

No. S245203
IN THE SUPREME COURT OF
THE STATE OF CALIFORNIA

SUPREME COURT
FILED

JUN 18 2018

~~Jorge Araverrete Clerk~~

FACEBOOK, INC.,
Petitioner,

~~Deputy~~

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. D072171; Superior Court of San Diego County, No.
SCD268262, Hon. Kenneth So, Presiding Judge

PETITIONER'S RESPONSE TO BRIEFS OF AMICI CURIAE

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. D072171; Superior Court of San Diego County, No.
SCD268262, Hon. Kenneth So, Presiding Judge

PETITIONER'S RESPONSE TO BRIEFS OF AMICI CURIAE

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
mholec@k@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	1
ARGUMENT	2
A. This Court should enforce the SCA’s important privacy protections.	2
B. Defendant’s amici have no response to Facebook’s constitutional arguments.	4
C. Defendant’s amici misrepresent Facebook’s Terms of Service.	8
CONCLUSION	13
PROOF OF SERVICE.....	14

TABLE OF AUTHORITES

	Page(s)
Cases	
<i>Byrd v. United States</i> (2018) 138 S.Ct. 1518	12
<i>City of L.A. v. Superior Court</i> (2002) 29 Cal.4th 1	5, 7
<i>Corngold v. United States</i> (9th Cir. 1966) 367 F.2d 1	13
<i>Facebook v. Superior Court (Hunter)</i> (2018) __ Cal.5th __, 417 P.3d 725	2, 3, 7, 8, 12, 13
<i>Flannery v. Prentice</i> (2001) 26 Cal.4th 572	9
<i>Montana v. Egelhoff</i> (1996) 518 U.S. 37	5
<i>O’Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423	11
<i>People v. Brown</i> (Ct. App. 1979) 88 Cal.App.3d 283	12
<i>People v. Cantor</i> (2007) 149 Cal.App.4th 961	13
<i>People v. Gurule</i> (2002) 28 Cal.4th 557	6, 7
<i>People v. Harwood</i> (1977) 74 Cal.App.3d 460	13
<i>People v. Johnson</i> (1989) 47 Cal.3d 1194	6
<i>People v. Superior Court</i> (1970) 10 Cal.App.3d 122	13
<i>Riley v. California</i> (2014) 134 S.Ct. 2473	4

<i>Rock v. Arkansas</i> (1987) 483 U.S. 44.....	5
<i>Stoner v. State of Cal.</i> (1964) 376 U.S. 483.....	12
<i>United States v. DiTomasso</i> (S.D.N.Y. 2014) 56 F.Supp.3d 584.....	13
<i>United States v. Scheffer</i> (1998) 523 U.S. 303.....	5
<i>Varjabedian v. City of Madera</i> (1977) 20 Cal.3d 285.....	9
Statutes	
Evid. Code, § 952.....	11
Other Authorities	
Aaron Mak, Vermont, <i>California Charging Ahead of Congress on Data Privacy</i> <i>Laws</i> , Slate (May 29, 2018).....	4
Adam Satariano, <i>G.D.P.R., a New Privacy Law, Makes Europe World's Leading</i> <i>Tech Watchdog</i> , N.Y. Times (May 24, 2018).....	4
Conor Dougherty, <i>Push for Internet Privacy Rules Moves to Statehouses</i> , N.Y. Times (March 26, 2017).....	4
H.R. Rep. No. 99-647, 2d Sess., p. 19.....	2
https://newsroom.fb.com/news/2018/04/data-and-advertising/	10
https://www.facebook.com/about/basics/manage-your-privacy/posts#1	10
https://www.facebook.com/about/basics/manage-your-privacy/posts#4	9
https://www.facebook.com/about/privacy/update	9
https://www.facebook.com/terms.php	10
Rules	
Cal. Rules of Court, rule 8.500(c)(1).....	9

INTRODUCTION

Defendant Lance Touchstone’s amici curiae¹ seek to weaken the important privacy protections in the Stored Communications Act (“SCA”). Amici ask this Court to rule that *every* Facebook user has impliedly consented to public disclosure of *all* of their social media communications—even the ones they specifically designate as private. But weakening the SCA in this way is not supported by the law and undermines expectations of all who use the Internet to communicate private information to friends, family members, and others.

The Constitution does not compel such privacy erosion. Indeed, the SCA already allows criminal defendants to obtain and use social media records at trial. It merely prohibits them from obtaining communications from *one particular source*—electronic communications providers. The U.S. Supreme Court and this Court have repeatedly upheld similar restrictions on evidence gathering, holding that defendants do not have an absolute right to third-party evidence from any source. Defendant and his amici offer no response to these authorities because there is none. They contend that providers are the most convenient source for obtaining electronic communications, but even if that were true, they cannot cite any case holding that the U.S. Constitution compels such convenience.

¹ Defendant’s amici are the California Public Defenders Association and the Public Defender of Ventura County (collectively, “CPDA”), San Francisco Public Defender (“SFPD”), and California Attorneys for Criminal Justice (“CACJ”).

In this case, Defendant’s counsel made no effort to obtain the records he seeks, even from his own sister, before burdening Facebook with a subpoena. The SCA rejects this approach, requiring instead that criminal defendants seek electronic communications the same way defendants have historically sought communications: from senders and recipients. That was a reasonable and constitutional decision for Congress to make. That the nature of electronic communications makes it easy to seize vast amounts of private data in one fell swoop from a single source is a reason to enforce the SCA’s protections, not to erode them.

ARGUMENT

A. This Court should enforce the SCA’s important privacy protections.

As this Court recently explained, Congress’s “most important” objective in passing the SCA was to protect privacy in the Internet age. (*Facebook v. Superior Court (Hunter)* (2018) __ Cal.5th __, 417 P.3d 725, 737 & fn.15 [quoting H.R. Rep. No. 99-647, 2d Sess., p. 19].) Congress also sought to foster the use and development of new technologies—which Congress believed would not occur if there were legal uncertainty over the privacy of electronic communications. (*Ibid.*)

The SCA has been successful in achieving its objectives. Americans rely on the SCA’s important privacy protections to communicate sensitive information to friends and colleagues. And electronic communications—as well as innovative electronic communications services—have flourished as a result.

Defendant’s amici describe the SCA as “dated” and argue that Congress failed to anticipate the Internet age and the growth of social media. (E.g., CACJ Br. at pp. 13-14.)

To the contrary, these technologies have flourished in large part *because of* the SCA’s privacy protections. If anything, Congress was remarkably prescient in recognizing the potential growth of online communications and the privacy concerns such technology would raise. The longevity of the SCA does not make it “dated”—rather, it means the SCA’s privacy protections have become part and parcel of the way people think about and use electronic communications. These longstanding expectations should not be disturbed.²

Defendant’s amici are also wrong that the growth of social media, and its growing importance in our lives, means that criminal defendants must have easy access to it. (See CACJ Br. at p. 13-14; CPDA Br. at p. 32.) They have it backwards. The fact that we now live so much of our private lives through online communication counts in favor of *more* privacy protection, not less. (See *Riley v. California* (2014) 134 S.Ct. 2473, 2485 [extending search-warrant requirement to cell phones in part because of the “vast quantities of personal information” stored on phones and cloud storage].) Every day, people communicate and store sensitive medical information, confidential financial information, and their most private photographs and videos online. These are hardly reasons to make social media *less* private and *more* accessible to third parties.

Indeed, the prevalence of social media and other forms of electronic communications is causing the world to move towards greater privacy protections in this

² See Amici Br. of Apple Inc., Google Inc., Oath Inc., Twitter, Inc., and Cal. Chamber of Commerce (“Tech Companies’ Amici Br.”) at p. 31 [explaining that weakening the SCA would “erode their trust in the technology platforms they currently rely on, and chill their communications on those platforms.”].

area, not fewer. (See, e.g., Conor Dougherty, *Push for Internet Privacy Rules Moves to Statehouses*, N.Y. Times (March 26, 2017) [“Online privacy is the rare issue that draws together legislators from the left and the far right”]; Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World’s Leading Tech Watchdog*, N.Y. Times (May 24, 2018) [“Brazil, Japan and South Korea are set to follow Europe’s lead, with some having already passed similar data protection laws”].) And the California legislature has pushed this State in the same direction. (See Aaron Mak, *Vermont, California Charging Ahead of Congress on Data Privacy Laws*, Slate (May 29, 2018).) The Court should reject amici’s efforts to move California in the opposite direction.

B. Defendant’s amici have no response to Facebook’s constitutional arguments.

Defendant’s amici ask the Court to read the SCA’s privacy protections narrowly and dodge its disclosure prohibitions to “avoid the constitutional issue.” (CPDA Br. at pp. 23, 26.) But, this Court should reach the constitutional issue and declare that the SCA is constitutional and does not violate criminal defendants’ constitutional rights. The SCA simply prevents criminal defendants from looking to electronic-communications providers as the “one stop shop” to obtain social media content shared between senders and recipients.

No court has ever held that there is a constitutional right to obtain evidence from one particular source. Defendant’s amici suggest that this Court writes on a blank slate (SFPD Br. at p. 3; CACJ Br. at p. 11), but that is not true. The U.S. Supreme Court and this Court have repeatedly upheld legislation that precludes defendants from using certain

evidence-gathering methods, and from looking to certain sources.³ None of Defendant’s amici addresses any of these cases in their briefs. Defendant’s reply brief ignored them as well.

Amicus CPDA cites *Rock v. Arkansas* (1987) 483 U.S. 44, but that case does not stand for an unlimited right to obtain evidence from any source. Rather, in *Rock*, the Court struck down a judge-made rule that precluded a criminal defendant from *testifying* because she had used hypnosis to refresh her recollection. The Court concluded that the “[w]holesale inadmissibility of a defendant’s testimony is an arbitrary restriction on the right to testify.” (*Id.* at p. 61 [italics added].) The Court, however, also made clear that “the right to present relevant testimony is not without limitation” and may “bow to accommodate other legitimate interests.” (*Id.* at p. 55.) Indeed, CPDA concedes that “[r]ules excluding evidence from criminal trials do not necessarily ‘abridge an accused’s right to present a defense so long as they are not arbitrary or disproportionate to the purposes they are designed to serve.’” (CPDA Br. at p. 28.)

Here, no one claims that the SCA’s disclosure prohibitions are arbitrary, nor do Defendant’s amici dispute that Congress had compelling reasons for enacting those prohibitions. As Facebook’s amici have explained, the SCA’s prohibitions serve vital

³ See, e.g., *United States v. Scheffer* (1998) 523 U.S. 303, 308 [upholding law precluding the defense from presenting polygraph evidence]; *Montana v. Egelhoff* (1996) 518 U.S. 37, 56 [upholding law precluding the defense from offering evidence of voluntary intoxication]; *City of L.A. v. Superior Court* (2002) 29 Cal.4th 1, 16 [upholding law barring defendants from obtaining police-officer complaints filed more than 5 years before a crime occurred].

national interests. (Tech Companies’ Amicus Br. at pp. 19–32.) That should be the end of Defendant’s constitutional challenge to the SCA.

Amici argue that social media records may be “outcome determinative” in a particular case, but even if true that is irrelevant. (CPDA Br. at p. 32.) A third-party’s confession to his attorney that he committed the crime with which defendant was charged is certainly outcome determinative, but the attorney-client privilege bars its admissibility. (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”].) Likewise, a defendant might obtain outcome-determinative evidence by wiretapping witnesses, searching through their mail, or calling witnesses who reside outside the subpoena power. But statutes limit those sources of evidence—regardless of how exculpatory they might be—because legislatures have balanced certain privacy interests, personal safety, and other burdens on society with criminal defendants’ right to procure evidence through those methods.

This Court has upheld many laws that place entire *categories* of evidence outside the defendant’s reach—for example, evidence barred by the attorney-client privilege (see *Gurule, supra*, 28 Cal.4th at p. 594), or police reports more than 5 years old (*City of L.A., supra*, 29 Cal.4th at p. 16). The SCA, in contrast, bars only a single *source* of evidence and does not preclude the defendants from obtaining the same evidence elsewhere.

In this case, contrary to amicus CPDA’s assertion, the issue of whether Defendant could have obtained the same evidence from other sources is not “hotly disputed.” (CPDA Br. at p. 16.) Defendant put *no* evidence in the record of any attempt to subpoena

the victim's friends or other contacts, including Defendant's own sister. (See Facebook's Ans. Br. at pp. 19-24; see also *Hunter, supra*, 417 P.3d at p. 747 [trial court should "require" subpoenaing party to "create a full record" on efforts to obtain records from other sources].) Rather, it appears Defendant simply decided it would be more convenient to get the victim's social media records directly from Facebook. (See Pet'n for Review, Ex. A, at p. 24. [Court of Appeal noting that it was "not persuaded that Touchstone exhausted his efforts to locate the victim"].)⁴

Moreover, because the SCA does not violate any constitutional rights, the Court should not rewrite it to provide for in-camera reviews, as amici urge. (See, e.g., CACJ Br. at p. 11; SFPD Br. at pp. 3-4.) A defendant is not entitled to in-camera review of evidence he obtained by unlawful wiretap to determine its exculpatory value. And like the law against private wiretaps, the SCA's disclosure prohibition makes no exception for in-camera review, as this Court has already explained. (See *Hunter, supra*, 417 P.3d at p. 747, fn. 32 ["neither the statutory language nor its legislative history supports amici curie's claim that the statute can reasonably be interpreted to permit disclosure of all electronic communications, public or private, to a court under all circumstances"].)

There are many good reasons for prohibiting in-camera reviews. As an initial matter, the burden on courts would be immense. But more importantly, such hearings

⁴ The trial court made no "findings"—express or implied—to the contrary. (See CPDA Br. at p. 17-18.) The trial court decided only the *legal* issue of whether a defendant's constitutional rights require compliance with a subpoena notwithstanding the SCA's disclosure prohibitions. (See App'x Ex. 7, at pp. 120, 134 [framing and ruling on the legal issue].)

would violate the privacy rights of the account holder whose records are at issue. Amici contend that the account holder's privacy could be protected by excluding criminal defendants from in-camera hearings. (CPDA Amicus Br. at p. 29.) But they ignore the critical fact that *the account holder himself* would likely be absent from any such hearing, leaving no one to protect his or her privacy interests. (See Facebook's Ans. Br. at p. 44.)

In sum, the SCA is a reasonable restriction on evidence gathering that serves many vital interests. This Court should put to rest once and for all the misguided notion advanced by Defendant and his amici that the SCA is unconstitutional.

C. Defendant's amici misrepresent Facebook's Terms of Service.

This Court held in *Hunter* that when a social media user designates a communication as private, he or she "evinces an intent *not* to consent to disclosure by a provider." (*Hunter, supra*, 417 P.3d at p. 746.) This is true regardless whether "the communication was configured by the user to be accessible to a 'large group' of friends or followers." (*Id.* at p. 749.) Nonetheless, one of Defendant's amici (CACJ) argues that *all* Facebook account holders have waived their privacy rights under the SCA and consented to disclosure of *all* of their private communications by agreeing to Facebook's Terms of Service. The argument relies on misrepresentations of Facebook's Terms of Service, ignores the settled expectations of Facebook account holders, and would lead to harmful consequences far beyond this case.

As an initial matter, the issue is not properly before this Court. Defendant did not address Facebook's Terms of Service in his merits briefs to the Court of Appeal, he did not mention them in his opening brief to this Court, and he added only a single sentence

about the Terms of Service in his reply brief. The argument has been waived, and the Court should not consider it. (See Cal. Rules of Court, rule 8.500(c)(1); *Flannery v. Prentice* (2001) 26 Cal.4th 572, 591 [declining to decide issue not raised in Court of Appeal as a matter of Court’s “ordinary policy”]; *Varjabedian v. City of Madera* (1977) 20 Cal.3d 285, 295 fn. 11 [arguments made for the first time in reply briefs are waived].)

In any event, Facebook’s account holders have not waived their privacy rights by agreeing to Facebook’s Terms of Service—which emphasize that their private communications remain private. CACJ misrepresents the Terms of Service by claiming that “any and all content [people] put on Facebook can be shared with unidentified third parties,” regardless of privacy settings. (CACJ Br. at p. 5.) In fact, Facebook’s Terms of Service and related privacy guidelines say no such thing, and repeatedly make clear that account holders decide who sees their content:

- “When you share and communicate using our Products, you choose the audience for what you share. For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people.”⁵
- “You can also choose to share publicly or with a specific group of people.”⁶
- “Every time you post a status update, photo or video, you can choose who can see it.”⁷
- “You own the content you create and share on Facebook and the other Facebook Products you use, and nothing in these Terms takes away the rights you have to your own content. You are free to share your content with anyone else, wherever you want.”⁸

⁵ <https://www.facebook.com/about/privacy/update> [underscore in original].

⁶ <https://www.facebook.com/about/basics/manage-your-privacy/posts#4>.

⁷ <https://www.facebook.com/about/basics/manage-your-privacy/posts#1>.

⁸ <https://www.facebook.com/terms.php>.

Far from “absolv[ing] itself of any responsibility to ensure the confidentiality of user data” (CACJ Br. at p. 8), Facebook informs account holders that it will not—and does not—share their private content with unauthorized third parties.

CACJ misleadingly relies on statements regarding *non-identifying, non-content* information that Facebook shares with third parties, and then portrays them as admissions that Facebook shares private “content” with others. (E.g., CACJ at p. 9.) But Facebook’s Data Policy states that, although Facebook shares aggregated statistics and reports about the kinds of people who view an advertisers’ ads and how they respond to those ads, Facebook does “*not* share information that personally identifies you ... with advertising, measurement or analytics partners unless you give us permission.” (CACJ Br. at p. 7, fn. 5.) “So our promise is this: we do not tell advertisers who you are or sell your information to anyone. That has always been true. ... We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don’t share information that personally identifies you.”⁹ Nothing in Facebook’s policies even suggests that private content is shared with advertisers.

Further, the fact that content is “collected and retained *by Facebook*” cannot, by itself, constitute consent to public disclosure. (CACJ Br. at p. 6, italics added.) Facebook could not operate its services, transmit messages, or permit account holders to view messages and other content unless Facebook itself retained that content on its servers. Indeed, the entire point of the SCA was to ensure that electronic

⁹ <https://newsroom.fb.com/news/2018/04/data-and-advertising/>.

communications do not lose their privacy protections because service providers necessarily store and transmit those communications. (See *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1447 [“Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure storage”].) The same goes for the vendors and related companies that Facebook may rely on to, among other things, provide technical infrastructure services, customer service, and facilitate payments. (CACJ Br. at p. 9, fn. 9.) Just as a lawyer must rely on support staff, paralegals, expert witnesses, messengers, and graphic artists to provide legal services to clients (see Evid. Code, § 952 [no waiver if confidential information is shared with third parties who are “present to further the interest of the client”]), so too must Facebook rely on certain partners to carry out its day-to-day operations.

Nothing in Facebook’s policies would lead account holders to expect that their private communications will be made public without their consent. The Court recognized as much in *Hunter*, when it held that “nothing of which we are aware in any of providers’ policies or answers to FAQs suggests that users would have any reason to expect that, having configured a communication to be available not to the public but instead to a restricted group of friends or followers, the user nevertheless has made a *public* communication—and hence has impliedly consented to disclosure by a service provider, just as if the configuration had been public.” (*Hunter, supra*, 417 P.3d at pp. 748-749.) Certainly nothing in Facebook’s Terms of Service puts account holders on notice that,

should they become victims or witnesses of a crime, Facebook will share all their private content with the alleged perpetrator.

Even if Facebook’s Terms of Service could be interpreted expansively to constitute a waiver of privacy—and they cannot—the Court should decline that invitation for several reasons. First, it would depart from the principle underlying the U.S. Supreme Court’s recent decision in *Byrd v. United States* (2018) 138 S.Ct. 1518, 1529, which held that an agreement between a business and customer that “concern[s] risk allocation between private parties” has “little to do with whether one would have a reasonable expectation of privacy” vis-à-vis *someone else* (in that case, the government conducting a search; in this case, a criminal defendant seeking the equivalent of a search). In other words, just because a user allegedly provides consent for one purpose, does not mean they provide consent for *all* purposes.

Second, because privacy rights are so important, courts interpret privacy waivers and statements of consent *narrowly*, and do not interpret consent to one type of disclosure as consent to other types of disclosure. (See *Stoner v. State of Cal.* (1964) 376 U.S. 483, 489 [hotel guest’s consent to hotel staff to enter room does not translate into consent to hotel staff to invite police into room]; *People v. Brown* (Ct. App. 1979) 88 Cal.App.3d 283, 290 [“Clearly, although by checking himself into a hospital, a patient may well waive his right of privacy as to hospital personnel, it is obvious that he has not turned ‘his’ room into a public thoroughfare”].)¹⁰ Indeed, broadly construing consent would


¹⁰ See also, e.g., *Corngold v. United States* (9th Cir. 1966) 367 F.2d 1, 7 [holding that giving a package to a common carrier does not mean the sender has consented to a search

have unintended consequences far beyond this case. As this Court noted in *Hunter*, if communications are deemed public, “then it would necessarily place no restriction on private party or *law enforcement* access to such communications.” (*Hunter, supra*, 417 P.3d at p. 747 [italics in original, citation omitted]). Surely, the criminal-defense bar does not wish for the government to have unfettered access to all private content on Facebook, but that is the natural consequence of their position.

CONCLUSION

The SCA protects the privacy interests of all Americans when communicating over the Internet. Eroding those protections—either by narrowly interpreting the SCA or by imputing consent when no consent actually exists—is not warranted by the Constitution and would have harmful consequences beyond this case. This Court should affirm the decision of the Court of Appeal and uphold the constitutionality of the SCA.

DATED: June 18, 2018


Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP

by customs agents]; *United States v. DiTomasso* (S.D.N.Y. 2014) 56 F.Supp.3d 584, 596-597 [although employee consented to employer’s right to search his emails for wrongdoing, he did not consent to employer doing so in cooperation with law enforcement]; *People v. Harwood* (1977) 74 Cal.App.3d 460, 468 [consent to premises search does not include the right to intercept telephone calls to the premises]; *People v. Superior Court* (1970) 10 Cal.App.3d 122, 127 [consent to enter house to search for burglar suspects did not extend to search of closets to uncover crowbar]; *People v. Cantor* (2007) 149 Cal.App.4th 961, 965-966 [search of vehicle exceeded scope of consent].

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

PROOF OF SERVICE

I, Susanne Hoang, 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, Suite 3000, San Francisco, CA 94105-0921. On June 18, 2018, I served the within documents:

PETITIONER'S RESPONSE TO BRIEFS OF AMICI CURIAE

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 June 18, 2018, at San Francisco, California.



Susanne Hoang

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 Interest

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

San Diego County District
Attorney: Intervenor

Summer Stephan, District Attorney
Mark Amador, Deputy District Attorney
Linh Lam, Deputy District Attorney
Karl Husoe, Deputy District Attorney
330 W. Broadway, Suite 860
San Diego, CA 92101

Apple Inc., Google Inc., Oath
Inc., Twitter Inc., and
California Chamber of
Commerce: Attorneys for
Amici Curiae

Jeremy B. Rosen
Stanley H. Chen
Horvitz & Levy LLP
3601 West Olive Avenue, 8th Floor
Burbank, California 91505-4681

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

Todd Howeth, Public Defender
Michael C. McMahon, Senior Deputy
Office of the Ventura County Public
Defender
800 S. Victoria Avenue, Suite 207
Ventura, CA 93009

California Attorneys for
Criminal Justice: Attorneys for
Amici Curiae

Donald E. Landis
The Law Office of Donald E. Landis, Jr.
P.O. Box 221278
Carmel, CA 93922

California Attorneys for
Criminal Justice: Attorneys for
Amici Curiae

Stephen Kerr Dunkle
Sanger Swysen & Dunkle
125 East De La Guerra Street, Suite 102
Santa Barbara, CA 93101

California Attorneys for
Criminal Justice: Attorneys for
Amici Curiae

John T. Philipsborn
Law Offices of J.T. Philipsborn
Civic Center Building
507 Polk Street, Suite 350
San Francisco, CA 94102

San Francisco Public
Defender's Office: Attorneys
for Amici Curiae

Jeff Adachi, Public Defender, City and
County of San Francisco
Matt Gonzalez, Chief Attorney
Dorothy Bischoff, Deputy Public
Defender
555 Seventh Street
San Francisco, CA 94103