.4th 1179, 1234, this Court held that a defendant did not have a pretrial right to conduct discovery into an FBI database, even though the defendant claimed he needed that discovery to effectively impeach an expert witness. And in *People v. Valdez* (2012) 55 Cal.4th 82, 106–107, this Court held that a defendant did not have a pretrial right to discover the identities of certain prosecution witnesses who feared for their safety. The list goes on. (See, e.g., *People v. Maciel* (2013) 57 Cal.4th 482, 507–508 [no pretrial right to witness identities]; *Alvarado v. Superior Court* (2000) 23 Cal.4th 1121, 1135 [same]; *People v. Martinez* (2009) 47 Cal.4th 399, 454, fn. 13 [no pretrial right to juvenile records]; *People v. Anderson* (2001) 25 Cal.4th 543, 577, fn. 11 [no pretrial right to psychiatric examination of witness]; *People v. Gurule* (2002) 28 Cal.4th 557, 594 [no pretrial right to invade the attorney-client privilege].)

This Court should reaffirm *Hammon* and continue to hold that there is no constitutional right to pretrial discovery. As this Court recognized in *Hammon*, it is difficult for a court to assess before trial which evidence the defendant will need at trial. “[T]he court typically will not have sufficient

information to” “balance the defendant’s need for cross-examination” against the privacy interests at stake. (15 Cal.4th at p. 1127.) Thus, “if pretrial disclosure is permitted, a serious risk arises” that information “will be disclosed unnecessarily.” (*Ibid.*)

In *Hammon* itself, the trial court denied pretrial discovery seeking confidential psychiatric records of a juvenile witness. At trial, the defendant ultimately admitted to the conduct he sought the privileged records to disprove; had the trial court released them, there would have been “not only a serious, but an unnecessary, invasion of the patient’s statutory privilege and constitutional right to privacy.” (*Ibid.* [citation omitted].) Likewise, in *Gurule*, the Court held that ample evidence at trial ultimately proved the same point that would have been demonstrated using the witness’s psychiatric records. (*Gurule, supra*, 28 Cal.4th at 594.)

Only at trial, when immersed in the evidence, can the trial judge effectively weigh the need for evidence against privacy concerns. The decision may ultimately depend on developments at trial, including for example: (1) whether and how a particular witness testifies; (2) how the prosecution’s theory develops at trial, including what evidence it introduces and what charges it decides to pursue or abandon at trial; and (3) what other evidence the defense introduces that could make the records superfluous.

Because it is undisputed that Defendant’s subpoena on Facebook seeks pretrial discovery, and because this Court has repeatedly held that there is no constitutional right to pretrial discovery, this Court need not go any further in addressing Defendant’s constitutional challenge.

**B. Any right to compel evidence from third parties—before or during trial—is subject to reasonable restrictions like the SCA.**

Even if a defendant has a right to discovery that arises either before or during trial, it is not absolute. Here, the SCA restricts only one potential



*source* of the evidence Defendants seeks—providers. As the U.S. Supreme Court held in *United States v. Scheffer* (1998) 523 U.S. 303, 308, “[a] defendant’s right to present relevant evidence is not unlimited, but rather is subject to reasonable restrictions.” Courts regularly uphold laws that preclude defendants from obtaining or using particular evidence. In fact, discovery and evidence codes are predicated on the idea that the right to evidence is not unbounded. For example:

- In *Scheffer, supra*, at p. 308, the Court upheld a law precluding the defense from obtaining polygraph evidence;
- In *Montana v. Egelhoff* (1996) 518 U.S. 37, 56, the Court upheld a law precluding the defense from offering evidence of voluntary intoxication;
- In *City of L.A. v. Superior Court* (2002) 29 Cal.4th 1, 16, this Court upheld a law barring defendants from obtaining police-officer complaints filed more than 5 years before a crime occurred; and
- In *Lucas v. Superior Court* (1988) 203 Cal.App.3d 733, 735, the court upheld a rule that only “material and necessary” witnesses may be compelled to attend trial more than 150 miles from their residence.

Some laws limit the *methods* a defendant can use to obtain evidence. For example, a defendant can obtain evidence about a particular conversation by asking any party to the conversation about it, but he may not obtain evidence of the conversation by wiretapping or otherwise unlawfully recording it. (See Penal Code, §§ 632, 633.)

Other laws limit the *sources* of evidence. For example, a defendant cannot subpoena an attorney to divulge communications covered by the attorney-client privilege. This evidence could be highly exculpatory—including, for example, a third-party’s confession to his attorney that *he* committed the crime with which defendant was charged—but that does not permit a defendant to obtain the evidence from that particular source. (See *People v.*

*Gurule* (2002) 28 Cal.4th 557, 594 [“a criminal defendant’s right to due process does not entitle him to invade the attorney-client privilege of another”]; *People v. Johnson* (1989) 47 Cal.3d 1194, 1228.)

Similarly, the SCA imposes a reasonable limitation on a defendant’s access to certain third-party evidence from a provider: far from absolutely prohibiting defendants from obtaining and using social media records at trial, it merely prohibits them from obtaining the contents of communications from *one particular source*—electronic communications providers. Defendant may obtain those records from public sources, senders or recipients, or the government, but Congress has determined that he cannot obtain them directly from Facebook.

Defendant argues that Facebook is the most convenient source of certain records, but that does not make the SCA unconstitutional. As the Court of Appeal explained in *O’Grady*, it was “far from irrational for Congress to conclude that one seeking disclosure of the contents of email, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message.” (*O’Grady, supra*, 139 Cal.App.4th at p. 1446.)

Allowing third parties to subpoena providers would also create immense burdens on providers and inundate them with requests, further underscoring the SCA’s rationality. Indeed, if this Court were to hold that Defendant can directly subpoena Facebook for records, what criminal defense attorney would not subpoena all social media records of every victim and potential witness as soon as charges were filed? It could be malpractice not to do so.

The SCA’s disclosure restrictions are just as reasonable and important in today’s modern era of social media. The fact that so much private content is now stored online makes the SCA’s disclosure prohibitions *more* critical

today, not less so. (See *Riley v. California* (2014) 134 S.Ct. 2473, 2485 [extending warrant requirement to cell phones in part because the “vast quantities of personal information” stored on phones and cloud storage].) It is unsurprising, then, that the California Legislature recently enacted CalECPA to reaffirm and strengthen the SCA’s protections.

In sum, the SCA is a reasonable restriction on Defendant’s ability to gather evidence and does not interfere with his constitutional rights.

**C. The prosecution’s ability to obtain records by search warrant does not make the SCA unconstitutional.**

Defendant is also wrong that the SCA is unconstitutional because it does not provide him the “same” investigatory tools as the prosecution. (OB 35.) In fact, Defendant is not seeking the same investigatory powers as the prosecution—the People cannot obtain the content of social media records without a warrant supported by probable cause (see Pen. Code § 1546.1, subds. (a), (b); *Warshak, supra*, 631 F.3d at p. 288), yet Defendant wants the ability to obtain such records with a simple subpoena.

In any event, due process does not require that a defendant have the same investigatory tools as the prosecution. As the Second Circuit explained in *Pierce, supra*, 785 F.3d at p. 842, fn. 2, it is not unusual or problematic for the government to have superior investigatory tools: “the search warrant provisions of Fed. R. Crim. P. 41(b) and the wiretap application provisions of 18 U.S.C. § 2516(1) both provide a means for the government to obtain evidence without a mechanism for defendants to do so.” (See also *Bray*, 281 Or.App. at p. 604 [holding that due process does not confer a “constitutional obligation to ensure ‘reciprocal discovery rights’ to defendant”]; *United States v. Tucker* (S.D.N.Y. 2008) 249 F.R.D. 58, 63 [same].)<sup>6</sup>

---

<sup>6</sup> In other situations where a defendant’s inaccessibility to discovery has been declared to be a due-process violation, it is because there was an asymmetry in the information being exchanged *between the Government*

Indeed, this is one of the reasons for *Brady*: because the prosecution has superior investigatory tools, the defendants must look to *the Government* for certain evidence and information. (*Wardius v. Oregon* (1973) 412 U.S. 470, 476, fn. 9 [discussing “the State’s inherent information-gathering advantages”].) If, for example, the defendant needs a pretrial lineup to develop a witness-identification defense, the solution is not to give the defendant the ability to coerce citizens into participating in a lineup; rather, the solution is to compel *the government* to conduct one on the defense’s behalf. (See *Evans, supra*, 11 Cal.3d at p. 620.)

And while *Brady* requires the government to disclose only the exculpatory fruits of any search, California law is even broader and requires the government to produce any relevant evidence it has obtained. (Pen. Code, § 1054.1, subd. (c).) Thus, the SCA’s search-warrant exception ultimately redounds to the defendant’s benefit. Should the prosecution attempt to use its search-warrant power in an unfair, one-sided fashion (for example, by requesting social media posts that are likely to include only incriminating evidence and intentionally not requesting posts that are likely exculpatory), Defendant can address that with the trial court and obtain an appropriate remedy. (See *Evans, supra*, 11 Cal.3d at p. 625.)

**D. The SCA does not provide an exception for in camera review, nor is one constitutionally required.**

Finally, Defendant suggests that Facebook should at least be required to produce records for an “in camera” review. (OB 36.) But the SCA makes no exception for in camera review, and that is a rational exercise of Congressional judgment that cannot be overturned by a state court.

---

*and the defense*, not an asymmetry with respect to access to third-party materials. (See, e.g., *Wardius v. Oregon* (1973) 412 U.S. 470 [Oregon rule forced defendants to reveal alibi witnesses but did not require prosecution to reveal alibi rebuttal witnesses].)

In camera reviews will not protect the privacy rights of people who use social media. There is no statutory basis for ensuring the account holder's participation in the in camera review. Indeed, the entire reason that Defendant claims he needs to subpoena Facebook directly is because he allegedly cannot locate the social media person whose records he seeks. Thus, the in camera determination of whether to release private records could take place without any input from the account holder. Here, Defendant argues that the victim *should not even be informed* of proceedings to release his own records, because he may be uncooperative and raise privilege objections or other privacy rights. (OB 23.)

In camera reviews also do not ensure that the prosecution will protect privacy rights of victims and witnesses. While the prosecution is entitled to learn the identity of the subpoenaed party and the "nature" of the requested documents, the prosecution is not entitled to view the actual subpoenaed documents until the defendant decides it will use that evidence at trial. (*Kling, supra*, 50 Cal.4th at p. 1077.) The trial court also has discretion to conduct hearings over the subpoenaed materials ex parte outside the presence of the prosecution. (*Ibid.*) Further, given that Defendant proposes that any in camera review take place before trial, the court has no context at that time to evaluate the constitutional significance of the request against the subscriber's privacy interests, resulting in cases where the trial court unnecessarily releases private information that is not ultimately necessary to the defense's case. (*Ante*, pp. 30–40.)

Permitting in camera reviews also undermines the efficient administration of justice. In camera review is resource-intensive for courts, litigants, and providers. The social media histories of some account holders are tens of thousands of pages long. Reviewing such documents in camera

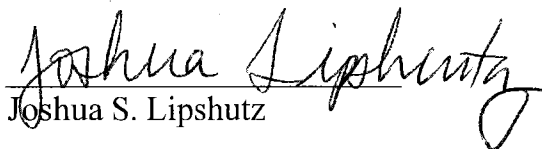
would add to California courts' docket backlogs, and would create a significant burden on the third-party providers required to produce the records. (See App'x 28.)

**CONCLUSION**

The judgment of the Court of Appeal should be affirmed.

DATED: March 19, 2018

**GIBSON, DUNN & CRUTCHER LLP**

By:   
Joshua S. Lipshutz

Attorneys for Petitioner  
Facebook, Inc.

DATED: March 19, 2018

**PERKINS COIE LLP**

By: \_\_\_\_\_  
James G. Snell

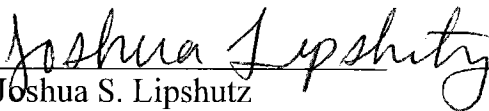
Attorneys for Petitioner  
Facebook, Inc.

## CERTIFICATE OF COMPLIANCE

Counsel of Record hereby certifies that pursuant to Rule 8.520(c)(1) of the California Rules of Court, the enclosed Petitioner's Answering Brief on the Merits is produced using 13-point Roman type and contains approximately 11,171 words including footnotes, which is less than the total words permitted by the rules of court. Counsel relies on the word count of the computer program used to prepare this brief.

DATED: March 19, 2018

**GIBSON, DUNN & CRUTCHER LLP**

By:   
Joshua S. Lipshutz

Attorneys for Petitioner  
Facebook, Inc.

Case Name: Facebook, Inc. v. Superior Court of San Diego  
Case No: S245203

### PROOF OF SERVICE

I, Lucy Ragnelli, declare as follows:

I am a citizen of the United States and employed in San Francisco County, California; I am over the age of eighteen years, and not a party to the within action; my business address is 555 Mission Street, San Francisco, CA 94105-0921. On March 19, 2018, I served the within documents:

### PETITIONER'S ANSWERING BRIEF ON THE MERITS

On the parties stated below, by the following means of service:

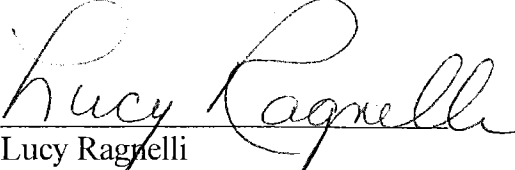
### SEE ATTACHED SERVICE LIST

- BY UNITED STATES MAIL:** I placed a true copy in a sealed envelope or package addressed to the persons as indicated above, on the above-mentioned date, and placed the envelope for collection and mailing, following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited with the U.S. Postal Service in the ordinary course of business in a sealed envelope with postage fully prepaid. I am aware that on motion of party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing set forth in this declaration.

I am a resident or employed in the county where the mailing occurred. The envelope or package was placed in the mail at San Francisco, California.

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

Executed on March 19, 2018, at San Francisco, California.

  
Lucy Ragnelli



**SERVICE LIST FOR *Facebook, Inc. v. Superior Court of San Diego***  
**CALIFORNIA SUPREME COURT CASE NO. S245203**

Superior Court of San Diego  
County: Respondent

Superior Court of San Diego County  
Central – Downtown Courthouse  
P.O. Box 122724  
San Diego, CA 92112

Court of Appeal, Fourth District,  
Div. 1

Clerk of the Court  
Court of Appeal, Fourth District,  
Div. 1  
750 B Street, Suite 300  
San Diego, CA 92101

Lance Touchstone: Real Party in In-  
terest

Katherine Ilse Tesch  
Office of the Alternate Public De-  
fender  
450 B Street, Suite 1200  
San Diego, CA 92101