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 SUPPLEMENTAL BRIEF ADDRESSING THE EFFECT OF *FACEBOOK, INC. V. SUPERIOR COURT (HUNTER)*

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 SUPPLEMENTAL BRIEF ADDRESSING THE EFFECT OF *FACEBOOK, INC. V. SUPERIOR COURT (HUNTER)*

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

TABLE OF AUTHORITIES

I. INTRODUCTION

Defendant Lance Touchstone argues that the Stored Communications Act ("SCA") is not "appropriate legislation for modern communication technology" and that its protections should not apply to social media. (Def's Reply Br. at pp. 7–10.) This Court rejected that very argument in *Facebook, Inc. v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245, holding instead that the SCA's privacy protections apply to all forms of electronic communications, including social media records.

The Court should now take *Hunter* to its logical conclusion and confirm that the SCA does not infringe on the constitutional rights of criminal defendants seeking discovery from social media providers. Neither this Court nor the U.S. Supreme Court has ever doubted the constitutionality of criminal discovery restrictions, even ones that categorically prevent the discovery of evidence that might exculpate criminal defendants—for example, laws against private wiretapping and invasions of the attorney-client privilege. (See, e.g., 18 U.S.C. § 2511; *Swidler & Berlin v. United States* (1998) 524 U.S. 399, 410.) To the contrary, evidentiary restrictions are constitutional in *all* cases as long as they further "legitimate interests" and are not "arbitrary." (*United States v. Scheffer* (1998) 523 U.S. 303, 308.)

This Court held in *Hunter* that the SCA was a rational means of furthering important national interests, including the development of new communications technologies and the protection of privacy interests in an age of electronic communications. To achieve these important goals, Congress did *not* categorically prevent the discovery of electronic communications; it merely required people to obtain

electronic communications from senders and recipients, rather than service providers—the same way parties have obtained non-electronic communications for over a century. There is nothing unconstitutional about that requirement, and this Court should say so. Otherwise, criminal defendants will continue raising case-by-case challenges to the SCA, arguing each time that the particular circumstances of their case require a constitutional exception to the law—a burdensome drain on court and party resources, and ultimately a futile exercise because, in the absence of any constitutional right to discovery, there is *no* set of circumstances that would justify violating the SCA. (See, e.g., *People v. Hammon* (1997) 15 Cal.4th 1117, 1125–1127; *People v. Gurule* (2002) 28 Cal.4th 557, 594.) This issue is ripe for review and deciding it will provide much-needed clarity for the lower courts.

Finally, the Court should hold that the SCA protects electronic communications that were previously public but are private at the time the discovery is sought. Revocation of consent is a well-recognized doctrine in the law, and there are strong policy reasons for applying it in circumstances where a person modifies the privacy settings of a post to make it non-public.

II. THE *HUNTER* DECISION

In *Hunter*, two criminal defendants served subpoenas on social media service providers Facebook, Instagram, LLC, and Twitter, Inc. The subpoenas sought public and private communications from the social media accounts of the homicide victim and a prosecution witness. The providers resisted the subpoenas because, among other reasons, the SCA precludes providers from disclosing electronic communications without the

account holder's consent. (*Hunter*, *supra*, at p. 1250.) The Court's opinion contained three holdings that are particularly relevant in this case.

First, the Court confirmed that the SCA applies to social media communications maintained by Facebook and other providers. The Court rejected the defendants' "unsupported and rather startling assertion" that there is "no such thing as true privacy" with social media, and affirmed that the SCA applied with equal force to social media communications and other forms of electronic communications. (*Hunter*, *supra*, at p. 1278.)

Second, the Court held that account holders do not impliedly consent to disclosure by sharing communications with a "large group" or friends or followers. (*Hunter*, *supra*, at p. 1281.) Indeed, "a registered user who configures a communication to be viewed by any number of friends or followers—but not by the public generally—evinces an intent *not* to consent to disclosure by a provider under 2702(b)(3), but instead to preserve some degree of privacy." (*Id.* at p. 1277.) Thus, the SCA does not permit a criminal defendant to seek non-public content from a provider.

Third, the Court held that the SCA does not prohibit the disclosure of communications configured for public access, where the public nature of the communication indicates consent to disclosure. (*Hunter*, *supra*, at p. 1274.) The Court acknowledged that public configuration does not automatically mean consent to disclose because, *inter alia*, the public configuration could have been erroneous or caused by a hacking incident. (See *id.* at p. 1287, fn. 42.) Further, the Court acknowledged that a provider could refuse to produce public communications by showing that the burden of

production outweighed any purported benefit—for example, if the requesting party could obtain the same records by other means. (*Id.* at p. 1290.)

The Court remanded for further findings, including whether the content sought by the defendants' subpoenas was configured for public or private access. (*Id.* at p. 1289.)

III. *HUNTER*'S APPLICATION TO *TOUCHSTONE*

Like the *Hunter* defendants, Touchstone argues that the SCA is not "appropriate legislation for modern communication technology" and that its protections should not apply to social media. (E.g., Def's Reply Br. at pp. 7–10.) The Court correctly rejected that argument in *Hunter* (*ante* p. 3), and should again hold that the SCA applies to all forms of electronic communications, including social media.

But the Court should also go further and resolve two questions left unanswered in *Hunter*. Specifically, the Court should hold that the SCA's disclosure restrictions do not infringe the constitutional rights of criminal defendants seeking discovery, and that account holders can revoke consent by reconfiguring communications as private.

A. The Stored Communications Act is constitutional.

Like the defendants in *Hunter*, Defendant Touchstone argues that the SCA's disclosure prohibitions violate his constitutional right to a fair trial. The constitutional issue is squarely presented in this case and deciding it will obviate needless litigation in the lower courts. Indeed, following *Hunter*, the criminal defense bar has made clear it will continue to challenge the SCA's constitutionality. (See, e.g., Ben Hancock, *Calif. Justices Leave Questions Hanging Over Defendant's Access to Private Social Media Posts*, The Recorder (May 24, 2018) [quoting defense attorney stating, "the Supreme

Court has said the door is still open for us to argue that the federal constitution requires disclosure"]; Stephanie Lacambra, *A Constitutional Conundrum That's Not Going Away—Unequal Access to Social Media Posts*, Electronic Frontier Foundation (May 31, 2018) [opining that *Hunter* "leaves untouched" the constitutional question].)

The SCA's constitutionality should not be resolved on a case-by-case basis, with each defendant attempting to show why the SCA should yield to his or her purported need for evidence. Rather, the constitutionality of an evidentiary or discovery restriction turns on whether the restriction is *reasonable*—and, if so, the restriction is constitutional in all cases. (See, e.g., *Scheffer*, *supra*, 523 U.S. at p. 308.) A rule limiting evidence presentation or discovery cannot constitute a rational exercise of legislative judgment in one case, but an arbitrary exercise in another case. For example, laws against wiretapping, unauthorized searches of third-party mailboxes, and calling witnesses who reside outside the subpoena power are constitutional restrictions on evidence-gathering in *all* cases; it would make no sense to reassess their constitutionality each time a defendant claims he can obtain critical evidence only by wiretapping a witness, searching through his mail, or calling a witness outside the subpoena power.

Likewise, the SCA's disclosure restrictions are constitutional in all cases. Congress acted rationally in requiring parties to obtain electronic communications from senders and recipients—and not from providers. As this Court recognized in *Hunter*, Congress worried that people and businesses would not use or develop new communications technologies if third parties could access those communications by

going directly to providers. (See *Hunter*, *supra*, at p. 1263.) And the SCA has been remarkably successful in furthering those vital national interests.

This Court has applied and 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.) The SCA, in contrast, bars only a single *source* of evidence and does not preclude defendants from obtaining the same evidence elsewhere.

Indeed, the parties in this case have fully briefed (at this Court's request) the many ways in which defendants can obtain electronic communications from other sources, making the SCA's constitutionality fully ripe for decision here. As Facebook explained, a criminal defendant can subpoena the senders or recipients of any of the messages he or she seeks. (Facebook's Ans. Br. at pp. 23–24.) If the defendant cannot locate those parties, he or she can ask the prosecution for assistance in serving subpoenas. (*Id.* at pp. 28–29.) And if the communications are material for the defense, it can ask the court to put the *prosecution* to the choice of obtaining the records from providers (which is permitted under the SCA) or facing appropriate evidentiary limitations, adverse instructions, or even dismissal of the action. (*Id.* at p. 30.)

Defendant Touchstone wants the special ability to obtain evidence from providers because it is often the most convenient method, but no court has held that a defendant has a constitutional right to obtain evidence from a particular source—even if it is arguably the most convenient source in a particular case. Because Congress had rational—and indeed compelling—reasons to make service providers off-limits to litigants seeking

other people's private communications, this Court should honor its judgment and reject Touchstone's constitutional challenge.

B. The SCA protects communications reconfigured as private.

In *Hunter*, the Court deferred deciding whether a provider must produce communications that were initially configured as public but later reconfigured as private. In this case, the Court should hold that reconfiguring communications from public to private eliminates any indication of consent. That holding is consistent with *Hunter* and the well-established doctrine of revocation of consent.

First, this rule is consistent with the rationale set out in *Hunter*. As this Court explained, the SCA imposes a default rule that providers may not disclose *any* communications—public or private. (*Hunter*, *supra*, at p. 1273 ["we conclude that, by virtue of section 2702(a), the Act generally and initially prohibits the disclosure of *all* (even public) communications . . . ."].) However, when a person configures content as public, this Court concluded that there is an indication the person has consented to disclosure. (*Ibid.* ["[S]ection 2702(b)(3)'s subsequent lawful consent exception allows providers to disclose communications configured by the user to be public"].) But the focus of the inquiry must always be consent—determining and honoring the account holder's wishes. (*Id.* at p. 1272 ["any restrictive privacy configuration employed by the user should be honored"], citing *Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965, 990.) When a person reconfigures a communication as private, that choice should also be honored and it should be presumed that the person either

mistakenly made the communication public in the first place, or that the person no longer consents to disclosure.

Second, the idea that consent may be revoked is well-recognized in the law. Fourth Amendment jurisprudence, for example, has long treated consent as freely revocable. (See, e.g., *Jones v. Berry* (9th Cir. 1983) 722 F.2d 443, 448 ["a person may revoke a consent to search at any time prior to the completion of the search"]; *In re Christopher B.* (1978) 82 Cal.App.3d 608, 615 [consent withdrawn where defendant consented to search of home, but then changed his mind and slammed and locked the front door].) So, too, with consent provisions in consumer-protection statutes, such as the Telephone Consumer Protection Act. (See *Van Patten v. Vertical Fitness Group, LLC* (9th Cir. 2017) 847 F.3d 1037, 1047 [allowing consumers to revoke their consent under the TCPA "is consistent with the common law principle that consent is revocable" and "is consistent with [the statute's] purpose"].) "[W]here Congress uses terms that have accumulated settled meaning under . . . the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms." (*Neder v. United States* (1999) 527 U.S. 1, 21 [citations omitted].)

Third, as described more fully in the Amici Brief of Apple Inc., Google Inc., Oath Inc., Twitter, Inc., and the California Chamber of Commerce, permitting people to revoke consent under the SCA is sound policy. If account holders could not update their privacy settings to protect their privacy interests, such a rule would "erode trust in the technology platforms [people] currently rely on, and chill their communications on those platforms."

(Amici Br. of Apple Inc., Google Inc., Oath Inc., Twitter, Inc., and the Cal. Chamber of Commerce at p. 31.)

Fourth, a contrary rule could require courts, litigants, and providers to analyze account-history reconfigurations—an incredibly burdensome and often impossible task. Moreover, as this Court observed in *Hunter*, the fact that a message was once configured as public does not necessarily mean that the account holder consented to disclosure: "any given communication . . . configured as public . . . might conceivably be [so configured] *not* by a registered user him- or herself, but by a person or entity who uses or hacks the user's account. Any such action . . . should be viewed as not constituting implied consent to disclosure by a provider." (*Hunter*, *supra*, at p. 1287, fn. 42.) Thus, a ruling that once-public means always-public would greatly complicate the determination of what information a provider could disclose, as courts would likely be forced to review a wide variety of evidence relevant to historical privacy settings on a message-by-message basis, which could involve testimony from the accountholder on the intent behind each communication and testimony from other people claiming that the communications were public. Not only would that drastically increase the burden on courts and third-party providers, but it would be prone to confusion and error.[1]

---

[1] Even requiring Facebook to produce all communications configured as *public* at the time of production is not possible using Facebook's current production tools, because those tools do not sort by privacy settings and thus do not have the ability to produce only public content. Any attempt to identify and produce solely public content would cause Facebook to incur substantial burden—a burden that outweighs any purported benefit, given that litigants can access and download the same public records online. (See *Hunter*, *supra*, at pp. 1290–1291 [noting that issue of burden may be raised in trial court].)

For these reasons, this Court should hold that the SCA protects from disclosure all electronic communications that are configured as private at the time of production.

IV. CONCLUSION

This Court should affirm the decision of the Court of Appeal and uphold the constitutionality of the SCA.

DATED: July 25, 2018

Joshua S. Lipshutz /s/#

Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP

CERTIFICATE OF WORD COUNT

I, Joshua Lipshutz, certify that, according to the software used to prepare this brief, the word count of this brief is 2,460 words, which is fewer than the 2,800 words allowed for Supplemental Briefs under California Rule of Court 8.520(d)(2). I swear under penalty of perjury that the foregoing is true and correct.

DATED: July 25, 2018

Joshua S. Lipshutz /s/
Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP

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 July 25, 2018, I served the within documents:

PETITIONER'S SUPPLEMENTAL BRIEF ADDRESSING THE EFFECT OF *FACEBOOK, INC. V. SUPERIOR COURT (HUNTER)*

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 July 25, 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