No. S230051

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA
FACEBOOK, INC., et al.,
Petitioners,
v.
SUPERIOR COURT OF THE STATE OF CALIFORNIA,
SAN FRANCISCO

Respondent.

DERRICK D. HUNTER and LEE SULLIVAN,

Real Parties in Interest.

REAL PARTIES LEE SULLIVAN AND DERRICK HUNTER'S REPLY TO PETITIONERS' SUPPLEMENTAL BRIEF

From the Published Opinion of the Court of Appeal,
First Appellate District, Division Five, No. A144315

San Francisco San Francisco Superior Court Nos. 13035657,
13035658.) The Honorable Bruce Chan, Judge, Dept. 22

JANELLE E. CAYWOOD
(CBN: 189980)
3223 Webster Street
San Francisco CA, 94123
Tel. (415) 370-2673
Fax. (888) 263-0456
Email: janelle@caywoodlaw.com
Attorney for Real Party
Lee Sullivan

SUSAN B. KAPLAN
(CBN: 57445)
214 Duboce Street
San Francisco, CA 94103
Tel. (415) 271-5944
Fax. (510) 524-1657
Email: sbkapl@yahoo.com
Attorney for Real Party
Lee Sullivan

JOSE PERICLES UMALI (CBN: 118434)
507 Polk Street, Suite 340
San Francisco, CA 94102
Tel. (415) 398-5750, Fax (415) 771-6734
Email: umali-law@att,net,
Attorney for Real Party Derrick Hunter

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES iv

ARGUMENT 1

I. THE STORED COMMUNICATIONS ACT DOES NOT PREVENT PROVIDERS FROM PRODUCING "PUBLIC" SOCIAL MEDIA POSTS AND "PRIVATE" POSTS MUST BE PRODUCED TO THE SUPERIOR COURT UPON A SHOWING OF GOOD CAUSE FOR AN *IN CAMERA* REVIEW DURING WHICH THE COURT WILL BALANCE A USER'S PRIVACY RIGHTS UNDER THE SCA AGAINST A DEFENDANT'S FEDERAL CONSTITUTIONAL RIGHTS 1

A. California Rule of Court 8.516(b) Precludes Providers' Claim of Waiver 2

B. Complete Social Media Posts are Not Available from the Users 3

C. It is Easier to Un-Ring a Bell or Un-Scream a "Scream out the Window" than to Retract a Public Post on the Internet. Therefore, Once a User Publicly Posts Information on the Internet, any Claims of Privacy Under the SCA Should be Deemed Forfeited and/or Waived. Regardless of how § 2702 is Construed, a Criminal Defendant's Federal Constitutional Rights Prevail over Conflicting Statutory Privacy Rights 4

D. Providers' Distinction Between 'Access' Under § 2701 and 'Divulging' Under § 2702 is Ultimately Meaningless in Criminal Cases. Superior Courts Judges, not Corporations, Control Third-Party Discovery in Criminal Cases 12

TABLE OF CONTENTS (CONT.)

Page

CONCLUSION 15

CERTIFICATION 17

PROOF OF SERVICE 18

TABLE OF AUTHORITIES

Cases **Page(s)**

Crispin v. Christian Audigier, Inc.
(C.D. Cal. 2010) 717 F.Supp. 2d. 965 14

Ehling v. Monmouth-Ocean Hosp. Serv. Corp
(D.N.J 2013) 961 F.Supp.2d. 659.....8,9

Freytag v. Commissioner
(1991) 01 U.S. 868 9

Johnson v. Zerbst
(1938) 304 U.S. 458 9

Konop v. Hawaiian Airlines, Inc.,
(9th Cir. 2002) 302 F.3d 868 10

Pacific Lighting Leasing Co. v. Superior Court
(1976) 60 Cal. App. 3d 552.....15

People v. Kling
(2010) 10 Cal.4th1068.....11,12

People v. Clark
(1990) 50 Cal.3d 583.....9

People v. Harris
(Crim. Ct. N.Y. 2012.) 949 N.Y.S. 2d 590 1,9

Lungren v. Deukmejian
(1988) 45 Cal.3d 727.....9

Snow v. DirectTV, Inc.,
(11th Cir 2006) 450 F.3d 1314 12

Viacom Int'l v. YouTube Inc.
(S.D.N.Y 2008) 253 F.R.D. 256.....1,10,12

TABLE OF AUTHORITIES (cont.)

Federal Statutes

18 U.S.C. § 2511(2)(g)(i).....1,2

18 U.S.C § 2701.....1

18 U.S.C. § 2702 .....passim

Legislative History

H.R. Rep. No. 99-647, (1986).....1,4

Sen. Report No. 99-541, (1986).....1

Rules of Court

Cal. Rules of Court, rule 8.516(b)(1)&(2).....2

The Web Means the End of Forgetting, Rosen Jeffrey,
New York Times Magazine, January 21, 2010 2,7,10

ARGUMENT

I. THE STORED COMMUNICATIONS ACT DOES NOT PREVENT PROVIDERS FROM PRODUCING "PUBLIC" SOCIAL MEDIA POSTS AND "PRIVATE" POSTS MUST BE PRODUCED TO THE SUPERIOR COURT UPON A SHOWING OF GOOD CAUSE FOR AN *IN CAMERA* REVIEW DURING WHICH THE COURT WILL BALANCE A USER'S PRIVACY RIGHTS UNDER THE SCA AGAINST A DEFENDANT'S FEDERAL CONSTITUTIONAL RIGHTS

The plain language of the Stored Communications Act ("SCA") set forth in 18 U.S.C. 2701, et seq., the language of other provisions of the Electronic Communications Act of which the SCA is a part, the legislative history, as well as the relevant case law make it clear that "public" social media posts fall under the SCA in that they are, like "private" posts, electronically transmitted communications as defined by § 2702 (a)(1) & (2)(A)&(B). However, the SCA's protection from unwarranted access by third parties (§ 2701 (a)(1) & (2)) and prohibition from electronic providers' unauthorized divulgement (§ 2702 (a)(1) & (2)) do not come into play where the user's "privacy interests" are eliminated when the user intentionally publicly posts information, thereby indicating the user agrees to its public use and dissemination, (H.R. Rep. No. 99-647, at p. 66 (1986); Sen. Report No. 99-541, at p. 36. (1986) *Viacom Int"l v. YouTube Inc.* (S.D.N.Y 2008) 253 F.R.D. 256, 264-265; *People v. Harris* (Crim. Ct. N.Y. 2012) 949 N.Y.S 2d 590, 593), and as an exception for providers to furnish

such "public" posts when requested. (18 U.S.C. § 2511 (2)(g)(I.)

A. California Rule of Court 8.516(b) Precludes Providers' Claim of Waiver

Petitioners' claim that defendants have waived the right to argue that the SCA does to constrain providers from producing public posts is without merit. (Pet. Supp. Br. at pp. 1-4.) Defendants agreed that social media posts fell within the ambit of the SCA insofar as they are electronically transmitted communications as defined by § 2702 (a)(1) & (2)(A)&(B), as referenced by the Court of Appeal (*Facebook, Inc. v. Superior Court* (2015) 240 Cal.App.4th 203, 213, review granted Dec. 16, 2016, No. S230051), but have not conceded that the SCA constrains providers from producing public posts. This Court's December 21, 2016, order for supplemental briefing vitiates providers' waiver argument under California Rule of Court 8.516(b) which permits this Court to decide not only any issues that are raised or fairly included in the petition or answer, applicable here, but also to "decide an issue that is neither raised nor fairly included in the petition or answer if the case presents the issue and the court has given the parties reasonable notice and opportunity to brief and argue it." (Cal. Rules of Court, rule 8.516(b)(1)&(2).) Waiver is, therefore, a non-issue in light of the Court's order for supplemental briefing.

B. Complete Social Media Posts are Not Available from the Users.

Petitioners again advance the argument that they need not produce content that was once publicly available because the information is available through other sources. (Pet. SB at pp. 1, fn. 1, 17-20.) We disagree. Again, one user is dead and the other asserted her Fifth Amendment privilege against self-incrimination so they are unavailable for subpoena. Moreover, many of the social media accounts have been deleted so the records cannot be downloaded from the internet. Therefore, the only way to ensure that the complete records have been produced to the superior court, and all exculpatory evidence produced to the defense, is for providers to produce the records as the custodian of records. Again, the issue presented herein is not how to authenticate social media records under Evidence Code § 1410, but access to the complete records in the first place when account holders are dead, unavailable, or the accounts or posts deleted. This Court should give great deference to the superior court's factual finding that the records sought were not available except through providers as custodian of records.

/

/

/

C. It is Easier to Un-Ring a Bell or Un-Scream a "Scream out the Window" than to Retract a Public Post on the Internet. Therefore, Once a User Publicly Posts Information on the Internet, any Claims of Privacy Under the SCA Should be Deemed Forfeited and/or Waived. Regardless of how § 2702 is Construed, a Criminal Defendant's Federal Constitutional Rights Prevail over Conflicting Statutory Privacy Rights

Petitioners concede that 18 U.S.C § 2702(a)(1) and (2) does not preclude providers from divulging public social media posts because the users consented to their release under § 2702(b)(3). (Pet. SB at pp. 4-6.) To that end, the Legislative History to § 2702 provides as follows:

> Consent may also flow from a user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use-e.g., continued use of such an electronic communication system. Another type of implied consent might be inferred from the very nature of the electronic transaction. For example, a subscriber who places a communication on a computer "electronic bulletin board," with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication. If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.

(H.R. Rep. No. 99-647, at p. 66 (1986).)

Notably, providers are silent about their terms of service in their supplemental brief. In Facebook's privacy policy, users are specifically advised, "you control what you share" and "to let anyone see something you

post, including strangers and people who aren't on Facebook, chose Public [control settings." (See https://www.facebook.com/about/basics/ what-others-see-about-you) Facebook users can also change the privacy settings on any given posts to completely private, any number of friends up to 5,000 friends, and to be visible to any friends of those 5000 friends. (*Ibid.*) A user can change the privacy settings on a post an unlimited number of times. (*Ibid.*) A user can also send a direct message to anyone on Facebook. (https://www.facebook.com/help/142031279233975.)

Twitter's privacy policy advises users that the user's posts are generally public by default: "Twitter *broadly and instantly disseminates* your public information to a wide range of users, customers, and services, including search engines, developers, and publishers that integrate Twitter content into their services, and organizations such as universities, public health agencies, and market research firms that analyze the information for trends and insights." (https://twitter.com/privacy, emphasis added.) [1]

---

[1] Twitter's privacy policy states as follows:

> Twitter is primarily designed to help you share information with the world. Most of the information you provide us through Twitter is information you are asking us to make public. You may provide us with profile information to make public on Twitter, such as a short biography, your location, your website, date of birth, or a picture. Additionally, your public information includes the messages you Tweet; the metadata provided with Tweets, such as when you

Twitter also allows users to send direct messages to users and send restricted tweets to an any number of users.) (*Ibid.*)

Instagram is an smart phone application that lets users share photos. "Followers" can comment on the photos and tag others. Instagram users can share photos simultaneously on Instagram and Facebook. Instagram accounts are generally set to public by default so any stranger can see a user's photographs on the internet, even strangers who do not have an Instagram account. Any Instagram user can "follow" an account that is set to public. (https://help.instagram.com/116024195217477.) However, with a swipe of a finger, a user can change his or her account to "private" in which case only those subscribers who the user accepts as "followers" can see the posts. (*Ibid.*) Notably, there is no limit on how many times a user can change his or her privacy configurations on Instagram. (*Ibid.*) A user can

---

> Tweeted and the client application you used to Tweet; information about your account, such as creation time, language, country, and time zone; and the lists you create, people you follow, and Tweets you Like or Retweet. Twitter broadly and instantly disseminates your public information to a wide range of users, customers, and services, including search engines, developers, and publishers that integrate Twitter content into their services, and organizations such as universities, public health agencies, and market research firms that analyze the information for trends and insights. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public. We may use this information to make inferences, like what topics you may be interested in. (See https://twitter.com/privacy)

of time.

For example, if a user's posts were publicly available for five years, but then she changed the privacy settings to private, or to be accessible only to 50 friends/followers, on the same day a subpoena was issued, is it really reasonable to argue she "actively restrict[ed] the public from accessing the information[?]" (*Ehling v. Monmouth-Ocean Hosp. Serv.Corp.* (D.N.J. 2013) 961 F.Supp.2s 659, 668.) No. Information publicly posted on the internet can and will be instantly disseminated. The *Ehling* decision is nearly four-years old and is already out-of-step with technology that permits the instantaneous dissemination of public, or widely disseminated, content. It's analysis is simply unworkable and, if followed, would lead to absurd results.

For example, what if a user changed his privacy settings 100 times on a given post - from public, to private, then to be accessible to 475 "friends", then back to public - and so on? Is it reasonable in that scenario to argue that he revoked his consent to publicly disclose information if providers received a subpoena on a day the post was configured to private? No. Any reasonable user knows once you make information publicly available on social media it can and will be ". . . *broadly and instantly disseminate[d]* . . . to a wide range of users, customers, and services,

including search engines, developers, and publishers . . ." just as Twitter advises in its terms of service. (https://twitter.com/privacy.)

Revoking consent to publicly disseminate is as possible as un-ringing a bell or un-screaming "a scream out the window" which, like a tweet, the user has "now gifted to the world." (*Harris*, *supra*, 949 N.Y.S. 2d 590, at 593-594.) Some things cannot be meaningfully undone. Accordingly, this Court must reject providers' statutory construction of 2702(b)(3) which would allow users to revoke consent to disclose by restricting access after public dissemination because that interpretation would lead to absurd results. If a statute is susceptible to more than one interpretation, courts must adopt the reasonable meaning and reject that which would lead to an unjust and absurd result. (*See People v. Clark* (1990) 50 Cal.3d 583, 605; *Lungren v. Deukmejian* (1988) 45 Cal.3d 727, 735.)

The better construction of § 2702 is to hold that once a social media user makes information publicly accessible on the internet to more than a very small number of people, the user waives or forfeits his or her right to assert the privacy protections of the SCA, even if the account or posts are later deleted or privacy settings restricted. Forfeiture is the failure to make the timely assertion of a right, waiver is the intentional relinquishment or abandonment of a known right. (See generally *Johnson v. Zerbst* (1938) 304

U.S. 458, 464; *Freytag v. Commissioner* (1991) 01 U.S. 868, 894, n. 2 (1991) [SCALIA, J., concurring in part and concurring in judgment] (distinguishing between "waiver" and "forfeiture".) This construction of § 2702 is keeping with technological changes since *Konop v. Hawaiin Airlines* (9th Cir. 2002) 302 F.2d 868 and *Viacom, supra*, 253 F.R.D. 256 were decided. Now, users can make instant and frequent changes to privacy settings via smart phones. This technology was not available when those cases were decided. Applying waiver/forfeiture principles to privacy claims under the SCA is consistent with society's understanding that sharing information on social media, is not a private communication unless the post is configured to private *at all times* or the information is made accessible to only a very small number of friends/followers. To that end, Facebook C.E.O. Mark Zuckerberg has stated as follows, as described by author and professor, Jeffrey Rosen in New York Magazine:

> In defending Facebook's recent decision to make the default for profile information about friends and relationship status public rather than private, Zuckerberg said in January to the founder of the publication TechCrunch that Facebook had an obligation to reflect "current social norms" that favored exposure over privacy. "People have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time," he said.

(*The Web Means the End of Forgetting*, Rosen Jeffrey, New York Times Magazine, January 21, 2010, at p. 5.) Because of the shifting societal

norms described by Zuckerberg, as well as the technological changes that permit instantaneous dissemination of social media posts made public, if a user publicly posts information on the internet, any claims that the user did not consent to disclosure under § 2702(b)(3) should be deemed waived or forfeited.

Given that privacy settings for social media posts can be changed an unlimited number of times, the only real solution is to permit superior court judges to review social media records *in camera* once a criminal defendant shows good cause following a subpoena to providers under Penal Code section 1326. The superior court can review the current and past privacy settings on the user's account and on individual posts, and take the user's efforts to keep posts private into consideration when balancing the user's privacy rights under the SCA against a criminal defendant's federal constitutional rights. Posts or communications limited to a small number of people would be afforded greater weight than public posts or posts to, for example, 1000 people. To the extent a superior court determines electronic records are material to the defense and outweigh the user's privacy interests under the SCA, the records should be released to the defense subject to a protective order prior to trial so the defense has time to meaningful review the records, investigate any information contained therein, and mount an

intelligent defense. (See generally *People v. Kling* (2010) 10 Cal.4th 1068.)

D. Providers' Distinction Between 'Access' Under § 2701 and 'Divulging' Under § 2702 is Ultimately Meaningless in Criminal Cases. Superior Courts Judges, not Corporations, Should Control Third-Party Discovery in Criminal Cases

Providers contend that legislative history suggesting that public content is not subject to the SCA applies only § 2701, not § 2702, or Chapter 121 or the SCA as a whole. (Pet. SB at pp. 7-10.) We believe this interpretation is ultimately meaningless in criminal cases. Legislative history and case law clearly states that the SCA does not prohibit access to electronic records configured to public when made. (See Sen. Report No. 99-541, at p. 36 (1986); H.R. Rep. No. 99-647, at pp. (1986); *Snow v. DirectTV, Inc.*, (11th Cir 2006) 450 F.3d 1314, 1321; *Viacom, supra,* 253 F.R.D. 256, 265; *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F.Supp. 2d. 965.) Petitioners further argue that the "public content" exception to the SCA applies only to non-user "access" under § 2701, not to providers "divulging" public records pursuant to a subpoena under § 2702. (Pet. SB at pp. 8-10.) However, assuming *arguendo* that providers are correct, this distinction is without significant import.

As discussed, *ante*, in Subsection C, the restrictions under § 2702 against providers producing records in response to a subpoena do not apply

when users make content publicly available because the consent to disseminate is implied. (18 U.S.C. 2702(b)(3); H.R. Rep. No. 99-647, at p. 66 (1986).) Therefore, petitioners essentially concede public content is not protected under § 2701 or § 2702 regardless of whether it is not subject to the SCA at all or a user's is deemed to have consented to disclosure by public posting the records.

Defendants assert that once a post is made public or provided to a large group, the user has waived and/or forfeited the right to complain about privacy breaches under the SCA. This construction is consistent with common knowledge that public internet posts are not truly gone even if deleted or configured to private. The longer the post is publicly available, the more this statement is true. Cases relying on computer bulletin boards are outdated and do not take into account new technology which permits the unlimited and instant changing of privacy settings, as well as instantaneous sharing of information made publicly available. The only real solution is for providers to give social media records to superior court judges and permit them to weigh the privacy interests of the users under the SCA against a criminal defendant's federal constitutional rights. Public content that was public for an extended period or time, or disclosed to large groups would be entitled to less weight than private content or content that was

disclosed to a small number of people. Protective orders should issue to protect social media users.

Providers' self-serving argument that they should have the unfettered discretion under Section 2702(b)(3) to decide whether or not public content should be provided to a criminal defendant upon a properly issued subpoena aggrandizes their role in both the criminal justice system and the world in general. It is superior court judges, not Facebook, Twitter, and Instagram employees, who take an oath to enforce and protect criminal defendants' federal constitutional rights, and who control discovery in criminal cases. The construction of § 2702(b)(3) that providers advance is absurd, unfair and must be rejected. As discussed in detail in *Kling*, "[i]it is undisputed that trial courts are authorized, indeed even obligated, to regulate the use of subpoenas to obtain privileged third party discovery." (*Kling*, *supra*, 50 Cal.4th at 1074, quoting *People v. Superior Court* (*Humberto S.*) 43 Cal.4th 747, 751.) The permissive language that providers "may" disclosed content based on content simply means that they are not statutorily barred from producing public content if it is subpoenaed. Given the important federal constitutional rights at stake for criminal defendants, this Court should construe § 2702(b)(3) to mean that providers must produce public content to a superior court upon a properly issued subpoena because the user's

consent is implied. The litany of civil cases providers rely upon to argue that providers, not courts, should control dissemination are inapt because they do not address the fact that a criminal defendant has a panoply of federal rights not available to civil litigants. (Pet. SB at pp. 12-15.) For that reason, "[i]t has long been held that civil discovery procedure has no relevance to criminal prosecutions." (*Pacific Lighting Leasing Co. v. Superior Court* (1976) 60 Cal. App. 3d 552.)

CONCLUSION

Defendants agree with providers on one key point: That "resolving the issues raised in this Court's supplemental briefing order will not allow the Court to avoid the constitutional questions presented in this case." (Pet. SB at pp. 3-4.) A criminal defendant's federal constitutional right to procure exculpatory evidence from third-parties must be reconciled with the SCA. Accordingly, this Court should affirm respondent court's ruling and hold that the SCA does not preclude a superior court judge from reviewing the social media records subpoenaed by Mr. Sullivan and Mr. Hunter in light of the important federal constitutional rights at stake. Providers should be ordered to produce the subpoenaed records to the superior court for an *in camera* review. Any exculpatory evidence contained therein should be produced to the defense subject to protective orders. Mr.

Sullivan and Mr. Hunter's federal constitutional rights are meaningless unless relevant social media evidence is produced prior to trial in time for a meaningful opportunity to review, investigate, and mount a cogent defense. Any inconvenience to providers in responding to criminal subpoenas pales in comparison to the billions they earn when measured against the rights of criminal defendants who face life sentences.

Respectfully submitted this 6th day of February, 2017.

By: JANELLE E. CAYWOOD
Attorney for Real Party
LEE SULLIVAN

SUSAN A. KAPLAN
Attorney for Real Party
LEE SULLIVAN

JOSE PERICLES UMALI
Attorney for Real Party
DERRICK HUNTER

CERTIFICATION

I hereby certify that Real Parties Lee Sullivan and Derrick Hunter's Reply to Petitioners' Supplemental Brief consists of 3576 words and that the font used was 13 point Times New Roman.

Dated: February 6, 2017

Respectfully Submitted,

JANELLE E. CAYWOOD
Attorney for Real Party
Lee Sullivan

PROOF OF SERVICE BY U.S. MAIL

Re: Facebook v. Superior Court No. S230051

I, JANELLE E. CAYWOOD, declare that I am over 18 years of age and not a party to the within cause; my business address is 3223 Webster Street, San Francisco, California 94123. On February 6, 2017, I served a **REAL PARTIES LEE SULLIVAN AND DERRICK HUNTER'S REPLY TO PETITIONERS' SUPPLEMENTAL BRIEF** on each of the following by placing a true copy thereof enclosed in a sealed envelope with postage fully prepaid and deposited in United States mail addressed as follows:

Heather Trevisan
Office of the San Francisco District Attorney
850 Bryant Street, Third Floor
San Francisco, CA 94103

Hon. Bruce Chan
San Francisco Superior Court
850 Bryant Street, Third Floor
San Francisco, CA 94103

James Snell
Perkins Coie, L.lp.
3150 Porter Drive
Palo Alto, CA 94304

Court of Appeal, First District
Division Five
350 McAllister Street
San Francisco, CA 94102

Eric Miller
John Tyler
Perkins Coie, Llp.
1201 Third Avenue, Suite 4900
Seattle Washington 98101

Donald M. Falk
Mayer Brown, LLP
Two Palo Alto Square
3000 El Camino Real
Palo Alto CA 94306

Donald Landis
Monterey County Public Defender
111 W.Alisal Street
Salinas, CA 93901

Jeff Adachi
Dorothy Bischoff
San Francisco Public Defender's Office
555 7th Street
San Francisco, CA 94103

Michael McMahon
800 S. Victoria Street
Ventura, CA 93009

John Phillipsborn
507 Polk Street, Suite 350
San Francisco, CA 94102

David Porter
Office of the Federal Public Defender
801 I Street, 3rd Floor
Sacramento, CA 95814

I declare under penalty that the foregoing is true and correct. Executed this 6th day of February, 2017, at San Francisco, California.

JANELLE E. CAYWOOD