

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.

SUPREME COURT
FILED

JAN 23 2017

Jorge Navarrete Clerk

Deputy

**REAL PARTIES LEE SULLIVAN AND DERRICK HUNTER'S
SUPPLEMENTAL BRIEF AS ORDERED BY THE COURT
ON DECEMBER 21, 2016**

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. SOCIAL MEDIA POSTS MADE PUBLIC WHEN PUBLISHED ARE NOT PROTECTED BY THE SCA AND MUST BE DISCLOSED PRIOR TO TRIAL WHEN SUBPOENAED. SOCIAL MEDIA POSTS AND PRIVATE MESSAGES THAT ARE SUBJECT TO THE SCA, MUST BE PRODUCED TO SUPERIOR COURTS FOR AN <i>IN CAMERA</i> REVIEW PURSUANT TO <i>PENNSYLVANIA v. RICHIE</i> AND <i>DAVIS v. ALASKA</i> , UPON A SHOWING OF GOOD CAUSE, TO DETERMINE IF RECORDS SHOULD BE PROVIDED TO THE DEFENDANTS TO PRESERVE THEIR CONSTITUTIONAL RIGHTS TO DUE PROCESS AND A FAIR TRIAL, TO PRESENT A COMPLETE DEFENSE, TO EFFECTIVE ASSISTANCE OF COUNSEL, AND TO CROSS-EXAMINE ADVERSE WITNESSES	1
A. <u>Reneesha Lee and Joaquan Rice’s Public Posts on Twitter, Instagram, and Facebook Should Be Produced Prior to Trial Because Electronic Information Configured to Public at the Time of Posting Does Not Fall Within the Ambit of the SCA</u>	1
B. <u>Social Media Posts to “Friends”, “Friends of Friends”, or “Followers” are Essentially Public Posts and Should Be Exempted from the SCA Because the User Has No Reasonable Expectation of Privacy in Posts Sent to the Masses</u>	7
C. <u>Because 18 U.S.C § 2702 is Not an Absolute Bar to the Dissemination of Private Electronic Records, the United States Constitution Mandates that the SCA Yield if the Records Sought Are Necessary For a Fair Trial</u>	14

TABLE OF CONTENTS (CONT.)

CONCLUSION 22

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Chaney v. Fayette County Pub. School</i> (2013) 977 F.Supp 2d 1308	10
<i>Crispin v. Christian Audigier, Inc.</i> (C.D. Cal. 2010) 717 F.Supp. 2d. 965.....	11,12,14
<i>Davis v. Alaska</i> (1974) 415 U.S. 308	18,19
<i>Ehling v. Monmouth-Ocean Hosp. Serv. Corp</i> (D.N.J 2013) 961 F.Supp.2d. 659.....	11,12, 14
<i>Fawcett v. Altieri</i> (Supp. 2013) 960 N.Y.S. 2d 592.....	9
<i>Guest v. Leis</i> (6 th Cir. 2001) 255 F.3d 325	9
<i>Konop v. Hawaiian Airlines, Inc.,</i> (9 th Cir. 2002) 302 F.3d 868	5
<i>Lockhart v. Fretwall</i> (1993) 506 U.S. 364.....	11
<i>Patterson v. Turner Construction Company</i> (1 st Dept. 2011) 88 A.D. 3d 931	9
<i>Pennsylvania v. Ritchie</i> (1987) 480 U.S. 39	16,17,18
<i>People v. Harris</i> (Crim. Ct. N.Y. 2012.) 949 N.Y.S. 2d 590	5
<i>People v. Superior Court (Moore)</i> (1996) 50 Cal. App. 4th 1202.....	11.

TABLE OF AUTHORITIES (cont.)

Cases	Page(s)
<i>Snow v. DirectTV, Inc.</i> , (11 th Cir 2006) 450 F.3d 1314	4,5
<i>United States v. Lifshitz</i> (2d Cir. 2004) 369 F.3d 173	8,9
<i>United States v. Meregildo</i> (2012) 883 F.Supp 523.....	9,10
<i>United States v. Steiger</i> (11 th Cir. 2003) 318 F.3d 1039.....	12
<i>Viacom Int'l v. YouTube Inc.</i> (S.D.N.Y 2008) 253 F.R.D. 256.....	3, 14
 Federal Statutes	
18 U.S.C. §§ 2510	3
18 U.S.C. § 2511(2)(g).....	4,5,12
18 U.S.C. § 2702	passim
 Legislative History	
H.R. Rep. No. 99-647, (1986).....	3
Sen. Report No. 99-541, (1986).....	2
131 Cong. Rec. S11790-03 (1985).....	3
131 Cong. Rec. E4128 (1985)	3
132 Cong. Rec. H4039, (1986)	2

TABLE OF AUTHORITIES (cont.)

Articles

Edwards, Ben. J.; *The Lost Civilization of Dial-Up Bulletin Board Systems*, *The Atlantic*, Nov, 4, 2016.....13

Zwillinger, Marc J., Genetski, Christian S.; *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, *Journal of Criminal Law and Criminology*, Northwestern University School of Law, Vol. 97, No. 2, 2007.....2, 20,21

ARGUMENT

I. SOCIAL MEDIA POSTS MADE PUBLIC WHEN PUBLISHED ARE NOT PROTECTED BY THE SCA AND MUST BE DISCLOSED PRIOR TO TRIAL WHEN SUBPOENAED. SOCIAL MEDIA POSTS AND PRIVATE MESSAGES THAT ARE SUBJECT TO THE SCA, MUST BE PRODUCED TO SUPERIOR COURTS FOR AN *IN CAMERA* REVIEW PURSUANT TO *PENNSYLVANIA v. RICHIE* AND *DAVIS v. ALASKA*, UPON A SHOWING OF GOOD CAUSE, TO DETERMINE IF RECORDS SHOULD BE PROVIDED TO THE DEFENDANTS TO PRESERVE THEIR CONSTITUTIONAL RIGHTS TO DUE PROCESS AND A FAIR TRIAL, TO PRESENT A COMPLETE DEFENSE, TO EFFECTIVE ASSISTANCE OF COUNSEL, AND TO CROSS-EXAMINE ADVERSE WITNESSES

A. Reneesha Lee and Joaquan Rice’s Public Posts on Twitter, Instagram, and Facebook Should Be Produced Prior to Trial Because Electronic Information Configured to Public at the Time of Posting Does Not Fall Within the Ambit of the SCA

Defendants Sullivan and Hunter assert that public postings of social media do not fall within the ambit of 18 U.S.C. § 2702 which prohibits providers from disseminating content-based electronic communications to citizens other than law enforcement. (18 U.S.C § 2702.) The Stored Communications Act (“SCA”) was enacted by Congress in 1986 as part of the Electronic Communications Privacy Act (ECPA). (See Pub.L. No.99-508, 100 Stat, 1848.) Title II of the ECPA contains the SCA, which was designed to “address [] access to stored wire and electronic communications

and transactional records.” (Sen. Report, 99-541, at 3 (1986).) Specifically, the legislative history makes it clear the ECPA was enacted to update the then existing federal wiretap law by bridging the gap in the Fourth Amendment, which only protected the privacy of physical locations such as “persons, places, and things” not necessarily the growing number of electronic communications stored by third-parties. (See 132 Cong. Rec. H4039 (1986) [statement of Rep. Kastenmeier; see also Sen Rep. No. 99-541, at 3-5.) “Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.” (Sen. Rep, No. 99-541, at 5 (1986).) The SCA was meant to “fill precisely this gap, and in essence, to create a Fourth Amendment Lite by statute.” (Zwillinger, Marc J., Genetski, Christian S.; *Criminal Discovery of Internet Communications Under the Stored Communications Act: It’s Not a Level Playing Field*, Journal of Criminal Law and Criminology, Northwestern University School of Law, p. 576, Vol. 97, No. 2, 2007.) At the time the SCA was enacted in 1986, electronic person-to-person communications “was at its nascent stage, and large scale third party data storage and processing was only an emerging business.” (*Id.* at 573, fn. omitted.) The SCA was therefore conceived before the World Wide Web, and certainly did not contemplate the use of Yahoo!, Gmail, Hotmail, much less social media such as

Facebook, Twitter, and Instagram.

The ECPA's legislative history makes it clear that electronic records made readily available to the public are not protected by the SCA. For example, the legislative history states that "a subscriber who places a communication on a computer 'electronic bulletin board' with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure of use of the communication." (H.R. Rep. No. 99-647, at 66 (1986).) Moreover, since its inception, the ECPA provided "several clear exceptions to the bar on interception so as to leave unaffected electronic communication made through an electronic communication system designed so that such communication is readily available to the public." (131 Cong. Rec. S11790-03 (1985) [statement of Sen. Leahy on a bill that was the precursor to the ECPA]; *see also* 131 Cong. Rec. E4128 (1985) [statement of Rep. Kastenmeier on the same bill]; *See also Viacom Int'l v. YouTube Inc.* (S.D.N.Y. 2008) 253 F.R.D. 256.)

Indeed, the provision of the ECPA governing federal wiretaps also explicitly states: "It shall not be unlawful under this chapter [18 U.S.C. §§ 2510 et. seq.] or chapter 121 of this title [referring to the SCA at 18 U.S.C. §§ 2701, et. seq.] for any person-(I) to intercept or access an electronic

communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public* ." (18 U.S.C. § 2511(2)(g), emphasis added). Thus, the legislative history and the statutory scheme under the ECPA clearly show that Congress did not intend to criminalize or create civil liability for acts of individuals who intercept or access communications that are otherwise readily accessible by the general public. Accordingly, we agree that social media posts made public at the time they were configured do not fall within the ambit of 18 U.S.C. § 2702, the provision of the SCA which prohibits providers from disclosing of content-based electronic records except to the government under a myriad of enumerated exceptions.

This Court has asked the parties to address cases which have interpreted the SCA to mean that electronic information is statutorily protected so long as the communicator actively restricts the public from accessing the information. For example, in *Snow v. DirectTV, Inc.*, (11th Cir 2006) 450 F.3d 1314, the court held "an express warning on an otherwise accessible webpage" is insufficient to give rise to SCA protection because it did to restrict access to the public. In *Snow*, the plaintiff sued DirectTV under the SCA for accessing his website and computer bulletin board. The federal appellate court affirmed the order dismissing the case for failure to

state a claim because the SCA only applies if the public is generally restricted from accessing the web site. (*Id.* at 1321-1323.) In *Snow*, any member of the public could access the bulletin boards by creating a password and clicking to agree to accept the terms of the web site. (*Id.* at 1321.) The court ruled, “In order to be protected by the SCA, an internet website must be configured in some way so as to limit ready access to the general public.” (*Id.* at 1322.)

In so ruling, the *Snow* court distinguished *Konop v. Hawaiian Airlines, Inc.*, (9th Cir. 2002) 302 F.3d 868. In *Konop*, plaintiff Konop created a list of Hawaiian Airlines employees who were eligible to access the website criticizing the airlines. (*Id.* at 872.) To gain access, one had to enter an eligible employee's name, create a password, and click "SUBMIT" indicating acceptance of the terms and conditions, which prohibited users from disclosing the website's contents and prohibited viewing by Hawaiian Airlines management. (*Id.* at 872-873.) *Konop*'s website, unlike *Snow*'s, required users wishing to view the bulletin board, to have knowledge not readily available to the public, such as the eligible employee's name. In *Konop*, the communications fell within the ambit of the SCA (though an exception was found to apply) because the records were restricted. (*Id.*)

The notion that public social media posts do not fall within the ambit

of the SCA is further supported by *People v. Harris* (Crim. Ct. N.Y. 2012.) 949 N.Y.S. 2d 590. In *Harris*, the defendant in a criminal case was charged with disorderly conduct. (*Id.* at 591-592.) The prosecutor sent a subpoena to Twitter seeking the defendant's tweets and account information because it was relevant to the ongoing investigation. (*Ibid.*) The defendant filed a motion to quash which was denied. (*Id.* at 592.) Twitter was served with the order to produce the records and thereafter moved to quash the trial subpoena on grounds the records were protected by the SCA. (*Ibid.*) The court ordered the records produced holding there is no reasonable expectation of privacy in "a tweet sent around the world." (*Id.* at 593.) Specifically, the court ruled defendant's Fourth Amendment rights were not violated because the Fourth Amendment does not protect information in the hands of third parties and because there is no reasonable expectation of privacy in tweets the user has made public, even if later deleted. (*Id.* at 594.) "If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interests in your tweets, which you have now gifted of the world." (*Ibid.*)

Snow and *Harris* support the notion that social media posts made with privacy settings configured to public, do not fall within the ambit of the 18 U.S.C. § 2702 of the SCA because the general public had ready

access to them when they were posted. In light of the foregoing, the providers must produce all of Joaquin Rice and Reneesha Lee public posts on Facebook, Instagram, and Twitter pursuant to subpoena. Ms. Lee cannot produce them because she has deleted many of her accounts and has asserted her Fifth Amendment rights when asked to authenticate the social media records. Mr. Rice cannot produce his public posts because he is deceased. The records must come from the providers who are the custodian of records given many of the accounts are now deleted.

B. Social Media Posts to “Friends”, “Friends of Friends”, or “Followers” are Essentially Public Posts and Should Be Exempted from the SCA Because the User Has No Reasonable Expectation of Privacy in Posts Sent to the Masses

When the SCA was enacted in 1986, neither the World Wide Web nor social media had been invented. As discussed, *ante*, both the legislative history as well as 18 U.S.C § 2511(2)(g) establish that electronic communications made public are not subject to the SCA. Similarly, posts to hundreds or thousands of “friends”, or “friends of friends”, are essentially public given there is no restriction on the receivers of the posts from disseminating that information to others still. The user loses control over dissemination once the information is posted. Given that both social media smart cellular telephone applications (“apps”) and smart phones are used by

virtually all citizens of modest means in the United States, it is commonly understood that posts limited to one's 500 closest "friends" can be instantly disseminated to unknown others if the user's "friend" takes a screen shot of the post with a smart phone and thereafter shows, texts, or emails that image to others with whom the user is not connected. Thus, once a photograph or post is posted to a large group of followers, that user has no reasonable expectation of privacy in that post since there is no restriction on its subsequent dissemination by "friends" and "followers." Neither social media platforms, social media cellular telephone apps, nor "smart" cellular telephones, were contemplated by the drafters of the SCA when it was enacted. This technology is too different to fit squarely under the SCA which did not concern electronic records that were widely disseminated. Therefore, when a provider receives a subpoena for posts made to a large group, the SCA should be deemed inapplicable because social media posts to large groups are essentially public posts in which the user has no reasonable expectation of privacy.

In other contexts, courts have emphasized that social media posts are not entitled to heightened privacy protections just because they are limited to "friends." Generally, people have a reasonable expectation of privacy in the contents of their home computers. (See *United States v. Lifshitz* (2d Cir.

2004) 369 F.3d 173, 190.) However, this expectation is not absolute and may be extinguished when a computer user transmits information over the internet. (*Id.* at 190; see also *Guest v. Leis* (6th Cir. 2001) 255 F.3d 325, 333.) In *Patterson v. Turner Construction Company* (1st Dept. 2011) 88 A.D. 3d 931, the appellate division held that the materials posted on a Facebook page would not be shielded from discovery in a civil case “merely because plaintiff used the service’s privacy settings to restrict access” if a showing is made that the records sought are material and relevant to the litigation. (*Ibid.*) In *Fawcett v. Altieri* (Supp. 2013) 960 N.Y.S. 2d 592, the court held that social media accounts are freely discoverable and do not require court orders to disclose because social media subscribers “share their political views, vacation pictures, and various other thoughts and concerns that subscribers deem fit to broadcast to those viewing the internet. Whether these broadcasts take the form of ‘tweets,’ or postings to a user’s ‘wall,’ the intent of the users is to disseminate this information.” (*Id.* at 596.) Therefore, the court reasoned, these materials should be produced in civil discovery, even if the social media posts are closed or private, if material and necessary to the case. (*Id.* at 597-598.)

Also, instructive is *United States v. Meregildo* (2012) 883 F.Supp 523. There, defendant Colon moved to suppress evidence the government

had obtained from his Facebook account by getting one of his “friends” to give the government access to defendant’s account. (*Ibid.*) The district court denied the motion holding that the defendant did not have a reasonable expectation of privacy in Facebook posts he shared with “friends” but not the public at large. (*Ibid.*) In so ruling, the court stated as follows:

While Colon undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his "friends" would keep his profile private. [citation omitted.] And the wider his circle of "friends," the more likely Colon's posts would be viewed by someone he never expected to see them. Colon's legitimate expectation of privacy ended when he disseminated posts to his "friends" because those "friends" were free to use the information however they wanted—including sharing it with the Government. Cf. *Guest*, 255 F.3d at 333 (finding that an e-mail sender—like a letter writer—loses their expectation of privacy upon delivery). When Colon posted to his Facebook profile and then shared those posts with his "friends," he did so at his peril.

(*Id.* at 526; see also *Chaney v. Fayette County Pub. School* (2013) 977

F.Supp 2d 1308, 1315 [no reasonable expectation of privacy in Facebook posts shared with “friends of friends” because she made her information available to hundreds or thousands of people she did not know.]

Similarly, Reneesha Lee and Joaquan Rice’s social media posts that are not public, but disseminated to large groups of “friends” and “followers,” or “friends of friends,” should not be protected by the SCA because they have no reasonable expectation of privacy in posts they

disseminate to masses. These records are not private because “friends” and “followers” have the unfettered discretion to share and disseminate their posts even if restricted when published. Social media posts to the masses should not fall within the ambit of the SCA because they are essentially public posts. The SCA does not protect electronic records that are publicly available. Social media posts to large groups are tantamount to public posts are not subject to the protections of the SCA.

To that end, we disagree with the holdings in *Ehling v. Monmouth-Ocean Hosp. Serv. Corp* (D.N.J 2013) 961 F.Supp.2d. 659 and *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F.Supp. 2d. 965, which held that non-public social media posts to “friends” falls within the ambit of the SCA because the user made some attempt to restrict access. We note that in the absence of a Supreme Court opinion on point, this Court is not bound by the decisions of lower federal courts, even on federal questions.” (*People v. Superior Court (Moore)* (1996) 50 Cal. App. 4th 1202, 1211; see also *Lockhart v. Fretwall* (1993) 506 U.S. 364, 376, conc. opn. J. Thomas.)

Real parties assert that social media posts to large groups of “friends” or “followers” but not made completely public, cannot be subject to the SCA on the theory that social media platforms are analogous to outdated computer bulletin boards systems (BBS) as asserted by *Crispin*,

supra, 717 F.Supp 2d 965, 981, and *Ehling, supra*, 961 F.Supp.2d. 659, 666-667. This is an area of law few courts have addressed. Real parties contend that social media posts disseminated to large groups of friends and followers are not subject to the SCA under 18 U.S.C. § 2511(2)(g)(1), which states that it is not unlawful under the federal wiretap statute or the SCA to access electronic communications that are readily available to the public. (*Ibid.*) We contend posts made available to a large group of people through social media apps, and cellular telephones that access the internet and have the capacity to screen shot any image, render these posts open to the public since all users know that any “friend” or “follower” can view the post and immediately disseminate it without restriction by the original poster.

This technology is vastly different than the nearly obsolete computer bulletin board systems of the 1990's, used at a time when there were no smart phones with ready internet access and only a comparatively small number of people had the technical ability or equipment to access these boards. “A computer bulletin board system is a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer to post messages, read existing messages, and delete messages.” (*United States v. Steiger* (11th Cir. 2003) 318 F.3d 1039, 1049.)

Computer bulletin board systems, used cumbersome dial-up technology through the telephone system that became nearly obsolete in the late 1990's with the advent of the World Wide Web.

Today, the media often calls BBSes an internet-before-the-internet. But that is a grossly inaccurate characterization. The internet is a global network of billions of computers, across which data flows like water. BBSes are like remote Pacific islands, each populated with pocket civilizations that communicate reluctantly via message-in-a-bottle. Over a telephone line, bandwidth is lean and every bit counts.

(Edwards, Ben. J.; [The Lost Civilization of Dial-Up Bulletin Board Systems](#), *The Atlantic*, Nov, 4, 2016.) Posts to large groups on social media are greatly distinguishable from private computer bulletin boards. Billions more consumers use social media platforms than bulletin boards of decades past. Now, even semi-public posts to groups can be made instantly public through the explosion of smart phones that can access the internet, take screen shot posts, and disseminate the images in seconds. This technology was not in existence when computer bulletin board systems were used in the 1990's much less when the SCA was enacted in 1986. Thus, it was reasonable to expect that bulletin board users' information would be relatively private and the likelihood of mass dissemination in seconds with a few clicks, was impossible. Now, reasonable persons assume that anything one posts on social media to a large groups can and will be disseminated in

the public realm. Accordingly, real parties assert that the SCA does not cover social media posts because users do not have a reasonable expectation of privacy information they share online with the masses and electronic communications made publicly available are not protected by the SCA.

Even if this Court finds that social media wall posts configured to be accessible only to “friends” and “followers” are subject to the SCA under rationale of *Crispin, supra*, 717 F.Supp 2d 965, 981, *Ehling, supra*, 961 F.Supp.2d. 659, and *Viacom, supra*, 253 F.R.D. 256, which held that YouTube videos restricted to “friends” could not be subject to a civil subpoena under 18 U.S.C. § 2702(a), a superior court judge may still conduct an *in camera* review of private electronic records upon and showing of good cause, and may provide those records to the defendant if necessary to enforce the panoply of constitutional rights afforded to criminal defendants facing a criminal trial.

C. **Because 18 U.S.C § 2702 is Not an Absolute Bar to the Dissemination of Private Electronic Records, the United States Constitution Mandates that the SCA Yield if the Records Sought Are Necessary For a Fair Trial**

California Courts are under the solemn duty to ensure that Mr. Sullivan and Mr. Hunter receive a fair trial, and have access to the evidence they need to mount a defense and cross-examination as guaranteed by the United States Constitution. Reneesha Lee tweeted information relevant to

impeach her with acts of violence and corroborated the defense theory that she implicated Mr. Sullivan in the murder because she believed he had been involved with another woman. These tweets provide good cause to order the production of her Twitter, Facebook, and Instagram accounts, not only to lay a foundation for the records we do have but also to request the superior court to conduct an *in camera* review for evidence pertinent to the defense located on other social media platforms that law enforcement did not obtain by search warrant. Ms. Lee's social media records are particularly critical for defendant Hunter, because his defense is that Ms. Lee was the getaway driver, not Hunter.

Similarly, in order to demonstrate good cause for the production of Joaquin Rice's social media records, the defense produced a few of Joaquin Rice's Facebook videos and posts to the superior court relevant to show that the murder was caused not because of a gang dispute as the prosecutor contended, but because the decedent had been threatening children online, and Q. Hunter shot Rice because Q. Hunter was afraid due to a personal dispute. Importantly, the defense subpoenaed records from Rice's Instagram and Twitter accounts, that were not obtain by law enforcement's search warrant.

Insofar as the social media communications fall within the ambit of the protections of the SCA, such as private messages, this Court can and must permit the superior court to conduct an *in camera* review of Rice and Lee's social media accounts and order the production of records necessary to ensure Mr. Sullivan and Mr. Hunter receive a fair trial at a time when they can mount a meaningful defense subject to any protective orders deemed necessary to protect privacy rights of Ms. Lee and Mr. Rice's estate.

Because 18 U.S.C. § 2702 is not an absolute bar to production to electronic records, but contains numerous exceptions for law enforcement, the United States Supreme Court's decision in *Pennsylvania v. Ritchie* (1987) 480 U.S. 39, permits this Court to order an *in camera* hearing to examine the records and disclose exculpatory evidence to the defense. In *Pennsylvania v. Ritchie*, the United States Supreme Court held that a criminal defendant's right to due process and to receive a fair trial guaranteed by the Fifth Amendment, as well as the right to secure evidence to present a complete defense under the Sixth Amendment trumps a victim's privacy rights in Child Protective Service records. There, the defendant was charged with committing sexual offenses against his daughter and sought to examine confidential records concerning her

compiled by the state protective services agency in which the state statutory scheme prohibited disclosure to the public. The defendant claimed the file “might contain the names of favorable witnesses, as well as other, unspecified exculpatory evidence.” (*Id.* at 44.) The United States Supreme Court determined that the trial court had erred by denying the request without inspecting the file, reasoning that the principle of due process of law requires the government to disclose evidence that is helpful to the accused. (*Id.* at 57.) Because pertinent state statutes provided certain exceptions to the general rule of confidentiality for the records at issue, including one applicable when a court of competent jurisdiction orders their disclosure, there was no absolute bar to disclosure and the defense was entitled to evidence in the confidential file helpful to the accused. (*Id.* at 58.) In so ruling, the Court stated as follows:

Given that the Pennsylvania Legislature contemplated some use of CYS records in judicial proceedings, we cannot conclude that the statute prevents all disclosure in criminal prosecutions. In the absence of any apparent state policy to the contrary, we therefore have no reason to believe the relevant information should not be disclosed when a court of competent jurisdiction determines the information is material to the defense of the accused. (*Id.* at 58.)

The United States Supreme Court concluded the defendant was entitled to have the confidential file reviewed by the trial court to determine

whether it contained information that would have impacted the outcome of the trial. If so, the defendant was entitled to a new trial. (*Id.* at 58.)

Here, like the Pennsylvania statute, the 18 U.S.C. § 2702 is not an absolute bar to the use social media records in criminal trials. For example, prosecuting agencies can obtain electronic records with a service provider by obtaining a warrant or subpoena under 18 U.S.C. § 2702(b)(ii) and 18 U.S.C § 2703(d) for use in criminal trials. Under the rationale of *Pennsylvania v. Richie*, given that the SCA is not an absolute ban on using social media records in criminal trials as it does not impinge on the prosecution's ability to obtain social media records, the SCA must yield to a defendant's constitutional right to a fair trial and to present a complete defense.

Here, under the SCA there is "no clear ... policy of 'absolute' confidentiality" but rather a one-sided, arbitrary, and unconstitutional preference that the government, but not the defense, is entitled to access to relevant electronic evidence. The SCA must yield to afford superior courts the opportunity to conduct an *in camera* review to locate exculpatory evidence relevant to the defense.

Similarly, the SCA must yield to protect the defendants' constitutional rights, which are paramount, under *Davis v. Alaska* (1974)

415 U.S. 308. In *Davis*, the United States Supreme Court held a criminal defendant's constitutional right to cross-examine witnesses trumped a state law declaring juvenile records to be confidential and not to be disclosed to the public. Specifically, the trial judge prohibited defense counsel from questioning a witness about the latter's juvenile criminal record, because a state statute made this information presumptively confidential. The United States Supreme Court found that this restriction on cross-examination violated the Confrontation Clause, despite Alaska's legitimate interest in protecting the identity of juvenile offenders. (*Id.* at 318–320.) The confrontation clause of the Sixth Amendment, the Supreme Court wrote, entitled the defendant to expose the possible bias of a key prosecution witness despite Alaska's confidentiality statute. In reversing the defendant's conviction, the Court ruled as follows:

The State's policy interest in protecting the confidentiality of a juvenile offender's record cannot require yielding of so vital a constitutional right as the effective cross-examination for bias of an adverse witness. The State could have protected Green from exposure of his juvenile adjudication in these circumstances by refraining from using him to make out its case; the State cannot, consistent with the right of confrontation, require the petitioner to bear the full burden of vindicating the State's interest in the secrecy of juvenile criminal records.

Similarly, Mr. Sullivan and Mr. Hunter's right to due process, to present a complete defense, and to procure records necessary to cross-

examine the witnesses, must prevail over statutory privacy rights under the SCA.

It is well-settled that when enacting the SCA, Congress simply failed to take into consideration criminal defendants constitutional right to access electronic records that are necessary to receive a fair trial. (See Zwillinger, Marc J., Genetski, Christian S.; *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, Journal of Criminal Law and Criminology, Northwestern University School of Law, P. 569, Vol. 97, No. 2, 2007.) According to Professor Christian Genetski and Marc J. Zwillinger, both of whom worked for the United States Department of Justice in the Computer Crime and Intellectual Property Section, the SCA is ripe for a constitutional challenge because criminal defendants have no ability to compel disclosure of potentially exculpatory evidence in the hands of a third party. (*Id.* at. 569-570.) The authors reviewed the Legislative History of the SCA and concluded a criminal defendant's constitutional rights to evidence was simply overlooked, not intentionally excluded, because Congress was focused on Fourth Amendment issues which constrain only government searches. (*Id.* at 577.) The authors proposed a statutory amendment to the ECPA to permit criminal defendants to procure electronic records needed to

defend a criminal case. (*Id.* at 597.) In conclusion, the authors stated as follows:

Congress' singular focus [in enacting the SCA] on the interplay between ISPs and government requests for electronic content, however, has left at least one gap that remains to be filled. The present inability under the SCA for criminal defendants, and to a lesser extent, civil litigants, to compel disclosure of electronic content from ISPs raises the specter of constitutional issues that the SCA to date has successfully mooted. As proposed herein, a simple amendment to the SCA that provides private parties the means to seek disclosure of content in appropriate cases, in keeping with appropriate safeguards, will clarify the law on an issue of growing contention, level the playing field for criminal defendants, and ensure the SCA's continued role as the preeminent arbiter of rights to remotely stored electronic content.

(*Id.* at 598-599.)

Thirty-one years have elapsed since the SCA was enacted and there is no sign that Congress intends to amend the statute to afford criminal defendants the right to access electronic records necessary to defend a criminal case in accordance with the panoply of rights guaranteed by the United States Constitution. Access to records protected by the SCA is too important for the Court to side-step the constitutional issues. We have already waited too long. In cases throughout California and United States, criminal defendants are routinely being denied access to critical, exculpatory evidence because an entire body of evidence remains barred. This case is not simply an intellectual issue about internet privacy, but a

matter or life and death for so many who are fighting for their lives in a criminal justice system that is already weighed down with racial and economic inequities.

CONCLUSION

Defendants Sullivan and Hunter respectfully requests that this Court order public social media records produced forthwith. For records deemed protected by the SCA, defendants request that the providers be ordered to produce the records for an *in camera* review, and that the superior court be ordered to produce exculpatory records to the defense subject to protective orders to safeguard the privacy of the account holders.

Respectfully submitted this 23rd day of January, 2017.


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


SUSAN B. KAPLAN
Attorney for Real Party in Interest
LEE SULLIVAN

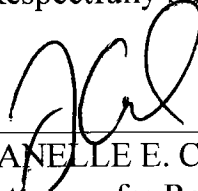

JOSE P. UMALI
Attorney for Real Party in Interest
DERRICK HUNTER

CERTIFICATION

I hereby certify that Real Parties Supplemental brief consists of 5002 words and that the font used was 13-point Times New Roman.

Dated: January 23, 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 January 23, 2017, I served a **REAL PARTIES LEE SULLIVAN AND DERRICK HUNTER'S SUPPLEMENTAL BRIEF AS ORDERED BY THE COURT ON DECEMBER 21, 2016**, 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, Llp.
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

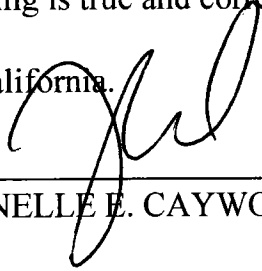
Jeff Adachi
Dorothy Bischoff
San Francisco Public Defender's Office
555 7th Street
San Francisco, CA 94103

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 26th
day of January 23, 2017, at San Francisco, California.



JANELLE E. CAYWOOD