APPENDIX

APPENDIX A

Court of Appeal, First Appellate District,
Division Five - No. A157902

S257385

IN THE SUPREME COURT OF CALIFORNIA

En Banc

FACEBOOK, INC. et al., Petitioners,

v.

SUPERIOR COURT OF SAN FRANCISCO COUNTY, Respondent;

DERRICK D. HUNTER et al., Real Parties in Interest.

The petition for review is denied.

[Filed Sept. 11, 2019]

/s/ Cantil-Sakauye
Chief Justice

APPENDIX B

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION FIVE

FACEBOOK, INC. et al.,

Petitioners,

v.

SUPERIOR COURT FOR THE CITY AND COUNTY OF SAN FRANCISCO,

Respondent;

DERRICK D. HUNTER et al.,

Real Parties in Interest.

A157902

San Francisco No. 13035657 and 13035658

BY THE COURT:*

The petition for writ of mandate/prohibition is denied.

Date Jul 30 2019 Jones, P.J., P.J.

* Before Jones, P.J. and Burns, J.

APPENDIX C

SUPERIOR COURT OF CALIFORNIA
County of San Francisco

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. Lee Sullivan and Derrick Hunter, Defendants.	Cause No. 13035657 & 13035658 ORDER AND JUDGMENT OF CONTEMPT [Filed July 26, 2019]

1. Facebook and Twitter appear to be misusing their immense resources to manipulate the judicial system in a manner that deprives two indigent young men facing life sentences of their constitutional right to defend themselves at trial. But Facebook and Twitter have made it clear that they are unwilling to alter their behavior, regardless of the harm to others – or the rulings of this court. That is inexcusable contempt.

Facts & Procedural History

2. Defendants Derrick Hunter and Lee Sullivan are on trial for murder, weapons, and gang charges-related charges arising from a drive-by shooting in 2013. Jury selection began on June 24, 2019. Opening statements were July 23, 2019.

3. Recognizing that social media messages among the defendants, the victims, and others had played a central role in the underlying police investigation and would be a focus of the prosecution's case, defendants subpoenaed social media messages from third party service providers Facebook, Inc. and Twitter, Inc. (collectively, "contemnors") back in 2014. This court (Chan, J.) recognized the messages' significance as well, and denied contemnors' motions to quash the subpoenas.

4. Contemnors obtained a writ of mandate from the Court of Appeal reversing Judge Chan's denial of their motion to quash and, subsequently, a superseding favorable opinion from the Supreme Court as well, remanding the case to this court. (See Opinion, 240 Cal. App. 4th 203 (2015); and Opinion, 4 Cal. 5th 1245 (2018).) Contemnors relied heavily on the Federal Stored Communications Act, 18 USC §§ 2701 et seq. (SCA), arguing that it prevents them from producing the subpoenaed documents. They also argued undue burden – an argument they later withdrew, abruptly and strategically. (RT 7/24/19 at 4.) (Transcripts of this court's hearings on May 1, 2019, and July 24, 2019, are attached and incorporated herein by reference.)

5. Both the Court of Appeal and the Supreme Court limited their rulings to the pretrial context, and indicated that their rulings might be different if the defendants were actually in trial. (Opinion, supra, 240 Cal. App. 4th at 459-460; and Opinion, supra, 4 Cal. 5th at 1261). Indeed, the Court of Appeal explicitly questioned the constitutionality of

the Stored Communications Act if it prohibits individual defendants from subpoenaing documents for use at trial, as contemnors maintain. (240 Cal. App. 4th at 460 & n.17.)

The Order

6. On remand, defendants asserted their right to a speedy trial and again subpoenaed documents from contemnors, this time for use at trial. Once again, contemnors moved to quash. At a hearing on May 1, 2019, the court denied contemnors' motions to quash and ordered contemnors to produce specified documents for in camera review. (RT 5/1/19 at 37-44.) At contemnors' request, the court delayed the effective date of its order so contemnors could seek writ relief. (Id. at 41-42.)

7. Subsequently, contemnors asked both the California Court of Appeal and then later the California Supreme Court to stay this court's May 1st order. Each court initially did so, to evaluate contemnors' petitions. (7/17/19 S. Ct. Order; 7/1/19 Ct. App. Order.) But both courts eventually ordered their stays dissolved, expressly citing the pendency of trial as a reason. (Id.)

8. As a result, the May 1st order requiring contemnors to produce documents was in effect as of July 17, 2019.

9. The May 1st order is clear, specific, and unequivocal. (5/1/19 TR at 40:10-16.) It requires contemnors to produce "the unproduced items that have been identified by the service providers at this hearing. That will be the ten private posts on Mr. Rice's Instagram account, the four private posts

on Ms. Lee's Instagram account, eight private direct messages on Ms. Lee's Twitter account, and the private posts and messages on Ms. Lee's Facebook account."))

Contemnors' Willful Violation of the Order

10. Nevertheless, by letter dated July 22, 2019, contemnors informed the Court of Appeal that they had not produced documents as ordered and that they did not intend to do so. (7/22/19 letter from Joshua Lipshutz, Esq.) Thus, on July 23, 2019, this court served contemnors with an order to show cause why they should not be adjudged guilty of contempt of court and punished pursuant to section 1209(a)(5) of the California Code of Civil Procedure. (7/23/19 OSC.) The court held a hearing on July 24, 2019, to give contemnors an opportunity to make this showing.

11. At the hearing, the court advised contemnors that their continued violation of the court's May 1st order would be adjudged contempt of court if it continued. Contemnors made clear through counsel that their failure to comply with the May 1st order was willful, and that they had no intent to comply, arguing that they were justified by a "disagreement over the requirements of federal law [the SCA] that must be resolved by an appellate court." (RT 7/24 at 7.)

12. Contemnors had made this same argument to both the Court of Appeal and the Supreme Court. Nevertheless, those courts dissolved their stays of the May 1st Order. If contemnors' SCA argument was not a sufficient basis for the appellate courts

to stay the May 1st order, it surely isn't a justification for contemnors to violate the order unilaterally, particularly in light of the prejudice it has caused to defendants' constitutional rights, as well as the drain on the prosecution's resources and the court's. Contemnors' stated justification for their violation, while imaginative and articulately presented, does not excuse it, and it certainly does not outweigh the real-world time pressures and resulting prejudice involved.

13. Contemnors' continued violation of the May 1st order ignores and upsets the balance that the Supreme Court and the Court of Appeal worked hard to strike — enabling contemnors to pursue their legal arguments while preserving defendants' constitutional rights. (The Court of Appeal ruled that "notwithstanding any potential issues of mootness that could arise from the dissolving of our prior stay, the court has decided to retain this matter for consideration," and set a briefing schedule (7/1/19 Ct. App. Order at 2).) Contemnors have used the court system's resources exhaustively to obtain rulings that suit them, but now they are deliberately ignoring one that does not.

Disposition

14. After due consideration of these facts, the court finds, beyond a reasonable doubt:

a) That the contemnors are guilty of contempt of court in violation of Section 1209(a)(5) of the Code of Civil Procedure — "Disobedience of any lawful judgment, order, or process of the court."

b) That contemnors had knowledge of the court's May 1st order, that they were able to comply with it as of May 1st and again as of July 24th, that they continue to have that ability now, and that they have willfully failed to comply.

c) That the contemnors are sentenced to pay fines of $1,000 apiece, the maximum permitted by Section 1209 of the Code of Civil Procedure.

d) That there is no good cause to stay execution of this sentence, and that contemnors are ordered to pay the fines immediately or risk remand.

e) That the clerk of the court is ordered to file this order, to enter the contempt on the court's docket, and to deliver a copy of this order to contemnors.

Dated: 7/26/19

/s/ Charles Crompton
JUDGE CHARLES CROMPTON
SAN FRANCISCO SUPERIOR COURT

Superior Court of California

County of San Francisco

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. Lee Sullivan and Derrick Hunter, Defendant.	Case Number: 13035657 & 13035658 **CERTIFICATE OF SERVICE BY MAIL** (CCP 1013a (4))

I, SARAH DUENAS, a Deputy Clerk of the Superior Court of the County of San Francisco, certify that I am not a party to the within action.

On JULY 26, 2019, I served the attached ORDER AND JUDGMENT OF CONTEMPT on the parties stated below by placing a copy thereof in a sealed envelope, addressed as follows:

GIBSON, DUNN & CRUTCHER LLP
Joshua S. Lipshutz, Bar No. 242557
jlipshutz@gibson-dunn.com
555 Mission Street
San Francisco, CA 94105

John R. Tyler, *admitted pro hac vice*
RTyler@perkinscoie.com
1201 Third Avenue,
Suite 4900
Seattle, WA 98101-3099

Anna M. Thompson, *admitted pro hac vice*
AnnaThompson@perkinscoie.com
1201 Third Avenue,
Suite 4900
Seattle, WA 98101-3099

PERKINS COIE LLP
James G. Snell, Bar No. 173070
JSnell@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304-1212

and, I then placed the sealed envelopes in the outgoing mail at 850 Bryant Street, San Francisco, CA. 94103 on the date indicated above for collection, attachment of required prepaid postage, and mailing on that date following standard court practices.

On the above mentioned date, I caused the documents to be sent to the persons at the electronic notification addresses as shown above.

Dated: JULY 26, 2019 T. MICHAEL YUEN Clerk

By: /s/ Sarah Duenas
SARAH DUENAS,
Deputy Clerk

Attachment 1

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF SAN FRANCISCO

--o0o--

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. DERRICK D. HUNTER, and LEE G. SULLIVAN, Defendants.	)	Court No. **13035658** 2473530 **13035657** 18018261 Pages 1-13

Reporter's Transcript of:

ORDER TO SHOW CAUSE RE FACEBOOK/TWITTER

(Taken during the Jury Trial in the above-named case)

WEDNESDAY, JULY 24, 2019

BEFORE: THE HONORABLE CHARLES CROMPTON, JUDGE

Department 19, San Francisco, California

--o0o--

REPORTED BY: DIANE WILSON, CSR 8557

A-P-P-E-A-R-A-N-C-E-S

FOR THE PEOPLE:

GEORGE GASON
District Attorney
District Attorney's Office
County of San Francisco
850 Bryant Street, Suite 300
San Francisco, CA 94103
BY: NATHAN QUIGLEY
Deputy District Attorney

FOR DEFENDANT HUNTER:

JOSE PERICLES UMALI
Attorney at Law
507 Polk Street
San Francisco, CA 94102

BICKA BARLOW
Attorney at Law
2538 Market Street
San Francisco, CA

FOR DEFENDANT SULLIVAN:

SUSAN KAPLAN
Attorney at Law
214 Duboce Ave
San Francisco, CA 94103

BICKA BARLOW
SANGEETA SINHA
Attorneys at Law
2538 Market Street
San Francisco, CA,

FOR FACEBOOK\TWITTER:

JOSHUA LIPSHUTZ
GIBSON, DUNN & CRUTCHER, LLP
Attorney at Law
1050 Connecticut Ave. N.W.
Washington, D.C. 20036-5306

THOMAS F. COCHRANE
GIBSON, DUNN, & CRUTCHER, LLP
Attorney at Law
233 So. Grand Ave
Los Angeles, CA, 90071-3197

--o0o--

WEDNESDAY, JULY 25, 2019 - AFTERNOON CALENDAR

BEFORE THE HONORABLE CHARLES COMPTON, JUDGE

--o0o--

(Whereupon the following proceedings were held outside the presence of the jury and include only colloquy regarding the O.S.C. matter to Facebook/Twitter)

THE COURT: Good afternoon.

All right. Back on the record in the Hunter and Sullivan case. The jury is not with us because we are here to deal with a third-party discovery issue.

Appearances, please.

MR. QUIGLEY: I'm Nathan Quigley. I'm back here.

MS. BARLOW: Bicka Barlow appearing for Mr. Sullivan and Mr. Hunter.

Mr. Umali is behind me as well.

MR. UMALI: I'm here as well.

MS. KAPLAN: Susan Kaplan here as well for Mr. Sullivan.

THE COURT: I see Ms. Sinha is here as well.

MS. SINHA: Just lurking in the back, Your Honor.

MR. LIPSHUTZ: Joshua Lipshutz and Thomas Cochrane for Facebook and Twitter.

THE COURT: Good afternoon.

All right. I've scheduled this hearing as a result of the service providers' failure to comply with my May 1st order that they provide the subpoenaed documents to me for in camera review and their letter to the Court of Appeal dated July 22nd indicating that they do not intend to do so. Given the service providers' unilateral actions and the documents' importance to our ongoing trial, I was forced to take the extraordinary step of releasing the jury early today to deal with this issue.

Unlike any reported case that's been cited to me or found by me, this case involves trial subpoenas and the need for the production of documents during trial. Both the Court of Appeal in this case and the Supreme Court observed the uniqueness of this case's procedural situation and the heightened concern that it raises for the defendants' Constitutional rights.

The service providers themselves bear at least partial responsibility for this situation. Since this case was assigned to me in early 2019, the service providers have spent months arguing that producing subpoenaed documents would be unduly burdensome requesting an evidentiary hearing in which they were to provide -- they would prove that, according to them, with a witness that they said they had to bring from the east coast. They sought cooperation of the parties and the Court in scheduling that hearing to accompany their witness, thereby delaying the start of trial, and then at the last possible moment, on the date of the hearing itself, the service providers announced surprisingly that they would not produce a witness after all and that, for the first time, they expressly with-

drew their burden argument that they had been making for years to this Court, the Court of Appeal, and the Supreme Court.

The subpoenaed documents' great potential importance to the defendants at trial has been cited more than once. I found the documents sufficiently relevant to justify ordering them produced at least for in camera review, and so did Judge Chan back in 2015. To my knowledge, neither the service providers nor anyone else has ever disputed these findings. That is not surprising. The People's trial witness list, exhibits proffered at pretrial hearings, opening statements yesterday, and the witness examination thus far have all confirmed that there is a strong justification for, at the very least, in camera review of the subpoenaed documents and potentially for the defendants to have access to them to ensure their rights under the 5th and 6th Amendment, the 14th Amendment guarantees, and perhaps on other basis as well.

It's worth noting that producing the subpoenaed documents entails zero risk of prejudice to the service providers. They are immunized from liability under the Stored Communication Act Safe Harbor Provision, and they ultimately abandoned their burden argument in the manner that I described.

By contrast, the potential prejudice to the defendants of denying the Court an opportunity to review the documents in camera, potentially to provide them to the defendants to defend themselves at trial if warranted, is immediate and undeniable given the defendants have been in jail for six years awaiting trial. The trial has now begin, and the crimes charged

here are potential life sentences. Time is of the essence. Both the Court of Appeal and the Supreme Court recognizes urgency and appeared to be motivated by it in dissolving their stays. And again, the service providers bear at least partial responsibility for this situation.

There is no longer a stay of my May 1st order by any court still in effect. Both the Court of Appeal and the Supreme Court have resolved their earlier stays, so the May 1st order compelling the service providers to produce the subpoenaed documents for in camera review is operative and binding on the service providers and the production is past due. All of the arguments raised by the service providers in their July 22nd letter to the Court of Appeal were already made to and considered by this Court, Court of Appeal, and the Supreme Court. All of them. Those arguments did not convince any of the Courts to grant a longer stay of the service providers' duty to produce the subpoenaed documents, and they surely don't entitle the service providers to engage in self-help for the same purpose. Immense judicial resources been devoted to the service providers' arguments, motions, and petitions, but the service providers apparently disagree with the results so far, so apparently the service providers have decided that they will simply not comply. That is unacceptable. The service providers' failure to comply with my May 1st order is contemptuous. I set this hearing to give the service providers clear warning of that, and an opportunity to explain themselves.

So, let me first hear from the service providers.

MR. LIPSHUTZ: Thank you very much, Your Honor. Thanks very much for the opportunity to be here to present to you today.

My clients, Facebook and Twitter, have as much interest as anyone in resolving this issue quickly and with finality, understanding the seriousness of the current matter before the Court. Providers, however, are unable to produce the private social media records at issue here, because in our view, such production would violate the Stored Communications Act, which is a federal statute. We understand this Court disagrees, and we mean the Court no disrespect by our actions. But in our view, this is a good faith disagreement over the requirements of federal law that must be resolved by an Appellate Court.

We understand this Court and the parties are eager to proceed with the trial that's already underway here, and we do not believe our actions need to or should hold up this trial. Defendants respectfully have other means of obtaining the very same documents at their current disposal.

THE COURT: I disagree with that. That's been dealt with. Stored Communications Act, if it prohibits production of the subpoenaed documents as you maintain, it appears to be unconstitutional. Both the Court of Appeal and the Supreme Court recognize this potential. That's at 240 Cal.App.4th 203 note 17 and 4 Cal 5th at 1261.

In any event, there's an order that you produce these documents, and the Appellate Court and the State Supreme Court have both recognized that that order needs to be complied with in order to vindicate these gentlemen's Constitutional rights.

MR. LIPSHUTZ: Respectfully, Your Honor, neither the Court of Appeal nor the Supreme Court have resolved the merits of the lawfulness of this Court's order.

THE COURT: Understood. And they're not going to wait to do that -- they're not going to wait to get the documents until they do that. There's a timeline for doing that. You're going to get your day in court on that. But in the mean time, these documents have to be produced for the vindication of these gentlemen's Constitutional rights.

MR. LIPSHUTZ: Several problems with that, Your Honor. First is that if we do produce the documents, it's our view that the arguments we're making on appeal could likely be moot. I know the Court of Appeals seem to be willing to overlook the mootness of that issue, but other Courts may not.

THE COURT: Well, as you said, Court of Appeals indicated otherwise, so I view that as a specious argument.

MR. LIPSHUTZ: Respectfully, the U.S. Supreme Court cannot overlook the mootness that would take place if we were to produce the documents, and under binding U.S. Supreme Court case law, we are forced to take the actions that we're taking today if we have any possibility of appealing the order up to the U.S. Supreme Court. U.S. Supreme Court will not take the case unless we have -- we have refused to comply with the order and are faced with contempt. That is the case law we're faced with.

So -- and I would point out, the Court of Appeal did ask this Court to show why the order that was

entered in May is not unlawful, so there is some question as to the legality of the order that is currently being adjudicated in the Courts of Appeal.

THE COURT: That same Court lifted its stay on my order indicating that you are obligated to produce the documents.

MR. LIPSHUTZ: It did, Your Honor, and we respectfully cannot comply with that order because of the --

THE COURT: I disagree you cannot comply.

All right. So your -- it would appear you're in contempt.

MR. LIPSHUTZ: That's up to Your Honor. I think there are certainly cases, In Re Noland, 45 Cal 4th 1217 at Page 1231 from 2009 that say that -- where the California Supreme Court said not every violation of a court order is subject to punishment as a contempt of court. We don't think that this action today justifies contempt of court because there is this ongoing legal dispute over the legality of the order. It is a good-faith dispute. We are not here --

THE COURT: I disagree.

MR. LIPSHUTZ: Well, I'm sorry that you disagree with a good-faith dispute, but there is a Court of Appeal order saying there is questions as to the legality of the order, and we would like --

THE COURT: You're ignoring the part of the Court of Appeals' ruling that indicates that the order to produce the documents is not stayed. So you can't pick and choose among what the Court of Appeal is saying.

MR. LIPSHUTZ: Understood, Your Honor.

Just -- as I explained, I think we are taking action that we think are required by federal law and in order to preserve our arguments for appeal up to the U.S. Supreme Court, if necessary.

THE COURT: All right.

Anything else that the service providers want to say in explanation of their actions?

MR. LIPSHUTZ: I would just point out that this same procedure took place in the D.C. Court of Appeal last year. We were forced to take a contempt order there as well. We did appeal it very quickly to the Court of Appeals. The whole thing was resolved in a matter of two weeks, I think. And our objections to the subpoena were upheld by that Court. Your Honor is correct that that was not a trial subpoena. It was a pre-trial subpoena. But we think the same arguments apply. The Stored Communications Act does not distinguish between pre-trial and trial communication. So we would certainly --

THE COURT: The act may not, but the Constitution does. And from what I can tell, every Court that has dealt with the distinction has acknowledged that it's quite different, including the Court of Appeal here and the Supreme Court here. So I don't think that citing cases that relate to pre-trial discovery has any persuasive value whatsoever here.

MR. LIPSHUTZ: My point was simply that we are willing to act and proceed as expeditiously as possible through the appellate courts. We think this issue could be resolved quickly, and in light of the fact

that Ms. Lee has not taken the stand here yet, it's possible it need not effect the trial.

THE COURT: I think that is very unrealistic. As I said, I think we're -- in the timing position that we are in, in part because of your clients' conduct, and I don't think that it will be any consolation to the defendants or their lawyers that you think you are vindicating federal rights.

MR. LIPSHUTZ: That may be so, Your Honor, but we have an obligation under federal law to protect the privacy of the other account holders that were required to protect under federal law.

California Code of Civil Procedure Section 1218 provides for a contempt sanction of a $1,000.00 in this situation. I think if Your Honor is contemplating contempt, we would propose that sanction and we would ask that the Court stay the sanction pending appeal. That would be our request.

THE COURT: It also authorizes five days in jail.

All right. I am going to take this under submission. I expect that I'll be ruling by Friday, the 26th, at the latest.

Is there anything anyone else wants to say at this time?

MS. KAPLAN: I think we made our record earlier.

THE COURT: I do as well.

Okay. Thank you, all.

MR. LIPSHUTZ: Thank you, Your Honor.

(Whereupon these proceedings concluded)

--o0o--

STATE OF CALIFORNIA)
) ss.
COUNTY OF TUOLUMNE)

I, Diane Wilson, a Certified Shorthand Reporter licensed to practice in and for the State of California, County of San Francisco, do hereby certify:

That on Wednesday, the 24th day of July, 2019, I was present at the above-entitled matter; that I took down in shorthand notes all proceedings had and testimony given; that I thereafter caused said shorthand notes to be reduced to typewriting using computer-aided transcription, the foregoing being a full, true and correct transcription thereof.

IN WITNESS WHEREOF, I have hereunto subscribed my hand.

/s/ Diane Wilson
Diane Wilson
Certified Shorthand Reporter No. 8557

Case: ***13035658****, 2473530,*
13035657*, 18018261*

Date: Wednesday, July 24, 2019

Attachment 2

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN FRANCISCO

BEFORE THE HONORABLE CHARLES CROMPTON, JUDGE PRESIDING

DEPARTMENT NUMBER 19

---o0o---

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. **DERRICK HUNTER, LEE SULLIVAN,** Defendants.	Court No. 13035658 17004548, 13035657 Pages 1-45

Reporter's Transcript of Proceedings

Wednesday, May 1, 2019

GOVERNMENT CODE §69954(d):

"ANY COURT, PARTY, OR PERSON WHO HAS PURCHASED A TRANSCRIPT MAY, WITHOUT PAYING A FURTHER FEE TO THE REPORTER, REPRODUCE A COPY OR PORTION THEREOF AS AN EXHIBIT PURSUANT TO COURT ORDER OR RULE, OR FOR INTERNAL USE, BUT SHALL NOT OTHERWISE PROVIDE OR SELL A COPY OR COPIES TO ANY OTHER PARTY OR PERSON."

Reported By: Jacqueline K. Chan, CSR No. 10276

APPEARANCES OF COUNSEL:

For the People:

George Gascón, District Attorney
City and County of San Francisco
850 Bryant Street, Suite 322
San Francisco, California 94103
BY: **NATHAN QUIGLEY**, Assistant District Attorney

For the Non-Parties:

Perkins Coie LLP
3150 Porter Drive
Palo Alto, California 94304
BY: **JAMES G. SNELL**, Attorney at Law

For Defendant Sullivan:

Law Offices of Bicka Barlow
2358 Market Street
San Francisco, California 94114
BY: **BICKA BARLOW**, Attorney at Law

For Defendant Sullivan:

Law Offices of Susan B. Kaplan
214 Duboce Avenue
San Francisco, California 94103
BY: **SUSAN KAPLAN**, Attorney at Law

For Defendant Hunter:

Law Office of Jose Pericles Umali
507 Polk Street, Suite 340
San Francisco, California 94102
BY: **JOSE PERICLES UMALI**, Attorney at Law

WEDNESDAY, MAY 1, 2018 9:33 P.M.

P-R-O-C-E-E-D-I-N-G-S

---o0o---

THE COURT: Good morning.

MR. QUIGLEY: Good morning.

THE COURT: Right. We're here on the Sullivan/Hunter case. We better get appearances, please.

MR. SNELL: Your Honor, Jim Snell for third party providers Facebook and Twitter.

MR. QUIGLEY: Good morning, Your Honor. Nathan Quigley for the People.

MS. KAPLAN: Susan Kaplan for Lee Sullivan who is in custody.

MS. BARLOW: And Bicka Barlow for Mr. Sullivan as well.

MR. UMALI: Jose Pericles Umali for Mr. Hunter and that's the last thing I'm going to say today.

THE COURT: All right.

MS. BARLOW: Your Honor, we have sitting at counsel table Eric Hernandez who is from our forensic -- digital forensic firm and he's going to be assisting me today.

THE COURT: Welcome. Good morning, Counsel.

Good morning, Mr. Hunter and Mr. Sullivan.

DEFENDANT HUNTER: Good morning.

DEFENDANT SULLIVAN: Good morning.

THE COURT: We're here to deal further with this discovery issue. As far as I can tell, what's really in the balance now is the private communications only. Is that correct?

MS. BARLOW: Well, I think -- as I've said, I think in the last hearing and I was reviewing our transcript from the last time, at least I was here and Mr. Snell was here, I think that the only outstanding discovery -- and I understand the Court has a production from the service providers that we have not yet gotten?

THE COURT: I do have a production of what I understand to be public messages that was provided to me on April 12th by Mr. Snell's office.

MS. BARLOW: We haven't seen those obviously since they have been produced to the Court and subpoenaed. So I think one outstanding question for the defense and I think the Court has to address now because of the public production is what remains, what quantity of it remains and what is private and what different aspects, you know, the privacy settings are relevant because that was an unanswered question in the Facebook litigation. *Facebook v. Superior Court* opinion left that as an open question. And given the fact that that now exists in a sort of separate file, I suppose it is relevant for our purposes and our discussion.

What is left: What are the privacy settings, what percentage of those messages and what settings, in particular with Facebook since they have multiples, and then what is the burden.

I think one of the issues that arises from the fact that they did this public production is credibility of the earlier declarations of the witnesses saying this was so burdensome they couldn't do it. And I also think the Court did mention at our last hearing that the Court was interested in deleted content. And after reviewing the declaration of Mr. Strahs, I believe it is S-T-R-A-H-S, it appears that they do have this information somewhere, but getting it is the question. I think that's a valid area of inquiry for our cross-examination.

THE COURT: Just on that last point, Ms. Barlow, I understood you to say before that you were accepting the representation that deleted stuff is deleted and so that really wasn't on the table any longer.

MS. BARLOW: Well, I did say that but then I just went back -- and the Court raised it and then I went back and I reread the Declaration of Preparation for Stay and it appears that at least the last two or three paragraphs of that declaration indicate the deleted content may actually exist. The form, where it is and how it can be retrieved I think is the question of burden. We did request that in the subpoenas. And my -- and in no way was I intending my statement to be a waiver of Mr. Sullivan's right to access that information if it actually exists.

THE COURT: All right.

MR. SNELL: Your Honor.

THE COURT: Yeah, Mr. Snell.

MR. SNELL: So the California Supreme Court in Hunter said the issues that this Court should be thinking about is if something was said as public and

later changed to private or deleted, what is the burden of wading through that, and as a matter of first impression is deletion or setting something from public to private revocation of consent. We talked at the last hearing that Judge Brown has found that deleting something or rendering it private is revocation of consent.

And we've gone through the burden both for Twitter and for Facebook. This would be for Facebook's Instagram and Facebook's records and produced the public information. So that has been burdensome but that burden has been sustained. And my understanding was aligned with yours that deleted content was not an issue based on the strength of the declarations that have been presented prior.

So our position is that the -- I think what we called it before was a potential hearing, an evidentiary hearing is not necessary. We're interested to hear how the Court feels about that and to obviously argue the merits of whether private content could be obtained at this stage of the proceedings, but we don't think there's a need for an evidentiary hearing based on the public production.

MS. BARLOW: And, Your Honor, if I can address one issue that was raised by Mr. Snell which is that the Facebook casts this Court with the definition of what is public as if it has been decided and it is a settled matter of law when, in fact, it was an open question. The Supreme Court rejected both the defense and Facebook's I'll use service providers to make it a little more straightforward -- service providers' arguments regarding what's public versus private and left

open for the trial court to reach that question of first impression.

And the fact now that Facebook has produced something that they deem to be public does not do away with that question because the question still remains of the, quote, private or restricted content, which of it is actually private legally, not is it restricted by the service providers' definition, but at what point does something become actually public even though someone has restricted access. And we had a short discussion. I know the Court doesn't really want to reach that question but because the service providers have forced the Court into a position of actually having to address it now given the production.

THE COURT: I understand. Well, let's -- let's start with what I've got which is the production from the service providers.

Mr. Snell, first of all, is this something that I'm expected to review in camera for anything that would need to be redacted or is this for release to the defense?

MR. SNELL: Your Honor, I think that's an issue for you to decide. We've complied with the Code in terms of how to get it to you and I think it's up to you to determine what to do with it. I can say that what's been done in both instances, both with respect to Twitter and Facebook is that the company has taken the preservation copy that existed and compared that preservation copy against what is presently publicly available on the internet and something presently publicly available on the internet, has produced that from the preservation copy so that's been emailed.

THE COURT: So the preservation copy, tell me about that.

MR. SNELL: So preservation copies were made for Twitter. The preservation copy was made in early December 2014, right after the subpoena was requested, and we have gone through the process of somebody making a manual comparison to what was in that -- there were 800 or so tweets -- against what's public and we produced from the preservation copy what is presently publicly available on the internet.

And with respect to Facebook --

THE COURT: Before you move on to Facebook, how many of the 800 wound up getting produced?

MR. SNELL: Every tweet that the user had posted and was in the preservation copy is presently available on the internet, Your Honor. So there is nothing from the tweets that has been withheld.

THE COURT: 800.

MR. SNELL: I can't remember the exact number. There is a difference in the sense that if there's a retweet, so if the user that's the subject of the subpoena had retweeted somebody else's content and that user deleted it, those retweets may not exist. That's what made the manual comparison somewhat cumbersome, but we were able to confirm that every tweet that the user who was subpoenaed in this instance posted is still available publicly on the internet and that the only content that apparently is not available publicly on the internet is eight direct messages.

And, in fact, Your Honor, we have prepared a two-page demonstrative that I think might help walk

through some of the questions that Ms. Barlow's raised and might clear some of these issues up for the Court. I think we've all struggled with the accounts at issue and what's happened to those.

THE COURT: All right. I'll be interested in seeing that in a moment. Tell me what you were going to tell me about the Facebook production.

MR. SNELL: Same process, Your Honor. So I believe the Facebook preservation was made in March of 2018 and so there was a manual comparison of materials in that March 2018 preservation. And where content was publicly available on the internet, that content was produced from the preservation copy.

And obviously, Your Honor, the clients are producing it from the preservation copies because that's the way they keep their business records. They have tools that will pull this information. The tools don't distinguish between public and private because they are usually responses being made to search warrants and so here they had to do the manual comparison made.

THE COURT: And the Facebook production, when you did the manual comparison, did that result in anything being removed from the preservation copy?

MR. SNELL: I believe so, Your Honor. On the exhibit we have, I think the Pistol.Dutch Facebook account there was material that's not public. And with respect to the account Nesha.Lee.35, there are private posted messages as well, so both of those accounts had public content.

THE COURT: Got it. And one more question about that exercise. How many personnel hours did it take? How much did it cost? Can you quantify the burden for me?

MR. SNELL: I'll start with Twitter because that's more manageable because we're only looking at tweets, but I believe that's a several hour project. I don't know the exact number of hours, but it was not an easy event because we have to look at each tweet and find it on the internet.

With respect to Facebook it was extremely, extremely cumbersome. And our office was involved at some point in helping to get the production out, and the way we were trying to get the preservation copy redacted was by applying some tags in Adobe. And Adobe couldn't accommodate I think the number of tags and so there was several rounds of QC that had to be done to make sure that no private content was produced. And my understanding from the Facebook side is that there was more than 100 hours of time spent trying to parse this data. Facebook page is a little bit more complicated in terms of content than the Twitter page, Your Honor. At least these were.

THE COURT: All right. That's helpful. Thank you.

You say you had a demonstrative you want to illustrate what you've done. Does the demonstrative also address what's left?

MR. SNELL: Not in terms of quantity, Your Honor, but it does address -- well, in some instances it does. I think it will be helpful.

THE COURT: All right.

MR. SNELL: I haven't talked yet about the Instagram accounts that are both private. And in one of the Instagram accounts there's ten posts and in another there's four posts. So I think that in terms of quantity illustrates what might be there.

THE COURT: All right. And did you -- or does your demonstrative tell me what remains on the Twitter and Facebook accounts, what's not been produced?

MR. SNELL: Yes on the Twitter account, no on the -- yes on the Twitter account with respect to quantity.

THE COURT: Yes.

MR. SNELL: No on the Facebook account with respect to quantity.

THE COURT: All right.

MR. SNELL: Although I think -- can I share the demonstrative? I think walking through it might be useful.

THE COURT: Let's end the suspense. Yeah.

MR. SNELL: Yeah.

THE COURT: All right. So Mr. Snell has just handed me and defense counsel and Mr. Quigley two pages of what look like they might be messages. In any event, it's two pages of it.

MR. SNELL: Thanks, your Honor. So just to walk through this, we have separated the two pages between the two folks who have been subpoenaed here. The first one is Jaquan Rice who is the decedent/victim here.

With respect to the Facebook account, Pistol.Dutch, you see the second bullet is the Facebook produced public account content on April 12th. That's the material you have, Your Honor. But also as noted by the California Supreme Court in Hunter, there was a 2013 search warrant and presumably the information in the account had been shared with defendants. So even though there is private information that Facebook did not produce from its own production, we're not aware that there's anything that wouldn't have been in the search warrant production from 2013.

MS. KAPLAN: Could I just briefly interject? You're talking about the search warrant with respect to Rice. There was never a search warrant with respect to Lee, correct?

MR. QUIGLEY: Yeah, we're just focused on Rice on this page now.

MS. KAPLAN: Thank you.

MR. SNELL: And then with respect to the dbfdutch Instagram account, that's the other Rice account that's subject to the subpoena, that account you can publicly see. We've taken the screenshot here and it has ten posts in it.

And we also know from the Hunter case, the Hunter California Supreme Court case, that the D.A. sought search warrants for three other Rice Instagram accounts and that content was turned over presumably with the defense according to the California Supreme Court.

So what's left with Rice as far as we can tell is ten posts on Instagram and we're not aware of what these

posts would contain that's not contained in the three other Instagram accounts or the Facebook account that's been produced pursuant to search warrant. So with respect to quantity, my understanding is we're just focused on the ten posts in this one Instagram account. I may be wrong on that but we're not less attuned to the merits.

THE COURT: All right.

MR. SNELL: And then the second page is Renesha Lee. This is the witness who I believe will be testifying at trial. And I think the highlight here is that Ms. Lee's never been subpoenaed. There were efforts by the defense I think, maybe some efforts, but she's never actually been subpoenaed. There were representations in the fall of 2018 that she would be but I don't think she has been.

But with respect to her, there is a Facebook account that does have private and public posted messages and with the April 12th production to Your Honor, all the public content from our preservation is now in your hands.

And then for the other two accounts there's a nina03 Instagram account and again we've taken a screenshot from what's publicly available now on the internet, and this account is private but it lists four posts. So I think with respect to content we're just talking about four -- four posts there.

And then for the Twitter account, all tweets were public and all tweets have been produced from the preservation and what's left over is eight private direct messages.

THE COURT: All right. So then the universe of what is in dispute at this point if I understand this would be 22 private posts and then whatever is on Facebook for Ms. Lee?

MR. SNELL: That's our understanding, Your Honor.

THE COURT: All right. And do you have any, I guess, even ballpark of what might be unproduced on that Facebook account?

Let's ask this. How many -- do you know how many messages were produced for Ms. Lee's Facebook account; in other words, how many public posts there were?

MR. SNELL: I don't know, Your Honor.

THE COURT: All right.

MR. SNELL: That's something that I can certainly confirm.

THE COURT: I'm just, you know, wondering if we can sort of deal with proportionality I guess based on what was public.

Anyway, all right. So do you want to address what Ms. Barlow said about deleted content? Like you I thought it was in the balance. But has that even been considered by the service providers whether that could be retrieved?

MR. SNELL: Yeah. Your Honor, my understanding in reading Hunter is deleted content was only focused on deletions of public content where that would be an indication of revocation of consent, not whether content that may have been deleted before the sub-

poena was served was somehow obtainable. Our position would be that that's not obtainable under the Stored Communications Act as an initial matter, but I don't think it exists either anymore.

THE COURT: And in terms of designating something public versus private as you use those terms because Ms. Barlow indicated there might be a dispute about that, how did you define them and when did you define them for, private and public as of what date?

MR. SNELL: So how do we define it? With Twitter, literally going to the internet and what's available on the internet. With Facebook, the same thing with one caveat. I think you need to be logged in to Facebook to see whatever somebody has protected and so the folks who were doing that were logged in.

With respect to --

THE COURT: Like any other user?

MR. SNELL: Yes.

THE COURT: All right. Go ahead.

MR. SNELL: With respect to timing, Your Honor, we tried to make it coincidental with the production, so the QC efforts were an effort to say whatever we have in our preservation copy that's public coincident with the time we're producing is what's being produced. And we believe that's what happened although with the Facebook production -- well, we know that's what happened with the Twitter production because everything is still public. With the Facebook production there's more content to sort through so it's more cumbersome, but I believe we got it right, Your Honor.

THE COURT: So we're talking roughly April 2019?

MR. SNELL: Yeah.

THE COURT: All right. Ms. Barlow, further questions? MS. BARLOW: Well, again, I think it just -- Mr. Snell's definitions begs the question as to what is public versus private and what is restricted versus completely unrestricted.

And I would note that in looking on Facebook myself and Mr. Rice's Facebook page, that Mr. Quigley and I were talking on the telephone. We're both looking at the page and he was seeing different things than I was seeing. So clearly Mr. Quigley is not friends with Jaquan Rice I believe.

MR. QUIGLEY: I didn't know I was testifying at the evidentiary hearing.

MS. KAPLAN: But I did that -- I did that same thing with my investigator where we looked at the same page and it was public and it had completely different feeds.

MS. BARLOW: So I think that there's an open question. The manner in which they produced it gives me even more pause. If that's the test, then I think the Court has to go further into the inquiry of what exactly public versus private is in the legal sense, not what you can see when you get on Facebook but -- and I think I suggested this to the Court, that if the legal definition of privacy is the expectation of the individual who is posting it. And if I post something to Facebook, and I'm going to focus on Facebook because they have so many different settings, and I say only my

friends can see it, then only my friends I understand can see that.

If I share it with friends of friends, then all the friends I have and all of their friends, and you've essentially at that point you've lost control of your post. Anybody who's a friend of a friend of a friend and the more friends you have, the more people will see it and the less you will know about who is seeing what you have posted. So it essentially becomes in essence public.

THE COURT: I understand the argument. I think I followed the Supreme Court's statements on it, both the oral argument that counsel directed me to and the written opinion. Really for right now, for purposes of this, what I care about is produced versus unproduced.

MS. BARLOW: Okay.

THE COURT: Because -- and then unproduced, you know, there may be differences of opinion about whether it's private or public and that might matter in terms of whether it gets compelled to be produced. But at this point I'm just trying to define the universe that's in dispute basically.

MS. BARLOW: Okay.

MR. SNELL: And, Your Honor, I don't want to have Ms. Barlow and Mr. Quigley testify, but my understanding is if you're logged in -- if you're not logged in, you might see something different than if you're logged in. I don't know if they were both logged in at the time.

THE COURT: Understood. All right. So there is some content for both users that has not been produced and I assume that the defense still wants me to order that produced.

MS. BARLOW: Absolutely, Your Honor.

THE COURT: All right. And I assume that the service providers still don't want to produce it.

MR. SNELL: That's correct, Your Honor.

THE COURT: All right. Tell me why I shouldn't order it produced, Mr. Snell, beyond what's in your brief. It looks like you filed something today which I have not read.

MR. SNELL: I don't think anything's been filed today, Your Honor.

THE COURT: All right.

MR. SNELL: It may have been filed last week.

THE COURT: All right. These are just courtesy copies of what you filed before. Okay. I did read that. A couple of thoughts on that.

I read your arguments about the safe harbor that exists in the Act and the good faith requirement and the safe harbor. As far as I'm concerned, if you -- if I were to order this stuff produced, you'd be complying with the order in good faith whether or not you agree to it. It doesn't seem to me that there's a good faith requirement that a party agree that an order is legally correct before the party complies with it. It happens all the time that parties think judges are morons but they still obey orders.

So I don't think that the argument you've made there about the applicability of the safe harbor is valid and so I think that the safe harbor does completely immunize the service providers if I order this material produced. Of course I would only order it produced in camera for my review.

And also, I read some arguments about the -- the obligation or the lack of obligation to provide discovery in a criminal case and the like. You know here, what I think we're dealing with is the Sixth Amendment confrontation right and making sure that the defendants have a complete -- a complete right to do so. So it's not really a matter of a discovery obligation but rather a confrontation right.

So with that understanding, Mr. Snell, tell me why I shouldn't order these evidence produced.

MR. SNELL: Great. Thank you, Your Honor.

Well, I think the first issue we have, and we're not privy to everything that the Court has because there's been a confidential filing, but the first question we have is what is the crystalized constitutional law issue that exists with respect to content that has not yet been produced.

With respect to Jaquan Rice, I think we're talking about ten private posts that are in one of four Instagram accounts, the other three of which have been produced. And my understanding, and I may get this wrong because we're not the ones -- we're third parties here, but my understanding is that with respect to Rice, the evidence is sought to show that he had an individual dispute with Mr. Hunter, Quincy Hunter, and that there's going to be some evidence that shows

that's not gang related but it's a personal issue, and I've not heard from the defense what they expect in these ten posts that might bear on that issue.

With respect to Ms. Lee, Your Honor, we're talking about eight direct messages on Twitter, a handful of four Instagram posts and some private content. I think with respect to that, they want to show that she's a jealous and violent person. In the information that you've seen, Your Honor, attached to their papers and what we've produced, she's -- there's ample evidence to make those arguments.

So with respect to what's missing and why it rises to the level of a constitutional concern, you know I think we need -- we would need much more -- well, we would ask the Court to give much more specificity, because I think we don't view the safe harbor the same way the Court does. We view that as a risk. It's easy for other folks to talk about the safe harbor. It's hard for the providers who are subject to potential criminal claims to read it the way Your Honor reads it. And the statute is completely unambiguous that, you know, providers are not to produce these.

And we talked at the last hearing about easy ways and hard ways. There are very easy ways to get this information. One with respect to Rice is if the Court really feels that there's something in these ten private posts that's important in this one Instagram account, the People have already obtained search warrants for the other three accounts. And under the Evans case that we cited, this California Supreme Court case where the Supreme Court said the trial court can force a pretrial lineup for the People to perform a pretrial lineup for the benefit of the defense, Your Honor, we

think you could either order the D.A. here to remedy a constitutional issue with respect to seeking a final search warrant for the last remaining Instagram account or do whatever you want evidentiary wise if they refuse to do that.

With respect to --

THE COURT: Let me say --

MR. SNELL: Yeah.

THE COURT: -- for reasons that I think we've discussed before, I don't see any alternatives as viable for obtaining this information in the form and the manner, and the authenticity guarantees that the defendants would need it. So I'm -- unless you have new arguments in that realm, I really am past it.

MR. SNELL: Yeah, I understand, Your Honor. We don't -- well, we strenuously disagree. They've never subpoenaed Ms. Lee.

THE COURT: I understand.

MR. SNELL: It's been going on since 2014. They've never issued a subpoena to the witness, which is another easy way to get this information. And I think the Evans case gives the Court clear guidance to fashion a remedy with respect to the parties and not with respect to nonparties.

Your Honor, let me briefly address the Stored Communications Act. As I said it's a federal statute. It's unambiguous. There are exceptions but they don't apply here. The defense has tried to sort of make it look like they might apply, they just -- they don't. Providers are prohibited unless there's an exception from providing this information.

THE COURT: Why wouldn't Section 2707(e)(1) apply and immunize the service providers? That's the good faith reliance defense that is addressed in your brief.

MR. SNELL: Yeah. I think our view, Your Honor, is that an order that tries to create an exception under the Stored Communications Act where one doesn't exist is not an order we can rely on in good faith. And that's something that -- and I may be getting ahead of myself but I think we would ask the Court for a firm ruling on the grounds for why the information is needed from the providers and would ask time for a writ.

Your Honor, we've also cited the O'Grady case that sided with us on the issue of good faith and said that you can't rely on the Court's order to create good faith where it doesn't exist.

THE COURT: Yeah. I think we may have a different reading of O'Grady in that instance. But I did -- as I said, to me I see that provision Section 2707(e)(1) as a complete defense that will be available to the service providers' right to order these items produced.

MR. SNELL: Your Honor, I'd like to make just a few more points.

THE COURT: Go ahead.

MR. SNELL: One is that we think there's a reasonable statute and there's statutes that are passed by legislators all the time that prohibit production of information. The California Supreme Court has agreed with that in the Gurule case that analyzed

privilege. The finding was that the due process violations do not allow you to trump the attorney/client privilege. That's a state law privilege, it's not a federal statute passed by Congress to protect privacy and to extend the original protections that exist for mail and other means of communication or electronic communications. So we would view the other Stored Communications Act even heightened from the Gurule case where privilege is sacrosanct.

And there's also the case, Your Honor, Webb. That's a case that actually the California Supreme Court was analyzing psychotherapists' records and these were records that were not held by the state. The cases that address psychotherapy records are mainly focused on the state or where they're in the possession of a government. And in the Webb case the Court held that it was very skeptical whether any risk -- any constitutional risk can be material enough to trump voluntary private psychotherapy visits and that the confidentiality of those should be sacrosanct as well.

We don't think it's unusual for a court to find that a statute like this, a reasonable statute should be upheld in spite of constitutional claims. And we think any time a court has held that you need to stray to address a constitutional issue, the remedy is with the state, it's not in ordering a private party to violate federal law.

And we've -- you know, the U.S. has submitted briefs that agree with that position. We've submitted that in the Wint case as part of our most recent filing, Your Honor. Wint was a case. This is in the D.C. Circuit. Wint was a case at trial. It was a trial subpoena

and the Court nonetheless found that there were not constitutional concerns that trump the Stored Communications Act and found that the Stored Communications Act should be upheld with respect to the providers in that instance.

And the U.S. submitted a brief saying we agree and if there's remedies the Court believes should be applied, they should be applied against the state with respect to the parties who were actually in the action, not with respect to a third party.

THE COURT: All right. Thank you.

Ms. Barlow.

MS. BARLOW: Well, I think we're on the same page as you are, Your Honor, in terms of the safe harbor provision of the S.C.A. And I think that it's well settled in criminal proceedings at least that confidential documents are routinely produced, even psychotherapists' records are produced even though there is a privilege that is statutory. The attorney/client privilege is a little bit of a different animal because it's actually a constitutional privilege. It's different than the attorney work product privilege, and so a statute can't trump that constitutional right to confidential communications with your attorney in the criminal arena.

And I briefed for the Court the California law on privilege and absolute privilege and I think the rationale there is very clear and it's a very useful roadmap for the Court which is that if there are exceptions that allow for production, essentially what exists with the S.C.A. is a qualified privilege, that

there are certain circumstances which allow production of this. And as long I think that this Court is engaged in the process and the Court is making findings such as materiality or good cause in the case of a subpoena, that does -- the order from the Court to produce the information would clearly provide the service providers with a safe harbor for complying with that.

And I agree with the Court that the rationale that it doesn't matter if they like your order or they disagree with it. If the Court orders the production, then there's a legal obligation to comply, that is outside of their own personal ideas of whether or not it's a valid order.

THE COURT: Let me ask the defendants' counsel. You heard Mr. Snell ask -- state that the service providers were going to writ if I order these items produced. Obviously that's going to slow the process down. I don't know what the defendants want in terms of the effect on a trial date that that would have.

MS. KAPLAN: Well, let me say this, Your Honor. I wanted to take this up before we got started but we got started quickly. So at this point both Mr. Sullivan and Mr. Hunter want to assert their right to a speedy trial, withdraw any time waivers and require a trial within 60 days.

And is that correct, Mr. Sullivan?

DEFENDANT SULLIVAN: Correct.

MS. KAPLAN: And for Mr. Umali, may I ask Mr. Hunter if is that correct?

MR. UMALI: That's correct. And I would like to add something once Ms. Kaplan is done.

THE COURT: You promised you weren't going to say anything else, Mr. Umali.

MR. UMALI: Not on the Facebook side, Your Honor.

THE COURT: And on that score, I mean we've got the May 14th start date.

THE CLERK: The last day is July 1st now.

THE COURT: Last day July 1st. All right.

MS. KAPLAN: So we'll move it up a few days.

THE COURT: But in any event, we had already set May 14th and I intended to honor that. I intend to honor that but -- and that's what my question really goes to.

MS. KAPLAN: Yeah.

THE COURT: There's no way this process gets done by May 14th.

MS. KAPLAN: Right. So our feeling is that we want a speedy trial. We've always wanted a speedy trial once this was resolved. It appears to us that the Supreme Court has wanted us to be in trial, wanted the trial court to resolve these issues, and that we are asserting once again our right to a speedy trial.

And Facebook may take a writ. And I'm sure this will be found to be incredibly disrespectful, but as far as I can tell, they have nothing but money and time to spend writting things and they have no real human people involved in their litigation.

Additionally, for example, yesterday, I read something about a 100 million-dollar fine or something like that they have to pay. So that being said --

THE COURT: They have rights too, okay.

MR. SNELL: Yeah.

THE COURT: Hold on, hold on. Disrespectful moment is over for everybody.

MS. KAPLAN: Right.

THE COURT: I understand Facebook's got its own interests here. I intend to protect them as well. I don't trivialize them.

MS. KAPLAN: Right, I understand that but --

MR. SNELL: Your Honor, no court in 30 years has forced providers to produce documents, whether there's a constitutional issue or not. I mean this is unprecedented. We understand these are serious proceedings, Ms. Kaplan, but it's completely unfair to be just be flip about the issues on our side. All right.

MS. KAPLAN: We routinely ask courts to force production of documents. That having been said, our position is we're in trial, we are in a speedy trial. We have a last day. If Facebook takes a writ, they will take a writ. It will be up to the Court of Appeals to decide or the Supreme Court or whoever to decide if they're going to do anything about it. They may very well not issue a stay. So I can't tie Facebook's hands, nor can any of us but our posture is very clear. We want a speedy trial. We have a last day. And we appreciate the Court's attention to getting things done in a timely fashion.

THE COURT: All right. Mr. Umali.

MR. UMALI: Can I just add, first of all, I join Ms. Kaplan in her comments. We are of the same position.

And I just want to add that quite some time ago, I announced that I was ready for trial in Department 22, that the case was transferred here for all purposes including trial.

From my notes -- I'm sorry. We were first transferred to Department 16. Because of Judge Brown's elevation to the Court of Appeals, we returned to 22 and we were transferred for trial and all purposes to this department. I believe on March 1, 2019, we were transferred to this court. At that point in time, Mr. Hunter did announce that he was ready for trial. We were ready for everything but for the resolution of the Facebook issues, but the Court did set a schedule with regard to our motions in limine. I was the first to file those and they were filed on the due date that the Court had set.

We understand that we have a May 6th opposition deadline, which is this coming Monday. I and my team have drafted almost all of our oppositions. We are just doing the finishing touches and we will file them on Monday morning to this court and of course serve everybody that needs to be served at that time.

There are some outstanding issues that need to be resolved quickly I think or else witnesses could be lost. And I -- I -- I would object to any delay whatsoever. And I would ask for a trial to commence as soon as possible. I think that I believe that the 402 hearings that would result from our in limine motions as well as the district attorney's in limine motions do constitute the beginning of the trial so for all intents and purposes, I am in trial.

I did want to add one personal note. There was some scheduling problem. I thought we were going to

be here for April 16th for a hearing. Apparently there was some miscommunication with regard to the court schedule at that time. I did fly back from New York on the evening of April 15th and was told that I don't need to be here at all on April 16th. I was prepared to go with the hearing which I thought -- which I think is the same hearing that we're doing today.

THE COURT: I apologize for that. I checked everything except my daughter's spring break schedule before we set that last hearing.

MR. UMALI: Your Honor, I mean no disrespect and I don't mean to disparage the Court or anybody else.

THE COURT: Not at all. I appreciate all of you being patient.

MR. UMALI: All I'm trying to do, Your Honor, is to say that I am eager to begin this trial because Mr. Hunter announced ready for trial in 2015. The Facebook appeals essentially occurred which took almost three years essentially to resolve and Mr. Hunter waited very patiently for that to be completed --

THE COURT: I understand.

MR. UMALI: -- because we believed it was important. THE COURT: May 15th we're on calendar. No more spring breaks. We'll get going then.

You mentioned something about witnesses who may be lost?

MR. UMALI: There are. There are three witnesses that I have that are the subject of my motion to compel discovery for current whereabouts and/or in

the alternative a meeting, with those witnesses. I requested those witnesses from the very start of the case, the whereabouts of those witnesses. Those witnesses -- the current addresses at the time which were not provided to me but I can tell from my investigation at least the neighborhood of those current witnesses was an area which has now been destroyed or demolished. So all those witnesses have been relocated.

Back in 2015 when I thought the case was ready for trial posture with a different deputy district attorney, Ms. Heather Trevisan, that those three witnesses would be provided to me, either their current whereabouts and/or a meeting in the District Attorney's Office where those witnesses were so I can serve trial subpoenas and interview them of course.

Because of the Facebook issues that has been delayed essentially for three years, but once this case started to come again forward towards trial posture, I made the same request both informally and in writing, and through a motion with this district attorney, Deputy District Attorney Mr. Quigley. I have not received a response. assume I'm going to receive a response.

Now, depending on what that response is, if the response, for example, is we don't have any current addresses, then there's a due process issue because all three witnesses are exculpatory witnesses essentially whose whereabouts have been withheld from the defense and those three are material exculpatory witnesses. So we need to move on with issues like that as soon as possible.

I think at the last -- I addressed this in camera with the Court, this issue. Mr. Quigley represented

that he thought we could resolve this issue informally. We have not yet done so but because of these delays, then I'm afraid that at some point I'm not going to have the time to find these witnesses, interview them and subpoena them to court.

THE COURT: I understand. Okay. Thanks for crystalizing that.

MS. KAPLAN: Your Honor, two short remarks in response to the Court's question. The first is that I would consider us to be in trial and that this hearing to be a 402 hearing. So I do not feel we are in any way pretrial.

And the second is that the -- Mr. Snell gave us a handout and on the second page of that handout where he has Renesha Lee listed. And the first thing he has listed is an account called Nesha.Lee.35 saying this is a public account. This account does not appear on Facebook. If you type in Renesha. Lee.35 it comes back to a woman named Flor, F-L-O-R, Perez, P-E-R-E-Z, who is clearly not Renesha Lee in any way, shape or form. So this account does not exist unless he knows where it is but it's not there.

THE COURT: All right. Let me hear from the defendants about production the service providers have already made. Is this an in-camera production along the lines of what we've been talking about with respect to the private items or something else? I know you haven't seen it yet so just speaking in the abstract.

MS. BARLOW: Well, I would assume that they're all, quote, public because they are things that we could see if we had the time to go and look at the individual posts on the particular pages. So I would

suggest that the Court doesn't have a need for an in-camera hearing unless there's no privacy concerns. And that also relieves the Court of the obligation of going through the posts and trying to figure out which ones might be relevant because of what the defense theory might be and how it relates to Ms. Lee and her posts. It seems like extra work for the Court that is really not necessary.

THE COURT: I think the only conceivable privacy issues, you know, might be, for example, with health care. I mean it's highly unlikely that there's something in here related to somebody's personal health, for example, and sometimes addresses and other identifying information of uninvolved people merit protection.

I'll review this stuff. I tend to agree that it's really hard to imagine what might need to be redacted but I think it's the safer course for me to go through it.

MR. UMALI: May I just make a suggestion, Your Honor?

THE COURT: Yes.

MR. UMALI: The Court mentioned something about health care posts and things like that.

THE COURT: Yeah.

MR. UMALI: My understanding of what some of those health care posts may reveal is that Ms. Renesha Lee at the time of the homicide in this case was actively trafficking prescription medication to the public.

THE COURT: All right. Well, that's not what I was talking about so I don't know.

MS. KAPLAN: Your Honor, we're aware due to our discovery that she suffers from a chronic health condition which involves the taking of narcotics for the treatment of that health condition and that she was I believe discovered in the hospital.

THE COURT: I'm sorry?

MS. KAPLAN: She was in the hospital.

THE COURT: Okay.

MS. KAPLAN: We all know -- in the end it might not be relevant, or may but we're all aware of her health condition.

THE COURT: That's good to know.

Let me just go back to Mr. Snell and Mr. Quigley for that matter. Do either of you -- just a simple question. Do either of you think I have it wrong in terms of doing an in-camera review of these items and what I'd be looking for to protect?

MR. QUIGLEY: No.

THE COURT: To excise if necessary?

MR. SNELL: No.

THE COURT: In other words, are either of you aware of anything sensitive in these other than what I've described theoretically that I should be looking for in order to potentially withhold from accounts?

MR. SNELL: Your Honor, I think the providers are agnostic on that point. I think the effort has been to produce only public information and I believe only public information has been produced.

THE COURT: All right. And so that means as Ms. Barlow described with the right manipulation of key strokes, this is something that anyone with public access to Facebook or Twitter or Instagram could find themselves?

MR. SNELL: Yes, Your Honor.

THE COURT: Mr. Quigley, anything more on that issue? MR. QUIGLEY: No.

THE COURT: All right. So the elephant in the room is burden I think with respect to the non-produced items.

And I understood, Mr. Snell, that you were going to provide a knowledgeable witness on that today to talk about the burden in what you did produce, so it's certainly not trivial what the parties have incurred but I think we need more -- before I can do the balancing I think we need to do, I think I need more detail on the burden that would be involved were the non-produced items to be produced.

MR. SNELL: Can I have a moment to confer with the client, Your Honor, on the issue?

THE COURT: Yes. In fact, why don't we take our morning break. We'll take 15. Let's come back at a quarter of.

(Brief recess.)

THE COURT: Thank you. Welcome back. We're back on the record.

All right. Mr. Snell.

MR. SNELL: Your Honor, I appreciate the break. Just one preliminary. During the break we did check

the Nesha.Lee.35 account and it does appear the account that was subpoenaed and which we produced documents.

MS. BARLOW: Your Honor, we also were looking at it over the break and it appears to be in part -- there's a new screen name or whatever you call it, but new identities of somebody who does not look like Ms. Lee. But going back in time to the public posts that are there, it appears to be her actual Facebook page and it was the one that was subpoenaed.

MS. KAPLAN: So we would need a custodian of records to say that at the time those posts were made, it was clearly the post of Renesha Lee. And what appears to be an attempt to change the identity by having a Hispanic name and Hispanic friends and Hispanic interests is -- whatever purpose it was done for, there still remains on the posts some photos of her and I think her child, and some comments that would hardly be attributed to a Ms. Gomez.

MR. SNELL: And, Your Honor --

THE COURT: Yes.

MR. SNELL: -- we can hardly be put to the test of identifying who actually made posts.

THE COURT: I understand.

MR. SNELL: We have affirmed that they're business records that's been produced and that defense will receive that if you allow it.

THE COURT: Very well.

MR. SNELL: And just harkening back to our last hearing, we're talking about public and private content. We're no longer I think in the world of the

Hunter Supreme Court's burden argument where public's available and private's not.

So if Your Honor is going to order a production of private content, I think that production would be similar to what Facebook and Twitter do in response to legal process. There is obviously a burden associated with it but it's something that they do in the ordinary course of business. And I don't think we want to advance a burden argument, Your Honor, with respect to what would be that sort of response in response to normal legal process.

THE COURT: All right. Well, I appreciate that both from the standpoint of simplifying the issues and from the standpoint of 100 plus hours that have already been spent and would have to be spent in further compliance with further orders is not trivial in my mind, it's significant.

And so I still -- I credit the service providers for having done so and for any further burden that is imposed here. Obviously, the defendants' rights, their Sixth Amendment right is very important here.

I think particularly even I know, Mr. Snell, you weren't able to see some of the statements of relevance that the defendants provided to me for in-camera review, but even just I think watching the video of the Supreme Court arguments and what the Chief Justice herself articulated, you know, better than I could about why in this particular case these posts are so significant. It seems like they were significant to the People in identifying the defendants, in deciding to charge them, presumably will be relied upon by the People at trial in some part. And as I think I said before, it's hard for me to imagine a case where there's

greater relevance imposed in a post like this. It's not to say that the Facebook account of a party or a defendant or a witness in every criminal case is going to be relevant or the like, but here, I think this is a special case and it seems to me that the Supreme Court would recognize that.

Anyway, so I'm prepared to order -- for the reasons we've talked about is to order the service providers to produce these items. What does that mean timing-wise for the service providers and any -- any writ requests you might want to file?

MR. SNELL: And my understanding, Your Honor, that it will be an oral order of the Court today that we would be acting from rather than from a written order?

THE COURT: That's correct.

MS. BARLOW: I'm sorry. I don't mean to interrupt you, but finish your thought and then I'll have my say.

MR. SNELL: Yeah. Your Honor, I understand there's some other scheduling issues going on in the case. I think we would want as much breathing room that we can get to prepare and file a writ.

I think there's a date, May 14th that's coming up, but if we could get three weeks that would be preferable, but whatever the Court could extend.

And also, Your Honor, with respect to the ruling, I think it would be helpful to get a little more guidance respectfully from you about --

THE COURT: Of course.

MR. SNELL: -- whether the Sixth Amendment right attaches to each of the items sought from each of the witnesses. I mean Rice is deceased so he won't be a witness at trial but to better understand the Court's rationale in preparing any writ papers.

MS. BARLOW: Your Honor, just so I understand what the service providers' position is, I want to be crystal clear on the record, is it -- if I'm understanding correctly is that they are withdrawing their argument of burden because the Court is poised to order them to produce this information; therefore, it's not burdensome to them anymore, it's simply a production as they do with any warrant.

Is that correct? It might not have been an artful statement.

THE COURT: I think what he's saying is that it's not burdensome but it's not inordinately burdensome.

MS. BARLOW: Right.

THE COURT: Such that it gives them a defense.

MS. BARLOW: That's what I thought.

MR. SNELL: And just to be clear, with respect to the pretrial issues that we dealt with, that the California Supreme Court dealt with in Hunter, we maintain that that sort of public production is extremely burdensome and we've now lived through it and it's extremely burdensome. With respect to a court order that public and private information needs to be produced, there is a burden but as the Court said, we're not going to rely on that burden because that's a sort

of response that the providers do to legal process in the ordinary course.

MS. BARLOW: And I'd also like to add, Your Honor, that I think the Court in its ruling has said Sixth Amendment right to confrontation, while that's an important right and it's clearly attached in a trial situation, I think that also *Pennsylvania v. Ritchie,* the Fourth Amendment due process clause is in some ways even more important. And I would hope that the Court would say that as part of the ruling that the Court is relying on on both of those constitutional rights in ordering the production just to make it a bulletproof type of opinion or order.

THE COURT: I understand. Yes, I think both of those rights of both of the defendants need to be protected here of course. And I find that both require the production of the unproduced items that have been identified by the service providers at this hearing. That will be the ten private posts on Mr. Rice's Instagram account, the four private posts on Ms. Lee's Instagram account, eight private direct messages on Ms. Lee's Twitter account, and the private posts and messages on Ms. Lee's Facebook account.

As I understand what you've told me, Mr. Snell, that's the sum total of what has been requested but not yet produced by the service providers.

MR. SNELL: That's my understanding, Your Honor.

THE COURT: All right. And to the extent there's any weighing that can be done with the withdrawal of the burden argument, I think that these rights are important enough in this particular case, as

I've said, given the relevance of electronic messages that's been raised in this particular case, with these particular charges and these particular defendants, it would certainly outweigh any -- a burden like the one you've described it as the one that's already been incurred. If we were talking about a far greater burden or something else, I might feel differently but I think the most important thing, or one of the most important things is to clarify again, you know, this ruling is really about this case and these defendants and their rights.

All right. What about timing and Mr. Snell's request for a stay?

MS. BARLOW: I would request, and I think Mr. Umali and Ms. Kaplan would agree with me on this, given the posture of the case and given the defendants have been in custody and very patient for quite some time around this litigation, that this court proceed as already decided to proceed with the beginning of trial and with the motions in limine, et cetera May 14th. And then if the service providers want a stay, they should seek it from the Court of Appeal, but they need to comply with the Court's order immediately or as soon as they can and then they can go to the court.

THE COURT: Well, I think -- I think I'm limited in my ability to extend a stay given the defendants' assertions of speedy trial rights, but I do want to give the service providers enough time to proceed to the Appellate Court, ask for a stay there without, you know, my order taking effect before they have an opportunity to do that.

MR. QUIGLEY: Well, I would just point out based on the timing -- I'm not a party to this, but I do

have concerns for getting half of -- getting certain -- like half of our balls rolling if there's another issue going on, which is the only part that I would care about.

But from what I'm -- just looking at the calendar, from what Mr. Snell asked for, I think that's only a week past the date we had set for the 14th and that's still six weeks prior to the last date that the Court set. So I think it's within the reasonable range here. And if the Appellate Court issued their stays, then that would be the end of it, but it doesn't sound like he's asking for something that sort of sabotages our schedule very much.

THE COURT: Right now we've got May 14th as a startup of 402s.

Let me suggest this. Mr. Snell, why don't I give you a stay until May 13th, the day before our 402s start just to be safe. Obviously you're going to ask the Appellate Court for a further stay and they'll rule on that.

All right. And what else do we need to do today?

MR. QUIGLEY: That's the only thing that's on today.

MS. BARLOW: So if I understand -- I'm sorry, I always like to clarify myself -- the Court has issued a stay as to the service providers' production to the 13th of May?

THE COURT: Yes.

MS. BARLOW: Okay.

THE COURT: So the order's stayed until May 13th so that they can seek an appellate review if they wish to and any stay from the Appellate Court.

THE CLERK: And you're not releasing those subpoenas that you have now?

THE COURT: Oh, the records that I have now, yes, I'm not releasing these until after I do the in-camera review. Given what I learned about the volume, I don't think that will take long.

And do we need to set a special hearing for that or should I just say I'll produce any unredacted portions on that --

MS. KAPLAN: That's perfect.

THE COURT: Perfect is what I shoot for.

MR. SNELL: Your Honor, I'd ask to clarify one thing.

THE COURT: Yes.

MR. SNELL: That it's clear we're not waiving our right to make a burden argument on public production and I don't think that's -- I think I made that clear when I was laying out the issues, but I just want to make that clear.

THE COURT: Right, because you said you --

MR. SNELL: We've sustained that burden in this case already.

THE COURT: Right, right. The burden's been incurred already.

All right. Anything else? Thank you all.

MS. KAPLAN: So, yes. May 14th

THE COURT: Put your hand up, please.

MS. KAPLAN: May 14th is our next court date; is that correct?

THE COURT: Yes.

MS. KAPLAN: And could Madam Clerk and Mr. Sheriff please be clear, if there are any intervening dates scheduled in our case, that the defendants do not need to come to court until May 14th. Every now and then there's something written down like briefs due and they show up.

THE CLERK: Yeah. I have May 6th for responses, but they've waived and so --

THE COURT: That's not even a hearing.

(Whereupon, at 11:07 a.m. the proceedings were concluded.)

---o0o---

State of California)
)
County of San Francisco)

I, Jacqueline K. Chan, Official Reporter for the Superior Court of California, County of San Francisco, do hereby certify:

That I was present at the time of the above proceedings;

That I took down in machine shorthand notes all proceedings had and testimony given;

That I thereafter transcribed said shorthand notes with the aid of a computer;

That the above and foregoing is a full, true, and correct transcription of said shorthand notes, and a full, true and correct transcript of all proceedings had and testimony taken;

That I am not a party to the action or related to a party or counsel;

That I have no financial or other interest in the outcome of the action.

Dated: May 2, 2019

/s/ Jacqueline K. Chan

JACQUELINE K. CHAN,
CSR No. 10276

Attachment 3

S256686

IN THE SUPREME COURT OF CALIFORNIA

En Banc

FACEBOOK, INC. et al., Petitioners,

v.

SUPERIOR COURT OF SAN FRANCISCO COUNTY, Respondent;

DERRICK D. HUNTER et al., Real Parties in Interest.

The requests to appear pro hac vice are granted.

In light of (1) the fact that trial has begun *(Martinez v. Illinois* (2014) 572 U.S. 833, 840; *People v. Rogers* (1995) 37 Cal.App.4th 1053, 1057, fn. 3; see also *People v. Superior Court (Douglass)* (1979) 24 Ca1.3d 428, 431, fn. 2), and (2) the trial court's finding of a strong justification for access to the sought information by real parties in interest (see, e.g., Pet's Ex. 1, RT of May 1, 2019, at pp. 38-39 & 41-42; see generally, *Kling v, Superior Court* (2010) 50 Cal.4th 1068, 1075), the petition for writ of mandate, prohibition, and/or other extraordinary relief is denied. The stay previously issued by this court is dissolved.

/s/ Cantil-Sakauye
Chief Justice

Attachment 4

IN THE COURT OF APPEAL OF THE
STATE OF CALIFORNIA
FIRST APPELLATE DISTRICT
DIVISION FIVE

FACEBOOK, INC. et al.,
Petitioners,
v.
SUPERIOR COURT FOR THE CITY AND COUNTY OF SAN FRANCISCO,
Respondent;
DERRICK D. HUNTER et al.,
Real Parties in Interest.
A157143
San Francisco No. 13035657 and 13035658

ORDER DISSOLVING STAY AND ORDER TO SHOW CAUSE

BY THE COURT:

The court has preliminarily reviewed the parties' briefing regarding this petition, as well as the record.

The court is mindful of the impending trial, including real parties' assertion of their speedy trial rights (with a last day of July 1, 2019), and petitioners' assertion of the need for a stay of the superior court's disclosure order notwithstanding the "safe harbor" provision of the Stored Communications Act (SCA, 18 U.S.C. § 2707, subd. (e)(1) [good faith reliance on a court order is a complete defense to any civil or criminal action brought under the SCA or any other law]; see also *Facebook, Inc. v. Superior Court* (2018) 4 Ca1.5th 1245, 1290, fn. 46 [observing that subdivision (a) of section 2707 "contemplates liability only for a

provider that violates the Act 'with a knowing or intentional state of mind,' " and that subdivision (e)(1) "provides a safe harbor for a provider who, in 'good faith,' relies on 'a court . . . order"].) Taking all of those issues into account, as well as the voluminous record (in excess of 1,300 pages), and the need for meaningful and time-consuming review of the issues presented by the petition, the court hereby dissolves our earlier May 9, 2019 order imposing a stay on the superior court's May 1, 2019 order requiring petitioners to produce additional documents in *People v. Hunter et al.,* San Francisco County Superior Court case Nos. 13035657 and 13035658. On or before July 3, 2019, petitioners shall inform this court. in writing of their compliance with the May 1, 2019 order.

Furthermore, notwithstanding any potential issues of mootness that could arise from the dissolving of our prior stay order, the court has decided to retain this matter for consideration, and to issue an order to show cause.

Therefore, good cause appearing from the petition for writ of mandate/prohibition on file in this action, IT IS ORDERED that respondent superior court show cause before this court, when the matter is ordered on calendar, why the relief requested in the petition should not be granted.

The return to the petition shall be served and filed within thirty (30) days of the issuance of this order to show cause. The reply to the return shall be served and filed within fifteen (15) days after the filing of the return. (Cal. Rules of Court, rule 8.487(b).)

This order to show cause is to be served and filed on or before July 1, 2019. It shall be deemed served

upon mailing by the clerk of this court of certified copies of this order to all parties to this proceeding and to respondent superior court.

The justices will be familiar with the facts and issues, will have conferred among themselves on the case, and will not require oral argument. If oral argument is requested, the request must be served and filed on or before August 6, 2019. If no request for oral argument is filed on or before that date, the matter will be submitted at such time as the court approves the waiver and the time for filing all briefs and papers has expired. (Cal. Rules of Court, rule 8.256(d)(1).) If oral argument is requested, the court will notify the parties of the exact date and time set for oral argument, which will occur before Division Five of this court at the courtroom located on the fourth floor of the State Building, 350 McAllister Street, San Francisco, California.

Date Jul 1 2019 Simons, J., Acting P.J.

Attachment 5

July 22, 2019

VIA TRUEFILING

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

Re: ***Facebook, Inc., et al. v. Superior Court of the City and County of San Francisco***, Case No. A157143 (San Francisco Superior Court Case Nos. 13035658 and 13035657)

Dear Presiding Justice Humes and Associate Justices:

On July 1, 2019, this Court ordered Providers to send an update on "their compliance with the [Superior Court's] May 1, 2019 order," which required Providers to produce to Defendants the private communications of third parties without finding a valid exception under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.* Providers hereby inform the Court that they are unable to comply with the Superior Court's order because compliance with the Superior Court's order would violate the SCA. Providers have consistently maintained this position before the Superior Court, this Court, and the Supreme Court.

Providers stand ready to produce the information Defendants have requested, if and when they receive a lawful request for the information that complies with the SCA. For example, the SCA allows for the production of a person's private content with the consent of the sender or recipient of the communication, or in response to a lawful search warrant. *Id.* at §§ 2702(b), 2703(c). Thus, as the Supreme Court noted, Defendants may ask the "Superior Court [to] compel [Ms.

Lee] to consent to disclosure by a provider," or the Superior Court may seek to determine whether "the prosecution [would] issue a search warrant under the Act, on behalf of a defendant." *Facebook Inc. v. Superior Court* ("*Hunter II*"), 4 Cal. 5th 1245, 1291 n.47 (2018).

Further, if the Superior Court evaluates those possibilities and determines they are not viable means of obtaining the content Defendants seek, the Superior Court may exercise its considerable trial management discretion to impose limitations on the prosecution at trial. For example, the Superior Court could prohibit the prosecution from calling the witness whose communications are at issue or limit her testimony *(see, e.g., Davis v. Alaska,* 415 U.S. 308, 320 (1974)), issue adverse jury instructions correcting for the absence of evidence *(People v. Cooper,* 53 Cal. 3d 771, 811 (1991)), or force the prosecution to choose between issuing a search warrant and facing adverse consequences *(General Dynamics Corp. v. United States,* 563 U.S. 478, 484-85 (2011)). If the prosecution declines to assist Defendants in obtaining necessary records in a manner that complies with the SCA, the proper remedy lies against the prosecution, not Providers.

Providers note that this Court has granted Providers' Petition for a Writ of Mandamus and is positioned to review the lawfulness of the Superior Court's May 1, 2019 Order under the SCA. Providers reserve all rights to continue challenging the legality of the order in those proceedings and in any other appellate proceedings that may become necessary.

Very truly yours,

/s/ Joshua S. Lipshutz	/s/ James G. Snell
Joshua S. Lipshutz Gibson, Dunn & Crutcher LLP	James G. Snell Perkins Coie LLP

Counsel for Petitioners Facebook, Inc. and Twitter, Inc.

Attachment 6

SUPERIOR COURT OF CALIFORNIA
County of San Francisco

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. Lee Sullivan and Derrick Hunter, Defendants.	Cause No. 13035657 & 13035658 ORDER TO SHOW CAUSE RE CONTEMPT

ORDER TO SHOW CAUSE RE CONTEMPT

To Facebook, Inc. and Twitter, Inc.

YOU ARE HEREBY ORDERED to appear before the above-entitled court in Department 21, located at 850 Bryant Street, San Francisco, California, on July 24, 2109, at 3 p.m., to show cause, if any, why you should not be adjudged guilty of contempt of court, and punished accordingly, for the acts of willful disobedience of the order of the above-entitled court, as provided in section 1209(a)(5) of the California Code of Civil Procedure, and as more fully described in your letter to the California Court of Appeal dated July 22, 2019. A copy of your letter is attached and shall be served on you with a copy of this order and by this reference incorporated as though fully set forth.

Dated: July 23, 2019

/s/ Charles Crompton
JUDGE CHARLES CROMPTON
SAN FRANCISCO SUPERIOR COURT

Superior Court of California

County of San Francisco

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. Lee Sullivan and Derrick Hunter, Defendant.	Case Number: 13035657 & 13035658 **CERTIFICATE OF SERVICE BY MAIL** (CCP 1013a (4))

I, JORY LATORRE, a Deputy Clerk of the Superior Court of the County of San Francisco, certify that I am not a party to the within action.

On JULY 23, 2019, I served the attached NOTICE TO APPEAR, by sending an electronic letter copy thereof, addressed as follows:

GIBSON, DUNN & CRUTCHER LLP Joshua S. Lipshutz, Bar No. 242557 jlipshutz@gibsondunn.com	PERKINS COIE LLP James G. Snell, Bar No. 173070 JSnell@perkinscoie.com John R. Tyler, *admitted pro hac vice* RTyler@perkinscoie.com Anna M. Thompson, *admitted pro hac vice* AnnaThompson@perkinscoie.com

and, I then sent the electronic letter on that date following standard court practices.

Dated: JULY 23, 2019 T. MICHAEL YUEN, Clerk

By: /s/ Jory Latorre
JORY LATORRE,
Deputy Clerk

APPENDIX D

Filed 5/24/18

IN THE SUPREME COURT OF CALIFORNIA

FACEBOOK, INC., et al., Petitioners, v. THE SUPERIOR COURT OF THE CITY AND COUNTY OF SAN FRANCISCO Respondent; DERRICK D. HUNTER et al., Real Parties in Interest.	S230051 Ct.App. 1/5 A144315 San Francisco City and County Super. Ct. Nos. 13035657, 13035658

INTRODUCTION AND OVERVIEW

Real parties in interest Derrick Hunter and Lee Sullivan (defendants) were indicted by a grand jury and await trial on murder, weapons, and gang-related charges arising out of a drive-by shooting in San Francisco. Each defendant served a subpoena duces tecum on one or more petitioners, social media service providers Facebook, Inc. (Facebook), Instagram, LLC (Instagram), and Twitter, Inc. (Twitter) (collectively, social media providers, or simply providers). The subpoenas broadly seek public and private communications, including any deleted posts or messages, from the social media accounts of the homicide victim and a prosecution witness.

As explained below, the federal Stored Communications Act (18 U.S.C. § 2701 et seq., hereafter SCA or Act)[1] regulates the conduct of covered service providers, declaring that as a general matter they may not disclose stored electronic communications except under specified circumstances (including with the consent of the social media user who posted the communication) or as compelled by law enforcement entities employing procedures such as search warrants or prosecutorial subpoenas. Providers moved to quash defendants' subpoenas, asserting the Act bars providers from disclosing the communications sought by defendants. They focused on section 2702(a) of the Act, which states that specified providers "shall not knowingly divulge to any person or entity the contents of" any "communication" that is stored or maintained by that provider. They asserted that section 2702 prohibits disclosure by social media providers of *any* communication, whether it was configured to be public (that is, with regard to the communications before us, one as to which the social media user placed no restriction regarding who might access it) or private or restricted (that is, configured to be accessible to only authorized recipients). Moreover, they maintained, none of various exceptions to the prohibition on disclosure listed in section 2702(b) applies here. And in any event, providers argued, they would face substantial technical difficulties and burdens if forced to attempt to retrieve deleted communications and should not be required to do so.

---

[1] Future undesignated statutory references are to title 18 of the United States Code.

Defendants implicitly accepted providers' reading of the Act and their conclusion that it bars providers from complying with the subpoenas. Nevertheless, defendants asserted that they need all of the requested communications (including any that may have been deleted) in order to properly prepare for trial and defend against the pending murder charges. They argued that the SCA violates their constitutional rights under the Fifth and Sixth Amendments to the United States Constitution to the extent it precludes compliance with the pretrial subpoenas in this case.

The trial court, implicitly accepting the parties' understanding of the SCA, agreed with defendants' constitutional contentions, denied providers' motions to quash, and ordered them to produce the requested communications for the court's review in camera. Providers sought, and the Court of Appeal issued, a stay of the production order. After briefing and argument, the appellate court disagreed with the trial court's constitutional conclusion and issued a writ of mandate, directing the trial court to quash the subpoenas. We granted review.

Our initial examination of the Act, its history, and cases construing it, raised doubts that section 2702 of the Act draws no distinction between public and restricted communications, and that no statutory exception to the prohibition on disclosure could plausibly apply here. In particular, we questioned whether the exception set out in section 2702(b)(3), under which a provider may divulge a communication with the "lawful consent" of the originator, might reasonably be in-

terpreted to permit a provider to disclose posted communications that had been configured by the user to be public.

Accordingly, we solicited supplemental briefing concerning the proper interpretation of section 2702. In that briefing, all parties now concede that communications configured by the social media user to be public fall within section 2702(b)(3)'s lawful consent exception to section 2702's prohibition, and, as a result, may be disclosed by a provider. As we will explain, this concession is well taken in light of the relevant statutory language and legislative history.

The parties differ, however, concerning the scope of the statutory lawful consent exception as applied in this setting. Defendants emphasize that even those social media communications configured by the user to be restricted to certain recipients can easily be shared widely by those recipients and become public. Accordingly, they argue that when any restricted communication is sent to a "large group" of friends or followers the communication should be *deemed* to be public and hence disclosable by the provider under the Act's lawful consent exception. On this point we reject defendants' broad view and instead agree with providers that restricted communications sent to numerous recipients cannot be deemed to be public — and do not fall within the lawful consent exception. Yet we disagree with providers' assertion that the Act affords them "discretion" to defy an otherwise proper criminal subpoena seeking public communications.

In light of these determinations we conclude that the Court of Appeal was correct to the extent it found

the subpoenas unenforceable under the Act with respect to communications addressed to specific persons, and other communications that were and have remained configured by the registered user to be restricted. But we conclude the court's determination was erroneous to the extent it held section 2702 also bars disclosure by providers of communications that were configured by the registered user to be public, and that remained so configured at the time the subpoenas were issued. As we construe section 2702(b)(3)'s lawful consent exception, a provider must disclose any such communication pursuant to a subpoena that is authorized under state law.

Ultimately, whether any given communication sought by the subpoenas in this case falls within the lawful consent exception of section 2702(b)(3), and must be disclosed by a provider pursuant to a subpoena, cannot be resolved on this record. Because the parties have not until recently focused on the need to consider the configuration of communications or accounts, along with related issues concerning the reconfiguration or deletion history of the communications at issue, the record before us is incomplete in these respects. Accordingly, resolution of whether any communication sought by the defense subpoenas falls within the statute's lawful consent exception must await development of an adequate record on remand.

We will direct the Court of Appeal to remand the matter to the trial court to permit the parties to appropriately further develop the record so that the trial court may reassess the propriety of the subpoenas under the Act in light of this court's legal conclusions.

I. FACTS AND LOWER COURT PROCEEDINGS

A. Grand Jury Proceedings and Indictment[2]

According to testimony before the grand jury, at midday on June 24, 2013, Jaquan Rice, Jr., was killed and his girlfriend, B.K., a minor, was seriously injured in a drive-by shooting at a bus stop in the Bayview district of San Francisco. Various surveillance videos showed a vehicle and someone firing a handgun from the rear window on the driver's side. A second person was depicted leaving the vehicle from the rear passenger- side door and firing a gun with a large attached magazine.

Witnesses identified defendant Derrick Hunter's 14-year-old brother, Quincy, as one of the shooters. During questioning in the early morning hours after the events, police homicide detectives told Quincy that they had "pulled all Instagram . . . [and] Facebook stuff," and were aware that he knew the shooting victim. Quincy related that the victim had "tagged" him on Instagram in a video featuring guns. The detectives responded that they had been "working all day" on the matter and had "seen those posts." Quincy ad-

---

[2] This and the following sections are based on the grand jury transcripts, of which we have taken judicial notice, as well as material in providers' appendix of exhibits — including pretrial moving papers and the transcripts of two sessions of a pretrial hearing.

mitted that he shot the victim six times — and asserted that the victim "would have done the same thing to us."[3]

Quincy stated that "Nina," his girlfriend's sister, had provided the car in which he, his brother, and one other male had driven. Within a few minutes of the shooting, police had stopped Nina, whose real name is Renesha Lee (hereafter sometimes Renesha), while driving the vehicle shown in the videos.

Renesha was codefendant Lee Sullivan's then girlfriend. She had rented the car used in the shooting and gave varying accounts of the events. According to her testimony before the grand jury, during the course of multiple interviews on the day and night of the killings, she initially "just made up names and stuff." Eventually she told the police that defendant Derrick Hunter and his younger brother Quincy were among those who had borrowed her car. Renesha did not mention defendant Sullivan's name until a few days later, when she "told them the truth about [Sullivan]," and that he had been involved along with the Hunter brothers.

Renesha related that on the day of the shooting she had driven with Sullivan and the Hunter brothers

---

[3] Ultimately Quincy was tried in juvenile court, found to be responsible for Rice's murder and the attempted murder of B.K., declared a ward of the court, and committed to the Department of Juvenile Justice for a term of 83 years four months to life. Under Welfare and Institutions Code section 607, subdivision (b), however, because of his age at the time of the crimes, he will not be confined beyond his 25th birthday. After the Court of Appeal affirmed in an unpublished opinion (A142771), we granted review (S238077) and held that matter pending disposition of the present litigation.

to a parking lot where they "got out and walked to Quincy['s] house." She explained that Sullivan told her the three young men were going to a store. Renesha recalled that she replied she would remain at the house and talk to her sister. She testified that Sullivan had not been wearing gloves when he and the others initially approached her to borrow the car, but she noticed that he was wearing gloves when they came out of Quincy's house and when they departed. According to Renesha, Sullivan drove away with the Hunter brothers in the backseat. She testified that when the three returned the car to her shortly thereafter it contained the phones of Sullivan and Derrick Hunter. She also testified that she had never seen Sullivan or either of the Hunter brothers with a gun.

Renesha explained that she had initially not revealed Sullivan's involvement because she had been scared and "just didn't want to have no parts of it because I'm the one that still has to live and walk these streets." She elaborated that once the police informed her that she might be arrested for murder, she "told them the truth," and yet still avoided implicating Sullivan until later in the process because she remained fearful of him. She maintained that after being threatened with prosecution she eventually told the full truth about Sullivan's role.

In presenting the case to the grand jury, the prosecution contended that defendants and Quincy were members of Big Block, a criminal street gang, and that Rice was killed for two reasons: (1) Rice was a member of West Mob, a rival gang, and (2) Rice had publicly threatened defendant Derrick Hunter's younger brother Quincy on social media. Inspector Leonard

Broberg, a gang expert and member of the San Francisco Police Department Gang Task Force, testified that in his opinion the alleged crimes were committed for the benefit of the Big Block gang. He explained that "gangsters are now in the 21st century, and they've taken on a new aspect of being gangbangers, and they do something they call cyber banging. [¶] They will actually be gangsters on the internet. They will issue challenges; they will show signs of disrespect, whether it's via images or whether it's via the written word. . . . [¶] [They use] Facebook, . . . Instagram, Socialcam, Vine . . . [and] YouTube. . . . They will disrespect each other in cyberspace." Inspector Broberg described a YouTube video made by victim Rice and shared by him via his Facebook account, in which he gave a tour of his West Point/ Middle Point neighborhood and identified specific places where he could be located — including the bus stop where he was shot. Broberg characterized the video as a challenge to others. In a subsequent declaration, Broberg explained that he "rel[ies] heavily on records from social media providers such as Facebook, Instagram, and Twitter to investigate and prosecute alleged gang members for gang crimes," and that in the present case, he "relied in part on" such records to secure evidence that Rice, Sullivan, and the Hunter brothers "were members of rival gangs and that the shootings were gang related." The same declaration adds: "We [the police] have not sought search warrants as to Renesha Lee."[4]

---

[4] Toward the end of the proceedings, the prosecutor read to the grand jury some "exculpatory evidence . . . that was requested by

Defendants were indicted and are presently charged with the murder of Rice and the attempted murder of B.K. They also face various gang and firearm enhancements. (Pen. Code, §§ 187, 664, 186.22, subd. (b)(1), 12022, subd. (a), 12022.53, subds. (d) & (e)(1).)

B. Description of the Subpoenas

Prior to trial, in late 2014, both defendants served subpoenas duces tecum (Pen. Code, § 1326, subd. (b)) on Twitter. Defendant Sullivan's subpoena sought "[a]ny and all public and private content" that had been "published by" Renesha Lee, who was identified by an attached photocopied screen shot of one of her Twitter accounts. The request specified no temporal boundary and stated that it "includes but is not limited to" (1) so-called record data, consisting of "user information [and] associated e-mail addresses," "activity logs," and "location data"; and (2) content information, such as "photographs, videos, private messages, . . . posts, status updates, . . . , and comments including information deleted by the account holder." It further sought the identity and contact information concerning the custodian of records who could authenticate the requested materials. Defendant Hunter's subpoena, issued a few weeks later, sought all "accounts" and tweets originating from Renesha Lee's "account and in response to or linking her account" from the beginning of 2013 "to the present." Neither

---

the defense attorneys in this case be presented to you." The panel was told that two witnesses reported to police that a young woman had been driving the car, and that one witness had identified the driver as Renesha Lee. Yet another witness identified the driver as Quincy Hunter.

defendant sought from Twitter any communication concerning victim Rice.

Only defendant Sullivan served subpoenas on Facebook and Instagram. The Facebook subpoena requested information regarding the accounts of both Rice and Renesha Lee. The language of the subpoena tracked Sullivan's request to Twitter, broadly seeking "[a]ny and all public and private content," including deleted material, that had been "published by" either Rice or Renesha Lee, each of whom was identified by an attached photocopied screen shot of that person's Facebook account. As with Sullivan's subpoena served on Twitter, the subpoena specified no temporal boundary and sought the same record data, content, and authentication information mentioned above.

Sullivan's subpoena served on Instagram similarly sought "[a]ny and all public and private content," including deleted material, published by Rice and Renesha Lee, each of whom was again identified by photocopied screen shots showing their account information.[5] In all relevant respects the demands for record, content, and authentication information tracked

---

[5] It appears from the record that there may have been up to four relevant Instagram accounts, at least one for Renesha Lee and possibly three for Rice. A photocopied screenshot attached as an exhibit to the subpoena pertaining to Renesha Lee indicated the account had four posts, one follower, and eight accounts that the account holder was following. It also shows an image of a padlock, with a notation, "this user is private." According to subsequent pretrial briefing by defendants, "Mr. Rice had multiple social media accounts" and "many . . . have been deleted, including accounts gang expert Leonard Broberg relied upon at the grand jury hearing." Moreover, according to that same subsequent briefing, defendants also asserted that "many of [Renesha Lee's social media] accounts have been deleted."

the demands directed to the other social media providers.

C. Providers' Responses to the Subpoenas

Counsel for Facebook and its subsidiary Instagram responded to the Sullivan subpoenas by a single letter in December 2014, asserting that as providers governed by federal statute (the SCA), they are precluded under that law from divulging the requested stored communications. The letter stated that under the SCA only the government may compel covered providers to divulge such stored content. Accordingly, the letter recommended that defense counsel instead seek the requested information directly from the account holder or from "any party to the communication" — persons who, unlike a covered provider, are "not bound by the SCA." Alternatively, the letter suggested that defense counsel might "work[] with the prosecutor to obtain" the requested information via an additional search warrant issued by the government.[6] A few days later, different counsel in the same law

---

[6] Finally, the letter explained that if defense counsel were to withdraw each subpoena "to the extent it seeks content," Facebook and Instagram might produce "non-content information" regarding the specified accounts, "such as basic subscriber information and [internet protocol] logs" — information that defense counsel might use to contact other parties to the communications, in order to attempt to obtain the information directly from them. ("Basic subscriber information" (more fully described *post*, fn. 23) and internet protocol logs are forms of record/non-content data that, as implied in the letter, might be employed to identify a recipient of a communication in order to attempt to obtain electronic communications directly from that person.)

firm responded similarly on behalf of Twitter to defendant Sullivan.

Eventually all three providers moved to quash the subpoenas. They reiterated the assertions in their letters that defendants might try to obtain the requested information directly from the social media user who posted the communication, or from any recipient[7] — or perhaps via an additional search warrant issued by the prosecution.[8] They also objected that the requests

---

[7] In this regard, providers relied on decisions such as *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1447 (*O'Grady*) [even when the Act precludes disclosure by a provider, it "does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the [SCA-regulated service provider] bailee" who is barred from disclosure]. (See generally Fairfield & Luna, *Digital Innocence* (2014) 99 Cornell L.Rev. 981, 1058 [suggesting that a "defendant could locate the relevant originator or recipient by accessing non-content identifying information, such as an IP address, and then seek production [from that person] directly"].)

[8] Of course defendants are independently entitled to general criminal discovery, including exculpatory evidence, from the prosecution under Penal Code section 1054.1. Moreover, under authority such as *Brady v. Maryland* (1963) 373 U.S. 83, *People v. Salazar* (2005) 35 Cal.4th 1031, 1042-1043 (and cases cited), and *Barnett v. Superior Court* (2010) 50 Cal.4th 890, 900-901, the prosecution is obligated to share with the defense *any* material exculpatory evidence in its possession — including that which is potentially exculpatory. (See also Rules of Prof. Conduct, Rule 5-110(D), amended Nov. 2, 2017 [requiring "timely disclosure to the defense of all evidence or information known to the prosecutor that the prosecutor knows or reasonably should know tends to negate the guilt of the accused, mitigate the offense, or mitigate the sentence"] and corresponding discussion [observing that "the disclosure obligations in paragraph (D) are not limited to evidence or information that is material as defined by *Brady v.*

as drafted were overbroad and vague. In any event, providers asserted, disclosure *directly from them*, as entities covered by the SCA, was barred by that federal law. In that respect providers' motions relied upon section 2702(a), which broadly states that a covered "person or entity" such as providers "shall not knowingly *divulge to any person or entity the contents of a communication while in electronic storage by that service*." (Italics added.) Based on this language, providers asserted that the SCA's prohibition on a provider entity's ability to disclose any content information applies broadly and does not depend on whether the registered user configured a given communication as private/restricted as opposed to public. Moreover, providers asserted, none of section 2702(b)'s exceptions to the bar on disclosure by a provider applies here. Nor, they observed, does the Act contemplate procedures for criminal defendants to compel production of such communications.

Maryland . . . and its progeny. For example, these obligations include, at a minimum, the duty to disclose impeachment evidence or information that a prosecutor knows or reasonably should know casts significant doubt on the accuracy or admissibility of witness testimony on which the prosecution intends to rely."].) As explained below, consistent with its discovery obligations under state and federal law, the prosecution has apparently shared with defendants information relating to victim Rice's social media accounts. (See *post*, fn. 10.)

D. Defendants' Opposition to the Motions to Quash

Defendants opposed the motions to quash,[9] but they did not contest providers' assertion that section 2702(a) prohibits providers from disclosing any of the sought communications — even those configured by the registered user to be public. Nor did defendants challenge providers' assertion that none of section 2702(b)'s exceptions apply in this case. Instead, defendants argued that their federal constitutional rights under the Fifth and Sixth Amendments to a fair trial, to present a complete defense, and to cross- examine witnesses support their subpoenas and render the SCA unconstitutional to the extent it purports to afford providers a basis to refuse to comply with their subpoenas. Defendants acknowledged that no court had ever so held, and asked the trial court to be the first in the nation to do so.

Defendants presented offers of proof concerning the information sought from the various accounts. The prosecution had secured from Facebook and Instagram some of the available social media communications attributed to Rice and, as obligated, had shared that information with defendants in the course

---

[9] As the Court of Appeal observed below: "[T]he record before us [makes it unclear whether defendant] Hunter joined in the opposition to the motions to quash below, but he has formally joined in Sullivan's arguments in this court. For simplicity's sake, we refer to the opposition below as that of [d]efendants collectively." We adopt the same approach.

of discovery.[10] Regarding the information concerning Rice's communications, defendants asserted that review of the full range of content from those various accounts is required in order to "locate exculpatory evidence" and to confront and cross-examine Inspector Broberg, in order to challenge his assertion that the shooting was gang related. In support defendants cited Broberg's grand jury testimony and attached examples of five Facebook screen shots reflecting videos alleged to have been posted by Rice. Counsel asserted that the subpoenaed records would show that Rice was "a violent criminal who routinely posted rap videos and other posts threatening Quincy Hunter and other individuals."

Although the prosecution had secured and shared *some* of Rice's Facebook communications and a portion of the Instagram posts attributed to him, the prosecution had not sought from providers the social media communications of their key witness, Renesha Lee. Nevertheless, it appears from the record that at least one of Renesha Lee's Twitter accounts was public and contained numerous tweets that were accessible to defense counsel. Counsel evidently accessed that ac-

---

[10] (See *ante*, fn. 8.) Defendants subsequently asserted, however, that although they have had "access to some of Mr. Rice's social media records through the discovery process that tend to support the prosecution's theory of the case," still they lacked "access to records necessary to present a complete defense and to ensure the right to effective assistance of counsel." Thereafter, in their joint reply brief filed in this court, defendants characterized the prosecution as having declined to obtain all of Rice's various Instagram accounts.

count and identified content that, they asserted, indicated a strong likelihood that other similar, yet undiscovered — and possibly deleted — communications might exist. Defendants alleged that the prosecution's case turns on Renesha Lee's credibility and that "she is the only witness who implicates Sullivan in the killing." [11] Moreover, defendants explained, they sought additional corroborating information, consistent with that found already in Renesha Lee's public tweets, to demonstrate that she was motivated by jealous rage over Sullivan's involvement with other women and that she had repeatedly threatened others with violence.

In support of these assertions defendants' opposition appended, as an exhibit, photocopied screen shots of what was represented as two of Renesha Lee's Twitter accounts. They quoted a September 2013 tweet showing a photograph of a hand holding a gun and making specific threats: "I got da. 30 wit dat extend clip….. BIIIITCH I WILL COME 2YA FRONT DOOR….." Various other tweets from both accounts suggested a similar theme. Defendants asserted their need for and intention to use these and any other similar tweets, posts, comments, or messages, including deleted content, made by Renesha Lee on Twitter, Facebook, or Instagram, in order to impeach her anticipated testimony at trial. Defense counsel stated that,

---

[11] Quincy, in his earlier confession, acknowledged that his brother Derrick was with him in the car when the shooting occurred, but he did not mention Sullivan as being in the car with them. Instead, he asserted that a third person, named Johnson, had been with him and his older brother in the car.

despite diligent efforts, Renesha Lee could not be located to be served with a subpoena duces tecum.

E. The Hearing on the Motions to Quash

The first session of the bifurcated hearing on the motions to quash was held in early January 2015. The trial court began by explaining that, in light of the pleadings, it was inclined to find the sought material "critical" to the defense against the pending charges, and to conclude that "defendants have a [constitutional] right to . . . information that's authentic . . . [and] reliable." The court questioned providers' alternative proposal that the prosecution could or should issue additional search warrants to them (the service providers) on behalf of defendants: "First, I think the District Attorney's office is going to . . . say[], . . . our job is not to perform your investigation for you. And, besides, the Penal Code . . . authorizes search warrants to be obtained [only] under certain circumstances, and . . . not to find evidence that might support an affirmative defense or mitigate a mental state [or impeach a witness]." The court also expressed concern about defendants' ability to obtain any tweets or posts that may have been deleted by the account holder, and regarding how those communications might be authenticated sufficiently to be allowed into evidence. In that respect, the court questioned whether Renesha Lee would be willing to "take ownership" of tweets attributed to her and quoted above, "[s]ome [of which] could be subjecting her to criminal liability."

The trial court next addressed Twitter's assertion that any "deleted contents" would "not [be] reasonably available" and hence providers would "not . . . be able

to produce deleted contents or authenticate deleted content." The court expressed skepticism concerning Twitter's assertion that it would be unable to produce deleted content, observing: "[W]hat I . . . know from my time in discovery [is] that when I delete e-mails, they are not all deleted. [¶] Now, I don't know . . . to what extent they are kept on some server or archive that could be retrieved through some sort of search function, or whether some forensic computer person has a way of reconstructing files or not. [¶] So . . . if you are going to say that you complied and . . . state under penalty of perjury [supported by a] showing . . . that you have done what you can do, that's a separate thing. But, I doubt very much I am going to change my position that this material is critical, it has to be produced, and you are the ones holding it." Accordingly, the court tentatively denied the motions to quash and ordered that the materials be provided to it for in camera review pursuant to Penal Code section 1326. At the same time, the trial court allowed additional briefing to be filed before it ruled finally on the matter.

In its subsequent brief Twitter reiterated its assertion that section 2702 of the SCA fails to "distinguish between 'private' and 'public' content for purposes of its restrictions on providers' disclosure" and it maintained that "service providers are prohibited from producing *any* content, regardless of status." Facebook and Instagram asserted in their own subsequent brief that section 2702 of the SCA bars the requested discovery and that the Act "contains no exception for criminal defense subpoenas." Consistent with their broad assertion that no exception applied under section 2702, they did not address whether any of the

sought communications had been configured by the account holder to be public or private/restricted. Twitter, by contrast, directly confronted that issue in its own final supplemental responsive brief, noting that one of the accounts in question is public, and that "[a]s of this filing, anyone can visit the account and review its content, including messages, photos, and videos. In fact, defendant has already done this and included some public content from the account in . . . support of his Opposition [brief]."[12]

In response, defendants contested the assertions by Facebook and Instagram that defendants could gain access to the sought communications by other means.[13] They argued that unless providers are or-

---

[12] Twitter also stated: "On Twitter, if an account is public, its Tweets are public — a user cannot make individual Tweets public or private on a post-by-post basis." Further, Twitter addressed the trial court's stated concerns regarding retrieval of deleted content. It asserted that even if the SCA permitted it to comply with the subpoenas' demands, still, any "content deleted by the user is not reasonably available to Twitter."

[13] Regarding Rice, defendants noted that because Facebook allows the default to be changed — and posts to be configured as public or private on a post-by-post basis — not all friends might have "content that Mr. Rice decided to withhold from a particular user." As observed *ante*, footnote 10, defendants conceded that they had access to some of Rice's social media records through the discovery process. But, they insisted, they nevertheless lacked access necessary to present a complete defense. Regarding Renesha Lee's social media records, defendants did not contest Twitter's assertions that one of her Twitter accounts was public and remained open and accessible to all as of the time of the trial court briefing and hearings. Still, defendants asserted, "many of [her other] accounts" (apparently referring especially to

dered to comply with the subpoenas, they will be deprived of the information they need and also will be hampered in their effort to "persuade a jury that the records in question originated from Ms. Lee's social media accounts."

After considering the additional briefing, in late January 2015 the trial court confirmed its earlier conclusions, commenting that it would be "untenable" to deny the requested material to defendants. The court further explored with the parties the issues of deleted communications and burdens that compliance would impose on providers. In that regard counsel for providers asserted that deleted *tweets* "don't persist in backup for all eternity" and to the extent some remained in storage, "they are going to be very cumbersome and burdensome to obtain." The court responded that it had insufficient information with which to weigh the benefit of production versus burdens, and noted that it could easily impose a temporal restriction on the information sought in order to render the request more reasonable and less burdensome. The court then asked counsel to address recovery of deleted content concerning "your other clients" — Facebook and Instagram. But that discussion never occurred, producing an evidentiary lacuna as to those providers. Thereafter, neither the parties nor the court addressed whether any of the sought tweets had been configured as public, or whether, for any time period, the user had protected the account and made tweets sent during that time accessible to followers only. Nor did the court or parties address the privacy

---

the Facebook and Instagram accounts mentioned earlier) "have been deleted," and hence they had no access to them, and yet providers did possess those "inactive and active accounts."

configurations of the remaining Facebook and Instagram communications sought by defendants.

F. The Trial Court's Ruling on the Motions to Quash

The trial court finalized its tentative rulings, denying all three motions to quash and ordering that providers submit all of the sought materials for its in camera review by a deadline in late February 2015.[14] The court stated that it understood providers might seek writ review challenging its oral production order, and recognized that the Court of Appeal might stay its production order.

After discussing the need for a preservation order (see *post*, fn. 47), the court vacated the trial date, which had been set for the next day. All parties agreed to reconvene in early March, after the trial court had an opportunity to conduct in camera review of the information that the providers had been ordered to produce, or alternatively at a later date pending resolution of the writ proceeding providers intended to file contesting the court's oral production order.

G. The Writ of Mandate Proceeding

Providers jointly filed a petition for a writ of mandate in the Court of Appeal contending that the trial court abused its discretion in denying the motions to quash. They asked the appellate court to "preserve the status quo" by issuing an immediate stay of the

---

[14] As the Court of Appeal observed, defendant Hunter apparently did not formally oppose Twitter's motion to quash his subpoena. Nevertheless, the trial court assumed such a motion and denied it on the same basis that it denied the motions to quash defendant Sullivan's subpoenas.

trial court's production order and planned in camera review. That court stayed the trial court's production order and issued an order to show cause asking why the relief sought in the petition should not be granted.

After full briefing and oral argument, the Court of Appeal filed an opinion concluding that the SCA barred enforcement of defendants' pretrial subpoenas and rejecting defendants' arguments that the Act violated their rights under the Fifth and Sixth Amendments to the federal Constitution. Reviewing the relevant case law with respect to the constitutional claims, the appellate court concluded: "The consistent and clear teaching of both United States Supreme Court and California Supreme Court jurisprudence is that a criminal defendant's right to *pretrial* discovery is limited, and lacks any solid constitutional foundation." (Italics in original.) The appellate court stressed, however, that its conclusion was confined to "*this stage of the proceedings*" and limited to the "pretrial context in which the trial court's order was made." (Italics in original.) It observed that defendants would remain free to seek "at trial the production of the materials sought here." The appellate court commented that the trial judge who would eventually conduct the trial "would be far better equipped" than the appellate court itself "to balance [defendants'] need for effective cross-examination and the policies the SCA is intended to serve," and suggested that the SCA might eventually need to be declared unconstitutional to the extent it precludes enforcement of such a *trial* subpoena issued by the trial court itself, or by defendants, with production to the court. With respect to the pretrial context, however, the appellate court

directed the trial court to vacate its order denying providers' motions to quash the pretrial subpoenas, and to grant the motions to quash.

II. PROPER INTERPRETATION OF THE STORED COMMUNICATIONS ACT

Because the parties agreed in the trial court that the SCA precluded providers from complying with defendants' subpoenas and the court accepted that proposition, the trial court proceeded on the assumption that providers' refusal to comply with the subpoenas raised only constitutional questions. It then decided the matter by resolving those constitutional issues in defendants' favor. As explained above, the Court of Appeal likewise viewed the case as raising only constitutional issues, and its decision in providers' favor was grounded on the appellate court's conclusion that defendants' constitutional claims were not viable in the pretrial context.

In their initial briefing in this court, the parties again proceeded on the assumption that the litigation raised only constitutional issues, and they debated the merits of defendants' constitutional contentions. Defendants reiterated the view that their federal constitutional right to due process under the Fifth Amendment, and their confrontation, compulsory process, and effective assistance of counsel rights under the Sixth Amendment, require that the Act be declared unconstitutional to the extent it precludes the enforcement of their subpoenas in this case. They candidly recognized that case authority supporting their position is sparse. Ultimately, they suggested that we should overrule or distinguish our own decisions (especially *People v. Hammon* (1997) 15 Cal.4th 1117 and

its progeny) in order to declare the SCA unconstitutional as applied and uphold their pretrial subpoenas. Providers, by contrast, asserted that no decision of any court supplies authority supporting defendants' entitlement to pretrial enforcement of their subpoenas. They argued that, to the extent defendants might later *at trial* be able to establish a due process right to the information they seek in order to secure a fair trial, their remedy at trial would not lie in a judicial declaration that the SCA is unconstitutional as applied to them. Instead, providers asserted, the trial court should at that time put the prosecution to a choice: (1) use its authority under the Act to acquire the sought materials on behalf of defendants and share them with defendants at trial, or (2) suffer consequences in the form of an adverse evidentiary ruling at trial, including potentially pivotal instructions to the jury, or outright dismissal of the prosecution's case.

As mentioned, our initial review of the SCA and the relevant legislative history of the pertinent provisions, as well as prior judicial decisions addressing related issues, led us to question the validity of the statutory interpretation of the SCA on which the case was litigated below. Specifically, we questioned whether the relevant statute, section 2702(a), which appears to bar providers from disclosing electronic communications configured by the user to be private or restricted, *also* bars providers from disclosing communications that had been configured by the user to be public. Accordingly, we requested supplemental briefing directed to that issue, identifying the portions of the legislative history that appeared most relevant.

As explicated *post*, part III.A., in the ensuing supplemental briefing all parties concede that section 2702(b)(3)'s lawful consent exception permits providers to disclose public communications. In order to understand the relevant provisions of the SCA and why we also conclude that the statute should be so construed, it is appropriate to review the Act's general history, the language of the relevant statutory provisions, the specific legislative history of those provisions, and prior relevant case law.

A. The SCA — History and General Background

Congress enacted the Electronic Communications Privacy Act in 1986. (ECPA; Pub.L. No. 99-508, 100 Stat. 1860.) Title I of that law, amending the prior "Wiretap Act," addresses the interception of wire, oral, and electronic communications. (§§ 2510- 2521.) Title II of the law, set out in chapter 121, is often referred to as the Stored Communications Act, or SCA. It addresses unauthorized access to, and voluntary and compelled disclosure of, such communications and related information. (§§ 2701-2712.)

Prior to the ECPA's enactment, the respective judiciary committees of the House of Representatives and the Senate prepared detailed reports concerning the legislation. Each explained that the main goal of the ECPA in general, and of the SCA in particular, was to update then existing law in light of dramatic technological changes so as to create a "fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." (H.R. Rep. No. 99-647, 2d Sess., p. 19 (hereafter House Report); see also Sen. Rep. No. 99-541, 2d Sess., p. 3 (hereafter

Senate Report) [speaking of protecting both "privacy interests in personal proprietary information" and "the Government's legitimate law enforcement needs"].)[15] Each report also highlighted a related objective: to avoid discouraging the use and development of new technologies.[16] These three themes — (1) protecting the privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies (with privacy protection being the primary focus) — were also repeatedly emphasized by the bill

---

[15] The House Report described privacy protection as "most important," and noted: "[I]f Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances." (House Report, *supra*, at p. 19, fns. omitted.) The Senate Committee expounded on this theme, observing that "computers are used extensively today for the storage and processing of information," and yet because electronic files are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection" absent new legislation. (Sen. Rep., *supra*, at p. 3; accord, House Rep., *supra*, at pp. 16-19.)

[16] In this latter regard, the House Report, noting the "legal uncertainty" that surrounded the government's legitimate access to such stored information, expressed concern that such conditions may expose law enforcement officers to liability, endanger the admissibility of evidence, encourage some to improperly access communications, and at the same time, "unnecessarily discourage potential customers [from] using such systems." (House Rep., *supra*, at p. 19.) Similarly, the Senate Report cited the same potential problems, and added that legal uncertainty might not only discourage use of "innovative communications systems" but also "may discourage American businesses from developing new innovative forms of telecommunications and computer technology." (Sen. Rep., *supra*, at p. 5.)

authors in their debate remarks.[17] As this history reveals, and as a leading commentator on the SCA has explained, Congress was concerned that "the significant privacy protections that apply to homes in the physical world may not apply to 'virtual homes' in cyberspace," and hence "tried to fill this possible gap with the SCA." (Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* (2004) 72 Geo. Wash. L.J. 1208, 1210.)[18]

---

[17] For example, Congressman Kastenmeier, the bill's primary author, stressed as a governing principle "that what is being protected is the sanctity and privacy of the communication." (132 Cong. Rec. 14879 (1986), at p. 14886.) Senator Leahy, the bill's sponsor in the upper house, repeatedly referred to the need to "update our law to provide a reasonable level of Federal privacy protection to these new forms of communications" in order to address inappropriate acquisition by "overzealous law enforcement agencies, industrial spies, and just plain snoops" of "personal or proprietary communications of others." (132 Cong. Rec. 14599 (1986), at p. 14600.) Cosponsor Senator Mathias described the legislation as "a bill that should enhance privacy protection, promote the development and proliferation of the new communications technologies, and respond to legitimate needs of law enforcement." (*Id*., at p. 14608.)

[18] Congress's conception of the internet more than 30 years ago was, of course, substantially different from the internet that exists today. "The World Wide Web had not been developed, and cloud computing services and online social networks would not exist for nearly a decade. Internet users in 1986 could essentially do three things: (1) download and send e-mail; (2) post messages to online bulletin boards; and (3) upload and store information that they could access on other computers. The definitions and prohibitions listed in the SCA align with these three functions as they existed in 1986. Because Congress has not updated the statute, courts have struggled to apply the SCA in light of the explo-

B. Key Provisions of the SCA

1. *Rules regarding unauthorized access to stored communications: Sections 2701 and 2511(2)(g)(i)*

Section 2701(a) provides that, subject to specified exceptions, "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and "thereby obtains" an "electronic communication while it is in electronic storage in such system" commits an offense punishable by a fine or imprisonment. At the same time, a separate provision contained in another part of the ECPA, section 2511(2)(g)(i), articulates a substantial limitation on section 2701's access prohibition: "It shall not be unlawful under . . . chapter 121 [that is, the SCA] . . . [¶] . . . to . . . 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."[19]

2. *Rules prohibiting disclosure by service providers and listing exceptions under which providers are permitted to disclose "communications" or "customer records": Section 2702*

---

sive growth of the World Wide Web." (Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act* (2011) 24 Harv.J.L. & Tech. 563, 566, fns. omitted (*Discovering Facebook*).)

[19] Section 2707 authorizes a civil action to enforce these and the following provisions of the SCA.

Section 2702 addresses disclosure by certain covered service providers — and by no other person or entity. (*Wesley College v. Pitts* (D.Del. 1997) 974 F.Supp. 375, 389.) Subsection (a)(1) declares that, subject to specified exceptions, "a person or entity providing an electronic communication service[20] to the public *shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service*." (Italics added.) Similarly, and again subject to the same exceptions, subsection (a)(2) declares that "a person or entity providing remote computing service[21] to the public *shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . .*" (Italics added.) Finally, subsection (a)(3) bars any service provider from knowingly divulging any non-content "record or other information pertaining to a subscriber or customer" to any governmental entity.

The next two subsections of section 2702 — (b) and (c) — list *exceptions to the general prohibition* on disclosure by a service provider set forth in subsection (a). Subsection (b) describes eight circumstances under which a provider "may divulge the contents of a communication." As relevant here, subparts (1)-(3) of subsection (b) permit disclosure: (1) "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient"; (2)

---

[20] An electronic communication service (ECS) is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (§ 2510(15).)

[21] The term "remote computing service" (RCS) is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." (§ 2711(2).)

pursuant to section 2703, which, as described below, permits a "governmental entity" to compel a covered provider to disclose stored communications by search warrant, subpoena or court order; and (3) "with the *lawful consent of the originator or an addressee or intended recipient* of such communication, or the subscriber in the case of [a] remote computing service" (italics added). As explained below, some of the communications sought under the subpoenas at issue here may fall within the lawful consent exception set forth in section 2702(b)(3).[22]

Finally, subsection (c) of section 2702 describes six circumstances under which a covered provider may divulge *non-content information* — that is, any "record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communications. . .)."[23] As relevant here, the last of these exceptions permits disclosure "to any person

---

[22] The five other exceptions listed in section 2702(b) include disclosure incidental to the provision of the intended service or protection of the rights or property of the service provider; matters related to child abuse; and disclosure to a law enforcement agency of inadvertently obtained information that appears to pertain to a crime.

[23] Such "non-content" records consist of logs maintained on a network server, as well as "basic subscriber information," including the following: "(A) name; [¶] (B) address; [¶] (C) local and long distance telephone connection records, or records of session times and durations; [¶] (D) length of service (including start date) and types of service utilized; [¶] (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and [¶] (F) means and source of payment for such service (including any credit card or bank account number)." (§ 2703(c)(2).)

other than a governmental entity" (§ 2702(c)(6)) — which includes defendants in this case.[24]

3. Rules governing compelled disclosure by a service provider to a governmental entity: Section 2703

As alluded to above, section 2703 governs compelled disclosure by covered providers to a "governmental entity." It sets forth the rules under which law enforcement entities may compel ECS and RCS providers to disclose private as well as public communications made by users and stored by covered service providers.[25]

C. House and Senate Reports Concerning the Relevant Provisions

The 1986 congressional reports took special note of then-existing electronic bulletin boards — early analogues to the social media platforms at issue here. In

---

[24] The five preceding listed exceptions include disclosures of non-content information (1) authorized under compulsion by a "governmental entity" under section 2703; (2) with the lawful consent of the customer or subscriber; (3) as necessary and incidental to the provision of the intended service or protection of the rights or property of the service provider; (4) self-initiated to a law enforcement agency under emergency conditions; or (5) related to child abuse. (§ 2702(c).)

[25] (§ 2703(a) & (b).) As alluded to *ante*, footnote 23, subsection (c) addresses compelled disclosure to a governmental entity of certain non-content information. Other subsections articulate the requirements of any court order compelling disclosure (§ 2703(d)), specify that there can be no cause of action against a provider who discloses information pursuant to this chapter (§ 2703(e)), and impose on providers a requirement to preserve evidence on request of a governmental entity "pending the issuance of a court order or other process" (§ 2703(f)(1)).

the course of these discussions, the respective judiciary committees focused on the configuration of posts as being private or public and indicated an understanding that section 2701, governing unauthorized *access* to communications, was intended to cover and protect only private and not public posts. Significantly, the reports indicated the same understanding regarding section 2702's ban on provider *disclosure* of electronic communications, as reflected in that section's lawful consent exception to the ban.

The extensive House Report, issued first, repeatedly focused on the public/private theme. It did so initially in a passage addressing section 2511(2) of the ECPA, which as noted above states in subsection (g)(i) that it "shall not be unlawful" under either the omnibus ECPA or its SCA subset to "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." The committee explained that under this provision, it would be "permissible to intercept electronic communications made through an electronic communication system that is *configured so that such electronic communication is readily accessible to the general public*" and that "[t]he *term 'configure' is intended to establish an objective standard of design configuration to begin determining whether a system receives privacy protection*." (House Rep., *supra*, at p. 41.) Later, when the report addressed the SCA's analogue to this access rule, it explained that section 2701 would not "hinder the development or use of 'electronic bulletin boards' or other comparable services. *The Committee believes that where communications are readily accessible to the general public, the sender*

has, for purposes of Section 2701(a), extended an 'authorization' to the public to access those communications. A person may reasonably conclude that a communication is readily accessible to the general public if the . . . means of access [is] widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. *To access a communication on such a system should not be a violation of the law*." (House Rep., *supra*, at p. 62, italics added.) On the other hand, the report noted, some electronic bulletin boards may provide, in addition to a public forum, private e-mail services — and it observed: "Section 2701 would apply differently to the different services. *Those . . . electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public*." (*Id*., at p. 63, italics added.) The subsequent Senate Report similarly focused on electronic bulletin boards and repeatedly echoed the same public/private distinction. (Sen. Rep., *supra*, at pp. 8-9, 35-36.)

The House Report next turned to the provision that we must construe here, section 2702, prohibiting *disclosure* by covered providers of communications contents. The committee revealed its understanding that the theme of distinguishing between public and private posts carried over from section 2701's access rule and applied as well to section 2702's bar on the divulging of communications by providers.

The report observed that although section 2702(a) articulates a general prohibition on disclosure by a provider, section 2702(b)(3), setting out one of eight

exceptions to that rule, permits such a provider to divulge contents "with the lawful consent of the originator or any addressee or intended recipient" of the communication. (House Rep., *supra*, at p. 66.) The committee explained that, in its view, *implied* lawful consent by a user — and hence permissible disclosure by service providers — would readily be found with regard to communications configured by the user to be accessible to the public. It stressed that consent as contemplated by section 2702(b)(3) "need not take the form of a formal written document of consent." (*Ibid*.) The report viewed consent to disclosure as being implied by a user's act of posting publicly, and/or by a user's acceptance of a provider's terms of service: "Consent may . . . 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*." (*Ibid*., italics added.) The report explained that "[a]nother 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*." (*Ibid*., italics added.) Moreover, the report continued, "*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*." (*Ibid*., italics added.)

In other words, the committee indicated its understanding that with regard to electronic communications configured by the user to be accessible to the public, a covered service provider would be free to divulge those communications under section 2702(b)(3)'s lawful consent exception. Nothing in the subsequent Senate Report took issue with this analysis. (Sen. Rep., *supra*, at pp. 36-38.)

D. Cases Construing the SCA in Light of the House and Senate Reports

Prior decisions have found that Facebook and Twitter qualify as either an ECS or RCS provider and hence are governed by section 2702 of the SCA.[26] All parties assume the same with respect to all three providers before us. We see no reason to question this threshold determination.

Only a few decisions have construed the relevant provisions of the SCA, and nearly all have concerned civil litigation. Most have focused on claims that a party had obtained unauthorized *access* to stored communications under section 2701, and hence are not directly applicable here. Two decisions have addressed the question we face in this criminal matter — whether section 2702 bars covered service providers

---

[26] See, e.g., *Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965, 987-990 (*Crispin*) [regarding Facebook posts and private messages]; *Ehling v. Monmouth-Ocean Hosp. Service Corp*. (D.N.J. 2013) 961 F.Supp.2d 659, 665-670 (*Ehling*) [implicitly concluding the same regarding Facebook posts].) A New York trial court has implicitly reached the same conclusion regarding Twitter tweets. (*People v. Harris* (N.Y.Crim.Ct. 2012) 949 N.Y.S.2d 590, 596.)

from *divulging social media communications* in response to a subpoena. For context — and because, as we will see, one of the key section 2702 disclosure cases subsequently relied on some of the section 2701 access cases — it is useful to briefly address the access cases before discussing the disclosure decisions.

1. "Unauthorized access" cases interpreting section 2701

Konop v. Hawaiian Airlines, Inc. (9th Cir. 2002) 302 F.3d 868 (*Konop*) concerned asserted unauthorized access to communications on a restricted and password-protected electronic bulletin board. The Ninth Circuit panel, citing some of the passages set out in the two judiciary committee reports noted above, concluded that this legislative history "suggests . . . Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards" and that Congress intended the configuration of communications would " 'establish an objective standard [for] determining . . . privacy protection.' " (*Id*., at pp. 875 & 879, fn. 8, quoting House Rep., *supra*, at p. 41.) Subsequently, *Snow v. Direct TV, Inc*. (11th Cir. 2006) 450 F.3d 1314, quoted and extended *Konop*'s observation. The Eleventh Circuit concluded that in light of section 2511(2)(g)(i) and some of the legislative history described earlier, Congress intended to confine the reach of section 2701's access bar to those stored electronic communications that were configured to be restricted and not readily accessible to the general public. (450 F.3d at pp. 1320-1321.)

More recently, in *Ehling, supra*, 961 F.Supp.2d 659, a federal district court addressed a party's asserted unauthorized access to a user's restricted Facebook posts. The court highlighted the House Report's understanding that the configuration of communications would determine whether any given post is "accessible to the public" (*id*., at p. 666), and it relied on section 2511(2)(g)(i) (permitting *access* to communications that are "readily accessible to the general public") as well as *Konop* and *Snow* in concluding that "the SCA covers: (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) *that are not public.*" (*Ehling, supra,* at p. 667, italics added.) The court found that Facebook "posts . . . configured to be private meet all four criteria." (*Ibid*.) In reaching this conclusion the court observed that decisions "interpreting the SCA confirm that information is protectable *as long as the communicator actively restricts the public from accessing the information*." (*Id*., at p. 668, italics added.)

The *Ehling* court elaborated: "The touchstone of the Electronic Communications Privacy Act is that it protects private information. The language of the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private." (*Ehling, supra,* 961 F.Supp.2d at p. 668.) It reasoned: "Facebook allows users to select privacy settings . . . . Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user. *The Court finds that, when users make their Facebook . . . posts inaccessible to the general public,* [*those*] *posts are 'configured to be private' for purposes of the SCA*. . . . [W]hen it comes to

privacy protection, the critical inquiry is whether Facebook users *took steps to limit access to the information* [in their posts]. Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has." (*Ibid*., italics added.)[27]

2. "Prohibited disclosure" cases interpreting section 2702

In addition to the civil decisions construing section 2701's *access* rules and recognizing a public/private distinction in that setting, a few civil cases have concerned section 2702's prohibition on disclosure, as applied to third party subpoenas designed to compel *providers* to *divulge* electronic communications by the providers' users.

a. O'Grady *and related cases regarding subpoenas to providers seeking e-mail communications*

The first group of decisions addresses requests for disclosure by e-mail providers of their users' e-mail communications. A leading example is *O'Grady, supra*, 139 Cal.App.4th 1423, in which a California appellate court held section 2702 prevented an e-mail service provider from complying with a subpoena issued on behalf of Apple Computer (Apple). Apple

---

[27] The court in *Ehling* observed that the plaintiff user had "approximately 300 Facebook friends" (961 F.Supp.2d at p. 662), and concluded that because she had configured her communications as limited to them, the posts were covered by section 2701. (*Ehling,* at p. 668.) Nonetheless, the court ultimately rejected the plaintiff's claim of unauthorized access, finding that because an authorized recipient/friend had voluntarily shared the plaintiff's restricted communications with others, section 2701's "authorized user" exception was applicable. (*Ehling,* at pp. 669-671.)

sought the e-mail communications of an online news magazine to discover the identities of those who leaked confidential information about an impending Apple product. In concluding that section 2702 prohibited disclosure by the provider of such private e-mails (*O'Grady,* at pp. 1440-1451), the court distinguished between public posts that were made available "to the world," and the "contents of private [e-mail] messages" at issue in that case. (*Id.,* at p. 1449, italics omitted.) The court noted that it would reach a different conclusion, and presumably find disclosure permissible, "if the discovery [could] be brought within one of the statutory exceptions — most obviously, a disclosure with the consent of a party to the communication" under the lawful consent exception of section 2702(b)(3). (*O'Grady,* at p. 1446; see also *id.*, at p. 1447.) Likewise, other courts have concluded that section 2702 bars e-mail service providers from divulging private e-mail communications in response to third party civil subpoenas when, as in *O'Grady*, no exception to the Act's prohibitions on disclosure is applicable. (See, e.g., *In re Subpoena Duces Tecum to AOL, LLC* (E.D.Va. 2008) 550 F.Supp.2d 606, 611 ["[a]greeing with the reasoning in *O'Grady*" and declining to enforce a subpoena seeking production of private e-mail communications absent an applicable exception to the prohibition on disclosure].)

b. Viacom *and* Crispin — *regarding subpoenas served on providers seeking social media communications*

Two additional section 2702 disclosure cases are more pertinent to our present inquiry because they concerned disclosure by service providers, not of private e-mail, but of *social media communications*. As

explained below, these decisions reflect an understanding that Congress intended section 2702 to prohibit disclosure by providers of only private or restricted, but not public, social media communications.

The first opinion, *Viacom Int'l Inc. v. YouTube Inc.* (S.D.N.Y. 2008) 253 F.R.D. 256, addressed efforts by copyright owners to compel a social media provider, YouTube, to divulge stored information regarding videos that users had configured as private or restricted. (*Id*., at p. 264.) The federal district court quoted the House Report's observation, noted *ante*, part II.C., that one who posts a communication with a reasonable basis for knowing that it will be available to the public should be considered to have implicitly consented to such disclosure under section 2702(b)(3). (253 F.R.D. at p. 265.) The court held, however, that YouTube was barred under section 2702(a) from disclosing "videos that [users] have designated as private and chosen to share only with specified recipients" — and that on the facts presented, section 2702(b)(3)'s lawful consent exception was inapplicable. (*Viacom*, at pp. 264-265.)

The second decision, *Crispin, supra,* 717 F.Supp.2d 965, also concerned disclosure by a social media service provider under section 2702 in response to a civil discovery subpoena. The plaintiff in *Crispin*, an artist, sued the defendants, clothing manufacturers, asserting they violated a license to use his art. The defendants in turn issued subpoenas to various service providers, including Facebook and social media provider MySpace. The subpoenas broadly sought all manner of communications, ranging from public to private, between the plaintiff and others. The plaintiff moved to quash the subpoenas on various grounds,

including that the providers were barred by section 2702 from making the disclosures. A magistrate concluded that the section did not apply, and declined to quash the subpoenas with respect to any of the communications.

On review, the district court, relying on the legislative history of the SCA and the decision in *Konop*, *supra*, 302 F.3d 868, discussed above, determined first that so-called "private messaging" communications, like the e-mails in *Konop*, were configured to be private and hence protected from disclosure by service providers under section 2702(a). (*Crispin, supra,* 717 F.Supp.2d at p. 987.) Turning to the other communications, Facebook posts and MySpace comments, the court analogized those communications to the technology that existed in 1986 — postings on a " 'computer bulletin board' " system. (*Id*., at p. 980.) The court concluded that "a completely public [bulletin board system] does not merit protection under the SCA" — and that " '[*o*]*nly electronic bulletin boards which are not readily accessible to the public are protected under the Act*.' " (*Id*., at p. 981, italics added.) In other words, the court determined that Facebook posts and MySpace comments configured by registered users to be public are not protected from disclosure under section 2702(a) of the Act. But, the court reasoned, those communications would not be subject to disclosure by a provider if the user, like users of older restricted-access electronic bulletin boards, had configured the post or comment to be accessible only by a restricted group. (*Crispin*, at p. 981.)

Accordingly, the court in *Crispin* determined that the dispositive question was whether the posts had

been configured by the user as being "sufficiently restricted that they are not readily available to the general public." (*Crispin, supra*, 717 F.Supp.2d at p. 991.) Further, the court found that any restrictive privacy configuration employed by the user should be honored, and would bar disclosure by a service provider under section 2702 of the SCA, even if the restricted group is comprised of *all* of a user's Facebook friends. (*Crispin*, at p. 990.)[28]

Applying these principles to the motion to quash the civil subpoenas before it, the *Crispin* court observed that the parties had provided an incomplete record regarding the nature of the various private message services and other posts and comments services offered by those social media entities. Accordingly, the court remanded the matter "so that [the magistrate] can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings and the extent of access allowed to his Facebook [posts] and MySpace comments." (*Crispin, supra*, 717 F.Supp.2d at p. 991.)

The gist of *Crispin*'s discussion and treatment was that communications configured by the user to be re-

---

[28] The *Crispin* court reasoned: "Although here a large number of [registered] users, i.e., all of plaintiff's Facebook friends, might access the storage and attendant retrieval/display mechanism, the number of users who can view the stored message has no legal significance. Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms, which may have thousands of employees who can access documents in storage, would be excluded from the statute." (*Crispin*, *supra*, 717 F.Supp.2d at p. 990.)

stricted in some manner fall within section 2702's prohibition on disclosure by providers and are not subject to a civil subpoena directed to those providers. On the other hand, the subpoenas would be enforceable to the extent they sought Facebook posts and MySpace comments that had been configured by the registered user to be publicly accessible.

In reaching these conclusions *Crispin* relied heavily on the SCA's *access* provisions and related case law — and it focused generally on section 2702's *disclosure* bar without also considering specifically the lawful consent exception set out in section 2702(b)(3). Accordingly, the decision can be read as concluding that if Congress intended to withhold liability under section 2701 concerning those who *access* public communications, Congress must also have intended not to protect those same public communications from *disclosure* by covered providers under section 2702. Under this view, which appears to have been endorsed by some commentators,[29] the Act simply would not cover

---

[29] See, e.g., *Discovering Facebook, supra,* 24 Harv.J.L. & Tech. at page 584 ["Under the SCA, information that is 'readily accessible to the general public' is not protected from disclosure"]; Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act* (2012) 17 Suffolk J. Trial & App. Adv. 296, 314, 319 ["case law has made clear that communications that are 'readily accessible' by the public are not protected by the SCA"; "where a user's privacy settings allow the general public to view such communications, it is clear that the SCA will not govern such 'readily accessible' communications"; and when comments can be "viewable by anyone with internet access" they "would not be protected by the SCA"]; see also Comment, *Balancing the Scales of Justice* (2011) 9 J. on Telecomm. & High Tech. L. 285, 296-297 [distinguishing Facebook's private "user-to-user

or protect communications that have been configured to be public. We do not endorse this reading of the Act, however. Instead, we conclude that, by virtue of section 2702(a), the Act generally and initially prohibits the disclosure of *all* (even public) communications — but that section 2702(b)(3)'s subsequent lawful consent exception allows providers to disclose communications configured by the user to be public. Thus, although we agree with the result in *Crispin*, we conclude that the decision in that case should have been grounded on the lawful consent exception to the general prohibition.

As observed *ante*, part II.C., the House Judiciary Committee discussed the public/private distinction articulated under section 2511(2)(g)(i) of the ECPA, and revealed that it viewed that same distinction as carrying over and applying under the related *access* provision of the SCA, section 2701. The House Report then proceeded to describe the *disclosure* provision, section 2702, in a manner showing that it considered the same public/private distinction to apply in that context as well *via the lawful consent exception* contained in section 2702(b)(3). We conclude that the *Crispin* decision properly focused on the user's configuration of communications, and it also reached the correct result — even though it did not explicitly rely,

---

messaging functions," which are similar to e-mail, and that "would be protected by the SCA," from posts and "publicly-viewable" content "that would not be covered under the SCA"].

as it should have, on the lawful consent exception and legislative history illuminating that exception.[30]

---

[30] We also briefly note a recent Tennessee intermediate appellate court decision, *State v. Johnson and Williams* (Tenn.Crim.App. 2017) 538 S.W.3d 32 (*Johnson*). That litigation, like the present case, arose pretrial in a criminal prosecution. A percipient witness told the police that various "social media communications" concerning the events had been sent and received by her, as well as the victim and other friends of the victim, and both defendants, before and after the alleged offenses occurred. (*Id*., at p. 38.) One of two defendants issued subpoenas to, among others, the relevant social media service providers, broadly seeking all such communications. The state — but not the providers — moved to quash the subpoenas. (*Id*., at pp. 44-48.) The trial court denied the state's motion as to the providers, finding that the state lacked standing to object on their behalf. (*Id.*, at pp. 47-49.) On review the appellate court agreed and then proceeded, in dictum, to address matters that might arise on remand.

The court described the evolution of the SCA, extensively quoted sections 2701, 2702 and 2703, and briefly discussed some of the cases cited above, including *Crispin.* (*Johnson, supra,* 539 S.W.3d at pp. 63-69.) The appellate court next focused solely on section 2703, which as noted earlier concerns a *governmental entity's* authority to compel disclosure from providers. (*Johnson*, at pp. 69-70.) The court observed that the underlying defendants did not qualify as governmental entities — and from there jumped to the broad conclusion that the defendants "could not obtain" pursuant to their subpoenas "*any* information directly from the social media providers under the terms of the SCA." (*Id*., at p. 70, italics added.) In proceeding as it did, the *Johnson* court's dictum failed to consider the legislative history outlined above, the scope of section 2702's disclosure bar, or the lawful consent exception to that bar. As a result, the court failed to consider whether any of the sought social media communications had been configured by the users to be public, and thus were disclosable by the providers pursuant to the defense subpoenas.

E. Conclusion Regarding Section 2702(b)(3)'s Lawful Consent Exception

In light of the foregoing analysis, we conclude that communications configured by a social media user to be public fall within section 2702(b)(3)'s lawful consent exception, presumptively permitting disclosure by a provider.

III. APPLICATION TO THIS CASE

A. Overview: The Parties' General Agreement in Their Supplemental Briefs That Public Communications May Be Disclosed Under the Lawful Consent Exception; Limitation of Our Analysis to That Statutory Issue; and the Need for Remand to the Trial Court

As alluded to earlier, in supplemental briefs concerning section 2702 filed in response to questions posed by this court, both parties now agree that a social media communication configured by a registered user to be public falls within section 2702(b)(3)'s lawful consent exception.[31] In reaching this conclusion,

---

[31] In their supplemental brief, providers initially maintain that defendants' failure to challenge providers' proposed statutory interpretation in the lower courts precludes this court from addressing the propriety of that statutory interpretation at this juncture. We reject this contention. It is this court, not defendants, that has raised issues different from those argued below. When this court discovers a possible statutory interpretation question that may obviate the need to address a constitutional claim and solicits supplemental briefing on that issue, the statutory interpretation question is properly before us for resolution. (See Rules of Court, rule 8.516(b)(2) ["The court may decide an

providers retreat from their assertions that no exception to the prohibition applies with respect to any of the sought communications. Providers concede that, based on the legislative history described earlier, "[w]hen a user chooses to make a communication freely accessible to the public, he or she has necessarily consented to its disclosure." Accordingly, providers acknowledge that "as applied to communications that are available to the public, [section 2702(b)(3)'s] lawful consent exception allows a provider to disclose communications to any member of the public."

Nevertheless, both parties urge us to address not only the scope of the lawful consent exception, but also the constitutional issues originally framed and briefed. As alluded to in footnote 31, and as explained below, we find it proper at this point to address only the statutory issues, and not the constitutional claims.

As observed earlier, in the lower court proceedings the parties did not focus on the public/private configuration distinction. The trial court made no determination whether any communication sought by defendants was configured to be public (that is, with regard

---

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"].) Here we are guided by the familiar principle that we should address and resolve statutory issues prior to, and if possible, instead of, constitutional questions (see, e.g., *Santa Clara County Local Transportation Authority v. Guardino* (1995) 11 Cal.4th 220, 230-231, and cases cited), and that "we do not reach constitutional questions unless absolutely required to do so to dispose the matter before us." (*People v. Williams* (1976) 16 Cal.3d 663, 667, and cases cited.)

to the communications before us, one as to which the social media user placed no restriction on who might access it) or, if initially configured as public, was subsequently reconfigured as restricted or deleted. Nor is it clear that the trial court made a sufficient effort to require the parties to explore and create a full record concerning defendants' need for disclosure *from providers* — rather than from others who may have access to the communications. Consequently, at this point it is not apparent that the court had sufficient information by which to assess defendants' need for disclosure from providers when it denied the motions to quash and allowed discovery on a novel constitutional theory. In any event, because the record is undeveloped, we do not know whether any sought communication falls into either the public or restricted category — or if any initially public post was thereafter reconfigured as restricted or deleted.

In light of our interpretation of the Act, it is possible that the trial court on remand might find that providers are obligated to comply with the subpoenas at least in part. Accordingly, although we cannot know how significant any sought communication might be in relation to the defense, it is possible that any resulting disclosure may be sufficient to satisfy defendants' interest in obtaining adequate pretrial access to additional electronic communications that are needed for their defense. For these reasons, we will not reach or resolve defendants' constitutional claims at this juncture. Instead, we conclude that a remand to the trial court is appropriate.

In order to provide guidance to the trial court on remand, we discuss two issues regarding the statutory

question that have been raised by the parties in their supplemental briefs.

B. Defendants' Contention That Implied Consent to Disclosure by a Provider Is Established When a Communication Is Configured by the User to Be Accessible to a "Large Group" of Friends or Followers

The parties now generally agree that communications configured by a social media user to be public fall within section 2702(b)(3)'s lawful consent exception and presumptively may be disclosed by a provider. Beyond this point of agreement, the parties disagree starkly concerning the proper scope and interpretation of the implied consent exception.

Defendants advance an expansive interpretation of the exception. They argue that a user's implied consent to disclosure by providers under section 2702(b)(3) should be triggered not only by communications configured by the user to be public, but also by those configured by the user to be *restricted*, but nonetheless accessible to a "large group" of friends or followers. Defendants contend that, in practice, social media users "lose[] control over dissemination once the information is posted," and can have no reasonable expectation of privacy even with regard to such restricted communications in light of the fact that any authorized recipient can easily copy any communication and share it with others. (Cf. *Moreno v. Hanford Sentinel, Inc*. (2009) 172 Cal.App.4th 1125, 1229-1230 [social media user had no reasonable expectation that a communication configured as restricted would not be shared with others and hence could not maintain a

tort action for public disclosure of private facts].) Defendants observe that the internet, attendant technology, and social media itself did not exist when Congress considered and enacted the SCA. (See *ante*, fn. 18.) Therefore, they assert, section 2702 of the Act, generally prohibiting providers from disclosing stored communications, "should be deemed inapplicable" on the ground that "social media posts to large groups are essentially public posts in which the user has no reasonable expectation of privacy."

In support, defendants rely primarily on distinguishable decisions finding social media communications discoverable in civil litigation from a social media user, not, as here, from a social media provider. (E.g., *Fawcett v. Altieri* (N.Y.Sup.Ct. 2013) 960 N.Y.S.2d 593, 597 [private social media posts may be compelled from a user in civil discovery "just as material from a personal diary may be discoverable"].) They also rely on cases such as *U. S. v. Meregildo* (S.D.N.Y. 2012) 883 F.Supp.2d 523, 526 (*Meregildo*) [rejecting Fourth Amendment claim and holding that a criminal defendant who restricted Facebook communications to "friends" had no legitimate expectation that a friend would not share that information with the government].) But none of these cases involving the propriety of compelling disclosure by social media *users* concerned or construed section 2702's prohibition on disclosure by *providers*.

Defendants criticize decisions such as *Crispin, supra*, 717 F.Supp.2d 965, and *Ehling*, *supra*, 961 F.Supp.2d 659, for analogizing social media communications to what they characterize as "nearly obsolete" electronic bulletin boards. They insist that focusing on such allegedly outdated sites prevented those

courts from understanding that sharing is the essence of modern social media. Indeed, defendants and amici curiae on their behalf argue that, in the context of social media communications, there generally is no such thing as true privacy. Accordingly, they assert, even those social media communications configured by a user to be available to only specific friends or followers and that exhibit a "veneer of privacy" should nevertheless be treated as public. Defendants argue that such communications should not be protected by section 2702(a) — or that, alternatively, they should be deemed to fall within the lawful consent exception of section 2702(b)(3).

Providers and amicus curiae Google, LLC (Google), by contrast, assert that 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. They too rely on *Meregildo, supra,* 883 F.Supp.2d 523, 525, which observed that Facebook "postings using more secure privacy settings reflect the user's intent to preserve information as private." They also rely on *Ehling, supra*, 961 F.Supp.2d at page 668, which, as noted earlier, focused on whether a Facebook user "actively restrict[ed] the public from accessing information" and found that when a user configures a communication to be available on only a limited basis and "inaccessible to the general public," such a post is " 'configured to be private' for purposes of the SCA." Under this authority, providers assert, a service provider re-

mains prohibited from disclosing such communications. For reasons that follow, we agree with providers and Google on this point.

To begin with, we reject defendants' unsupported and rather startling assertion that social media communications and related technology fall categorically outside section 2702(a)'s general prohibition against disclosure by providers to "any person or entity."[32]

---

[32] For similar reasons we reject a somewhat related alternative interpretation of that quoted phrase advanced by amici curiae on behalf of defendants, the California Public Defenders' Association and the Public Defender of Ventura County. Asserting that the phrase "any person or entity" in section 2702(a) should be interpreted to exclude a court, amici curiae propose to interpret that phrase to permit providers to disclose any and all stored communications (no matter how configured) to a trial court for its in camera review — and then, presumably, for the trial court to release at least some of those private communications to defendants.

In support of their argument that a trial court does not qualify as a person or entity under the statute, amici curiae simply cite *Marbury v. Madison* (1803) 5 U.S. 137. They argue that Congress must be presumed to have been aware of "existing law" (including Penal Code section 1326's in camera review procedures) as well as the Fifth and Sixth Amendment rights of defendants — and hence, they postulate, Congress must have contemplated that such an exception for in camera and ex parte review by a trial court would be "read into the Act" by the courts, "when and if," as here, "the need arises." Amici curiae add that "Congress . . . knows that the courts are the forum where controversies such as the one here will be resolved and that the courts will determine their own procedures" — including amici curiae's contemplated compelled compliance with in camera review by the trial court. Finally, amici assert that to the extent the Act "is interpreted to prohibit [in camera] judicial assessment of the exculpatory significance of the subpoenaed records," the SCA, as applied

Nor can we accept defendants' interpretation of section 2702(b)(3)'s lawful consent exception, which would sweep far more broadly than was envisioned by Congress. The legislative history suggests that Congress intended to exclude from the scope of the lawful consent exception communications configured by the user to be accessible to only specified recipients. There is no indication in the legislative history of any intent to do otherwise in the case of communications sent by a user to a large number of recipients who, even in 1986 when the Act was adopted, could have shared such communications with others who were not intended by the original poster to be recipients.

In this respect, providers argue, defendants' view "would effectively eliminate expectations of privacy in *all* communications" and hence "would undermine the privacy rights of all users, including those of criminal suspects and defendants. If the SCA excluded electronic communications that are made to ['large'] groups of people, then it would necessarily place no restriction on private party or *law enforcement* access to such communications. And if people had no reasonable expectation of privacy in communications sent through and maintained by the intermediary, simply because those communications could be later shared by their recipients, that would remove all Fourth Amendment protections for communications as well."

---

in this case, violates defendants' Fifth and Sixth Amendment rights, and hence is unconstitutional. Putting aside the constitutional claim, neither the statutory language nor its legislative history supports amici curiae's claim that the statute can reasonably be interpreted to permit disclosure of all electronic communications, private or public, to a court under all circumstances.

(Italics in original.) Providers assert there is no indication that Congress contemplated such a result.[33]

As observed *ante*, part II.C., the House Judiciary Committee suggested, in its discussion of *access* rules, an understanding that a user's configuration would "establish an objective standard" to determine privacy protection. When subsequently addressing the *disclosure* rules — and the lawful consent exception to those rules — the House committee stressed that a user's consent to disclosure could be implied in view of, among other things, providers' available published policies. (House Rep., *supra*, at p. 66.) Providers' posted policies and answers to frequently asked questions (FAQs), described below, are readily available, and they appear to shed light on the issues presented in this litigation. Although we will highlight and quote some of these available policies and FAQs, we emphasize that in doing so we do not preclude any party from advancing any additional point or argument — including the legal significance that should or should not be accorded such policies and FAQs.

The policies and FAQs warn registered users that a communication configured as public will generally become, in the words of the House Report, *supra*, at page 62, "readily accessible to the general public," and available to *any* person via the internet, whether that

---

[33] Moreover, as amicus curiae Google notes, if defendants' "premise were correct, a communication shared with only one person would be equally public because a single recipient could share a private communication with the world (and some recipients do). . . . The ability to share an electronic communication accordingly cannot be the basis for removing privacy protections from content posted with less-than-public privacy settings."

person is registered with the social media provider, or not.[34] This widespread availability of public posts on the internet is the result of providers' business model, which allows and facilitates crawling and indexing by search engines (and in some instances, use of a so-called firehose stream) that generate search results lists displaying a link to the user's current social media page, a title and a snippet of text.[35] In other

---

[34] See, e.g., Twitter Privacy Policy, *Information Collection and Use / Tweets, Following, Lists, Profile, and other Public Information* <http://twitter.com/privacy> [as of May 22, 2018] [the service "broadly and instantly disseminates your public information to a wide range of users, customers, and services, including search engines"]; Facebook Help Center, *Appearing in Search Engine Results*

<https://www.facebook.com/help/392235220834308> [as of May 22, 2018]; Facebook Help Center, *What is Public Information?*

<https://www.facebook.com/help/203805466323736?helpref=faq_content> [as of May 22, 2018]; Instagram Help Center, *Controlling Your Visibility*

<https://help.instagram.com/116024195217477> [as of May 22, 2018]. All internet citations in this opinion are archived by year, docket number and case name at <http://www.courts.ca.gov/38324.htm>.

[35] See, e.g., Google Search, *How Search organizes information*

<https://www.google.com/insidesearch/howsearchworks/crawling-indexing.html> [as of May 22, 2018]; Google Search Console Help, *Create Good Titles and Snippets in Search Results* <https://support.google.com/webmasters/answer/35624?hl=en> [as of May 22, 2018]. Regarding Twitter's firehose stream, see, e.g., Financial Times Lexicon, *Definition of Twitter fire hose* <http://lexicon.ft.com/Term?term=Twitter-fire-hose> [as of May 22, 2018].

In addition, the three largest search engines — Google, Bing, and Yahoo! — also display in their results a link to a cached

words, when, for example, a Facebook user configures a post as public, that communication becomes both (a) available to all two billion registered Facebook users, and (b) again in the words of the House Report, "readily accessible to the general public" via crawling by search engines. The result is that, as counsel for providers conceded at oral argument, a public communication is available to "everyone in the world" — even to those who are not registered Facebook users, but who have open access to the internet.

Providers' FAQs warn that even communications configured as restricted still might be shared by an authorized recipient with anyone else.[36] At the same

---

version of the social media user's page. (See, e.g., Google, *Search Help/View webpages cached in Google Search Results/How to get a cached link* <https://support.google.com/websearch/answer/1687222?hl=en> [as of May 22, 2018].) Google explains that "[c]ached links show you what a webpage looked like the last time Google visited it" and that "Google takes a snapshot of each webpage as a backup in case the current page isn't available. . . . If you click on a link that says 'Cached,' you'll see the version of the site that Google stored. (*Ibid*.)

[36] Even with regard to communications that a user configures — either initially when sent, or subsequently as reconfigured — to be available to only a defined group (such as followers or friends), any such restriction operates only within the confines of the service and the licensing agreements under which other entities interact with the provider. Providers are generally careful to avoid describing the effect of privacy configuration more broadly. (See, e.g., Facebook Help Center, *When someone reshares something I posted, who can see it?* <https://www.facebook.com/help/569567333138410> [as of May 22, 2018] ["When someone clicks Share below your post, they aren't able to share your photos, videos or status updates *through Facebook* with *people who weren't in the audience you originally selected to share with*" (italics added, boldface omitted).])

Accordingly, when a user configures a post to be available to only specifically listed persons, the provider will be able to honor that user's choice only *within the service* — by disabling those recipients from, in turn, sharing that communication with others within the system through the system's sharing tools. Moreover, all three providers warn users that such configuration protection within each system does not prevent any authorized recipient from employing mechanisms outside the system to copy any post (by, for example, downloading or creating a screen shot) and then sharing the communication with anyone on the internet. (See, e.g., Twitter, *About public and protected Tweets / Who can see my Tweets?* <https://support.twitter.com/articles/14016> [as of May 22, 2018] ["Keep in mind that when you choose to share content on Twitter with others, this content may be downloaded or shared"].) Indeed, as Twitter advises, even when a user protects communications by restricting them to specific persons, that user's communications might nevertheless be shared by any such person with anyone else. (Twitter Help Center, *Twitter Privacy Policy / Information Collection and Use / Direct Messages and Non-Public Communications* <https://twitter.com/privacy?lang=en > [as of May 22, 2018] ["When you use features like Direct Messages to communicate privately, please remember that recipients may copy, store, and re-share the contents of your communications"]; see also Facebook, *Data Policy / How is this information shared? / Sharing our Services / People you share and communicate with* <https://www.facebook.com/policy.php> [as of May 22, 2018] ["people you share and communicate with may download or re-share this content with others on and off our Services"]; Instagram, *Privacy Policy / 3. Sharing of your information / Parties with whom you may choose to share your User Content* <https://help.instagram.com/155833707900388> [as of May 22, 2018] ["Once you have shared User Content or made it public, that User Content may be re-shared by others. . . . [¶] If you remove information that you posted to the Service, copies may remain viewable in cached and archived pages of the Service, or if other Users or third parties using the Instagram API [Application Programming Interface] have copied or saved that information."].)

time, 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.

For all of these reasons we reject defendants' proposed broad interpretation of the lawful consent exception. We hold that implied consent to disclosure by a provider is not established merely because a communication was configured by the user to be accessible to a "large group" of friends or followers.[37]

---

[37] At the same time, we do not endorse the view, expressed by counsel for providers at oral argument, that if it were *possible* for a registered Facebook user to restrict a communication to "only" all of the other *two billion* Facebook users, such a communication would not qualify as public under the Act. To our knowledge, no case has endorsed that view and on its face the claim seems rather questionable, particularly inasmuch as Facebook does not generally limit who may join its social media platform. In this regard, we note that what is public under the SCA is not defined by what a social media provider labels as "public."

Nor are we aware of any prior case involving a user who has placed minimal restrictions on a communication within a large social media service (as another hypothetical example, a user who might disseminate a communication to all two billion Facebook users except for one or two people). Although we hold that limiting a communication to a "large group" does not render a post public, and acknowledge that on remand the trial court might find that the public configurations at issue in this case render the resulting communications public under the SCA, we

C. Providers' Argument That Section 2702 Affords a Provider Discretion to Decline to Comply with a Valid State Subpoena

Providers contend that to the extent section 2702(b)(3)'s lawful consent exception applies to any of the communications at issue here, that provision simply *authorizes* them to comply with the subpoenas, but does not by itself *compel* them to comply with the subpoenas. They further assert that section 2702(b) affords providers who are authorized to disclose, the "discretion" to refuse to do so — even in the face of an otherwise proper subpoena lawfully issued under state law. We agree with the first proposition, but not with the second.

As observed earlier, section 2702(a) sets out a general prohibition against disclosure of communications by a service provider; and section 2702(b) lists exceptions under which a provider "may" disclose such communications — including, in subsection (3), communications regarding which a user has lawfully consented to disclosure. As the parties have conceded, such consent is applicable when a user posts a communication configured to be public. Plainly, section 2702(b) merely permits a provider to disclose, and it does not by itself impose a duty or obligation to disclose. Yet providers maintain that by use of the word "may," the section also operates to "ensure that providers would

---

also observe that neither the hypothetical discussed at oral argument nor this additional hypothetical involving minimal restrictions is presented in this case. Therefore, we need not and do not resolve whether such communications would be sufficiently public to imply consent to disclosure under section 2702(b)(3).

retain the discretion to choose whether to disclose content based on a user's consent" — even in the face of a lawful subpoena. In support, they rely on language in an order by a federal magistrate judge, *In re Facebook, Inc.* (N.D. Cal. 2012) 923 F.Supp.2d 1204, 1206, stating that although "consent may *permit* production by a provider, it may not *require* such a production." (Italics in original, boldface omitted.) Providers also rely on that order's footnote 7, which cited *United States v. Rodgers* (1983) 461 U.S. 677, 706 for the general proposition that "[t]he word 'may,' when used in a statute, usually implies some degree of discretion."

As explained below, a California Court of Appeal decision, *Negro v. Superior Court* (2014) 230 Cal.App.4th 879 (*Negro*), has thoroughly considered and rejected providers' argument. In that litigation, the plaintiff sued multiple defendants concerning business transactions. Prior to trial, the plaintiff subpoenaed defendant Negro's e-mail service provider, Google, seeking e-mail communications between him, his codefendants, and others. Defendant Negro eventually expressly consented to disclosure by Google of e-mails between himself and specific persons and entities covering a defined range of dates. But despite its user's express consent, Google refused to comply with the civil subpoena. On review, the Court of Appeal considered and applied section 2702(b)(3)'s lawful consent exception, ultimately finding that the defendant had given his express and enforceable written consent to service provider Google's disclosure of his e-mails. (*Negro,* at pp. 893-899.) Having found the lawful consent exception satisfied, the appellate court further concluded that the subpoena was itself enforceable and that Google was required to comply with

it. In the process, the court carefully considered and rejected the contention that providers raise now — that the statute empowers providers to defy subpoenas seeking communications that are exempted from section 2702's prohibition on disclosure under the section's lawful consent exception. (*Id*., at pp. 899- 904.) Because we find the *Negro* court's reasoning persuasive, we quote that decision's analysis at some length.

As an initial matter, the court in *Negro, supra,* 230 Cal.App.4th 879, rejected the claim that the SCA confers "a blanket exemption or immunity on service providers against compulsory civil discovery process." (*Id*., at p. 899.) The court acknowledged that the SCA does not, on its face, contain any exception for or mention of civil (or for that matter criminal) discovery subpoenas. But the court explained that the Act's failure to expressly include such subpoenas does not "suggest that it rendered" the normal state law "discovery process impotent in all circumstances." (*Ibid*.)[38]

Turning to the same argument reprised by providers here, the court in *Negro* addressed Google's assertion "that the language of the Act makes the consent

---

[38] The court continued: "Nor do we . . . perceive anything in the language of the Act suggesting that Congress intended to grant service providers a blanket immunity from obligations imposed by discovery laws. The Act does not declare civil subpoenas unenforceable; *it does not mention them at all*. As we have said, it *preempts* state discovery laws insofar as they would otherwise compel a service provider to *violate the Act.* It is this preemption that excuses service providers from complying with process seeking disclosures forbidden by the Act. But nothing in the Act suggests that service providers remain shielded from state discovery laws when the disclosures sought are *not* forbidden by the Act." (*Negro, supra,* 230 Cal.App.4th at p. 900, fn. omitted, first italics added, subsequent in original.)

exception 'permissive' and the provider's disclosure under it 'voluntary' . . . so that 'Google may not be compelled by an order issued in a civil proceeding to disclose content, even with the user's consent.' " (*Negro, supra,* 230 Cal.App.4th at p. 900.) The appellate court observed that Google relied on section 2702(b)'s "use of the word 'may' to frame the exception for disclosure based on a user's consent," and on the passage quoted above from the federal magistrate's order in *In re Facebook, Inc., supra,* 923 F.Supp.2d at page 1206. (*Negro,* at p. 900.) The court determined that the magistrate's reasoning "places much more weight on a very small word than it is designed to bear. It is certainly true that 'may' generally conveys permission, and that when used in contradistinction to 'shall' it implies a discretionary power or privilege, as distinguished from a mandatory duty. [Citations.]" (*Id*., at p. 901.) But, the court reasoned, "The subdivision where 'may' appears is framed not as a grant of discretionary power *or* as the imposition of a mandatory duty but as a special *exception* to a general *prohibition.* In such a context all 'may' means is that the actor is excused from the duty, liability, or disability otherwise imposed by the prohibition. Stating that the actor 'may' engage in the otherwise proscribed conduct is a natural way — indeed the most natural way — to express such an exception." (*Id.,* at p. 902, italics in original.)

The appellate court in *Negro* continued: "Another federal magistrate judge has observed that 'there should be a clear expression of congressional intent before relevant information essential to the fair resolution of a lawsuit will be deemed absolutely and categorically exempt from discovery and not subject to

the powers of the court under [rules governing disclosure]." [Citation.] Congress's use of the word 'may' to frame an exception to the Act's general prohibition on disclosure is not such a 'clear expression of . . . intent' as will justify a reading of the Act that categorically immunizes service providers against compulsory civil process where the disclosure sought is excepted on other grounds from the protections afforded by the Act." (*Negro, supra,* 230 Cal.App.4th at p. 902.)

Finally, the appellate court concluded: "In sum, we find no sound basis for the proposition that the Act empowers service providers to defy civil subpoenas seeking discovery of materials that are excepted from the Act's prohibitions on disclosure. Insofar as the Act permits a given disclosure, it permits a court to compel that disclosure under state law." (*Negro, supra,* 230 Cal.App.4th at p. 904.) Accordingly, the court held that in light of the fact that the user/defendant had consented to disclosure by the service provider, "the Act does not prevent enforcement of a subpoena seeking materials in conformity with the consent given." (*Ibid*.)

Providers do not directly address the logic or substance of the *Negro* court's analysis quoted above. Instead, they assert, first, that the appellate court's decision is distinguishable because the underlying lawful consent in that case was express, whereas the present case concerns implied consent. This attempt to avoid *Negro*'s analysis ignores the legislative history described *ante*, part II.C., disclosing that Congress specifically contemplated that *implied* lawful consent would satisfy the lawful consent exception. It also is in tension with providers' own concession that implied

lawful consent is effective with regard to communications configured by a registered user to be public. (See *ante*, pt. III.A.)

Alternatively, providers suggest that the SCA should be interpreted to bar the enforcement of any state subpoena that directs service providers to divulge public communications *that the Act permits but does not require them to disclose.* They assert that *Negro*'s contrary analysis and conclusion must be wrong because "it would permit a state subpoena to compel disclosure of content where the SCA itself does not. Such an expansion would weaken the protections of the SCA and impermissibly broaden federal law. It would thereby conflict with the SCA's comprehensive scheme of regulating the circumstances under which the disclosure of content is permissible or required."

In this respect providers implicitly rely on the fact that section 2703 lists circumstances in which a provider is compelled to disclose to governmental entities — and yet, as the *Negro* court observed, the Act, although preempting state discovery laws that would compel a provider to violate the federal statute, "does not mention" civil (or criminal) subpoenas issued by nongovernmental entities in that section or indeed at all. (*Negro, supra,* 230 Cal.App.4th at p. 900; see *ante*, fn. 38.) Consistently with *Negro*'s analysis, we believe that if Congress intended to preclude a state from enforcing a nongovernmental entity's civil or criminal subpoena that is lawful under state law (and as to which the federal statute does not preclude disclosure), such a prohibition would have been made clear

in the Act. We find no intent by Congress to preempt state law in this setting.[39]

D. Additional Issues Raised in the Supplemental Briefs, Some of Which Should Be Explored and Resolved on Remand to the Trial Court

Having addressed the legal issues that can be decided on the present record, we turn to other matters raised in providers' briefs that cannot be resolved at this stage — and some of which must await exploration on remand.

1. Providers' assertion that most of the communications at issue are private and hence the lawful consent exception will not assist defendants

As observed earlier, the subpoenas in this case broadly seek "any and all public and private content." Providers in their supplemental briefs assert variously that "much" or "most" (or all except a "small subset") of the communications sought by the subpoenas were configured by the users to be private or restricted, not public, and hence the lawful consent exception generally will not assist defendants in this case. Because the parties did not acknowledge the relevance and applicability of the lawful consent exception in the trial court, no reliable record was made concerning either registered user's configuration of

---

[39] To the extent dictum in *Johnson, supra,* 538 S.W.3d 32, is inconsistent (see *ante*, fn. 30), we disagree with its approach and analysis.

the social media communications at issue here.[40] Moreover, as noted earlier, it is not apparent that the

---

[40] At the time relevant in this case, it appears that each provider's default setting for registered users was public, meaning that unless the user configured communications to be private, they were public. (Regarding Twitter, see *Twitter Privacy Policy/Information Collection and Use/Tweets, Following, Lists, Profile, and other Public Information* <http://twitter.com/privacy> [as of May 22, 2018]; regarding Facebook, see Electronic Frontier Foundation, *Facebook's Eroding Privacy Policy: A Timeline* (Apr. 28, 2010) <https://www.eff.org/deeplinks/2010/04/facebook-timeline> [as of May 22, 2018] [observing that in November 2009, Facebook reset user privacy default settings to public]; see also Facebook Newsroom, *Making it Easier to Share With Who You Want* (May 22, 2014) <http://newsroom.fb.com/news/2014/05/making-it-easier-to-share-with-who-you-want/> [as of May 22, 2018] [noting that in mid-2014 — well after most of the communications at issue in this litigation were sent — Facebook again changed its privacy policy default, reverting, for new users, from public to friends, and giving existing users new tools to help ensure that they post publicly only when they intend to do so]; regarding Instagram, see Instagram Help Center*, Controlling Your Visibility/Setting Your Photos and Videos to Private* https://help.instagram.com/116024195217477> [as of May 22, 2018].)

From what we can glean from the record, it appears that Renesha Lee may not have changed the default on one of her Twitter accounts and made her tweets and/or any replies private. (See *ante*, pt. I.D. and related discussion.) The record does not address the configuration of Renesha Lee's Facebook communications. Finally, regarding Instagram, the record suggests that Renesha may have configured one Instagram account to be private. In addition, the record suggests that she may have had, and deleted, multiple additional accounts with some or all of the social media providers. The configurations of these additional accounts are unknown. (See *ante*, fn. 5.) Regarding victim Rice, the limited record suggests that he had accounts, perhaps multi-

trial court had sufficient information to fully assess defendants' need for discovery when it denied providers' motions to quash and allowed defendants discovery on a novel constitutional theory.

2. Providers' assertion that lawful consent to disclosure is revoked by a user's reconfiguration of a communication from public to restricted or by a user's deletion of a public communication

As noted, providers concede that they may, pursuant to the lawful consent exception set forth in 2702(b)(3), disclose a post configured by the user to be public. They maintain, however, that the fact a user may have *initially* configured a post for public distribution should not necessarily resolve the question of the applicability of the lawful consent exception. Specifically, providers observe that a communication originally configured to be public subsequently can be reconfigured by the user to be restricted, can be deleted by the user, or the user can close the account.[41] They

---

ple, and of unknown configuration, with Facebook and Instagram — and that some if not all of those accounts (including at least one relied upon by the prosecution's gang expert) have been closed. (*Ibid*.)

[41] In this regard Facebook tells users: "If you accidentally share a post with the wrong audience, you can always change it." (Facebook, *Privacy Basics / Manage Your Privacy* <https://www.facebook.com/about/basics/manage-your-privacy/posts#6> [as of May 22, 2018]; see also Facebook Help Center, *How can I adjust my privacy settings?* <https://www.facebook.com/help/193677450678703?helpref=related> [as of May 22, 2018] ["You can view and adjust your privacy settings at any time"].) Twitter allows an account to be changed from unprotected to protected and vice versa, and states: "If you at one time

argue that when such a change occurs before a provider is served with a subpoena, the reconfiguration or deletion should be understood as a revocation of lawful consent for purposes of section 2702(b)(3) — with the result that the provider would be prohibited by section 2702(a) from complying with a subpoena regarding any such communication.[42]

---

had public Tweets (before protecting your Tweets), those Tweets will no longer be public on Twitter, or appear in public Twitter search results [within the provider's system]. Instead, your Tweets will only be viewable and searchable on Twitter by you and your followers." (Twitter Help Center, *About public and protected Tweets / What happens when I change my Tweets from public to protected?* <https://support.twitter.com/articles/14016#> [as of May 22, 2018].) At the same time, Twitter explains, the opposite also occurs: "If you later change your account settings to no longer protect your Tweets, Tweets that were previously protected will become public and may be indexed by third-party search engines." (Twitter Help Center, *Why are my Tweets appearing on Google after deleting or protecting them? / Protected Tweets* <https://support.twitter.com/articles/15349#> [as of May 22, 2018].) Finally, Instagram also allows an account to be changed from the default (public) to private, and vice versa. (Instagram Help Center, *Privacy Settings & Information / Privacy settings / How do I set my photos and videos to private so that only approved followers can see them?* <https://help.instagram.com/196883487377501/?helpref=hc_fnav> [as of May 22, 2018].)

[42] Amicus curiae Google hypothesizes that any given communication originally configured as public, or any subsequent reverse reconfiguration of a communication from restricted to public, might conceivably be undertaken *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, Google argues, should be viewed as not constituting implied consent to disclosure by a provider. We agree, and observe that the trial court on remand will be in a

Defendants, by contrast, insist that once a registered social media user configures a communication as public and posts it, triggering section 2702(b)(3)'s lawful consent exception and presumptively allowing disclosure by a provider, the user cannot subsequently revoke that implied consent to disclosure, even if the user promptly reconfigures any post as restricted or deletes the post or closes the account. In support, defendants assert that "any reasonable user knows once you make information publicly available on social media it 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."[43] Defendants assert that after a public communication has been made so widely available, "[r]evoking consent is as possible as un-ringing a bell."

The parties have cited no decision explicitly addressing whether reconfiguration, deletion or account closure operates to revoke consent for purposes of section 2702(b)(3), nor have we found any such case. It appears that providers' revocation claim poses a question of first impression.

Providers may be understood to invoke Congress's intent to protect users' privacy (as described *ante*, pt. II.A.), and to suggest that their proposed interpretation — under which a provider would be required to

---

position to permit providers to attempt to establish, as a preliminary matter, that a given communication was configured, reconfigured, or deleted, by someone *other than* the registered account owner without authority of the owner.

[43] See *ante*, footnote 34.

honor a user's reconfiguration or deletion so long as it was undertaken by the time a subpoena is issued — would afford greater protection to that privacy interest. [44] Defendants, on the other hand, question whether a social media user's reconfiguration or deletion of a public post can in reality effectuate a revocation of consent to disclosure[45] — and whether Congress intended to ensure revocability of consent in this

---

[44] In support providers cite *Van Patten v. Vertical Fitness Group, LLC* (9th Cir. 2017) 847 F.3d 1037, 1047, which notes the "common law principle that consent is revocable." (Accord, *Neder v. United States* (1999) 527 U.S. 1, 21 [" ' "[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" ' "]; *Osorio v. State Farm Bank, F.S.B.* (11th Cir. 2014) 746 F.3d 1242, 1253 [quoting a dictionary for the proposition that " '[u]nder the common law understanding of consent, the basic premise of consent is that it is "given voluntarily," ' " and quoting the Rest.2d of Torts, § 892 for the proposition that " 'Consent is a willingness in fact for conduct to occur' " and that " ' "[C]onsent is terminated when the actor knows or has reason to know that the other is no longer willing for him to continue the particular conduct" ' "]; see also *State v. Brown* (Ore. 2010) 232 P.3d 962, 967 ["[A] person who places an item in plain view has relinquished any constitutionally protected privacy interest in the item. That person, however, may renew the privacy interest simply by removing the item from plain view."].)

[45] In this regard, providers warn users, the acts of reconfiguration or deletion (or even account closure) do not reach outside the provider's system and prevent third parties that may have indexed and cached any communication from continuing to make a given communication available in its prior form to anyone on the internet. For example, Facebook notes that in that situation it has no "control over content that has already been indexed and cached in search engines" and it offers the same advice as do Instagram and Twitter to their own registered users: in order to

context. Because the record does not indicate whether, in fact, any public communication sought by defendants was subsequently reconfigured or deleted before the relevant underlying subpoena was issued, we express no opinion on the revocation of consent issue — and leave it to be explored, if necessary, by the trial court on remand.

"request the immediate removal of [a particular] search listing, you will have to contact the specific search engine's support team." (Facebook Help Center, *Appearing in Search Engine Results/I'm showing up in the results of other search engines even though I've chosen not to* <https://www.facebook.com/help/392235220834308/?helpref=hc_fnav> [as of May 22, 2018].) And yet even if a user identifies each search engine that displays the communication and seeks expedited recognition of any reconfiguration or deletion, the providers indicate that the most that can be said is that any given search engine will "eventually index updated . . . information" to reflect any reconfiguration protection or post deletion. (Twitter Help Center, *Why are my Tweets appearing on Google after deleting or protecting them?/How and when to send Google a request to remove information* <https://support.twitter.com/articles/15349#> [as of May 22, 2018].) Indeed, Instagram observes that there is no such thing as immediate reconfiguration or deletion of a public communication that has become available on a search engine; instead, "[i]t may take some time for these [other third party search engine] sites and Google to re-index and remove" a given communication "even if you delete your account." (Instagram Help Center, *Controlling Your Visibility/Instagram Privacy on the Web/How can I remove my images from Google search* <https://help.instagram.com/116024195217477> [as of May 22, 2018].)

3. Technical difficulties that providers may face in determining the applicable privacy configuration and retrieving deleted communications — and protecting providers from excessive burdens

Providers assert that in light of a registered user's ability to reconfigure communications, "providers may not easily be able to determine the intended audience of a communication at any given point in time" and "it may be difficult for a provider to accurately identify" whether a given communication when posted was public or restricted. Likewise, speaking on providers' behalf, amicus curiae Google avers: "Providers do not routinely maintain records of past privacy settings for each post or message. Lacking such records, it would be *impossible* to determine the privacy configuration that applied when a communication was posted or sent." (Italics added.) Providers also assert that "if a user changes the privacy setting for a communication, a service may not be able to accurately determine prior privacy settings." In addition, providers assert it would be difficult for them to retrieve deleted communications. As noted by the trial court, however, a subpoena recipient has a general obligation to undertake reasonable efforts to locate responsive materials. Again, any technical difficulties a given provider may face in determining the relevant history of a particular communication, or retrieving any deleted communication, are matters to be explored at the anticipated hearing on remand.

Providers similarly urge that they should be protected from excessive burdens. As observed *ante*, part II.A., Congress articulated its main purposes in enacting the SCA: affording privacy protections to users

while accommodating the legitimate needs of law enforcement. It also articulated a tertiary goal: to avoid discouraging the use and development of new technologies. Providers' briefs characterize this additional purpose as one of "enhanc[ing] the use of communications services and protect[ing] providers from being embroiled as a nonparty in litigation." Amicus curiae on providers' behalf, Google, characterizes this additional purpose even more specifically as "protecting providers from an otherwise limitless burden of responding to requests to disclose their users' communications." Providers rely on dictum in *O'Grady, supra*, 139 Cal.App.4th 1423, in which the court voiced concern about the prospect of such subpoenas to providers in routine civil cases. (*Id.*, at pp. 1445-1447.)[46]

In light of the statutory scheme, it appears that Congress sought to limit burdens placed on service providers by various means — most obviously, by establishing broad prohibitions and specific exceptions regarding access and disclosure under sections 2701 and 2702, along with rules and procedures pursuant to which the government may compel disclosure under section 2703. With regard to burdens related to disclosure in particular, Congress significantly limited the potential onus on providers by establishing a

---

[46] In a related vein, providers observe that they stand in jeopardy of incurring civil liability under section 2707 of the Act if they knowingly or intentionally violate the SCA. But that section by its terms contemplates liability only for a provider that violates the Act "with a knowing or intentional state of mind." (*Id*., subd. (a).) Moreover, the statute provides a safe harbor for a provider who, in "good faith," relies on "a court . . . order." (*Id*., subd. (e)(1).)

scheme under which a provider is effectively prohibited from complying with a subpoena issued by a nongovernmental entity — *except* in specified circumstances. But when any one of the exceptions does apply, there is no indication that Congress intended that providers would be categorically relieved from the burden of compliance with an otherwise lawful civil or criminal subpoena. Hence, as the court held in *Negro*, *supra*, 230 Cal.App.4th 879, a provider may properly be subject to the burden of compliance with a subpoena, even with respect to communications configured by the registered user to be *private*, when a user expressly consents to disclosure by his or her service provider. Likewise, a provider may properly be subject to the burden of compliance with a subpoena when a user implicitly consents to disclosure by configuring a social media communication as *public*.

Of course, any third party or entity — including a social media provider — may defend against a criminal subpoena by establishing that, for example, the proponents can obtain the same information by other means, or that the burden on the third party is not justified under the circumstances. (*City of Alhambra v. Superior Court* (1988) 205 Cal.App.3d 1118, 1134; cf. *Kling v. Superior Court* (2010) 50 Cal.4th 1068, 1074-1075, 1078.) Indeed, the Act itself specifically contemplates that providers may raise such issues in the context of compelled disclosure to a governmental entity under section 2703(d) (a court "may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider"), and the same principles would apply in the present setting.

As noted, providers advanced similar arguments regarding the burden of compliance with the subpoenas in the earlier trial court proceeding. (*Ante*, part I.E.) In response, the trial court ruled that absent additional factual information demonstrating impossibility or the extent of burdens, it could not engage in any such balancing of production versus burden. Providers' current claim of undue burden can properly be addressed by the trial court on remand.[47]

---

[47] The trial court on remand might also consider two additional and somewhat related legal issues that have been only generally alluded to in the briefing to date in this case, but which are highlighted in our January 17, 2018 order granting review in the related matter of *Facebook, Inc., v. Superior Court* (*Touchstone*) (2017) 15 Cal.App.5th 729 (S245203). That order directs the parties to address, among other things (1) whether a trial court may compel a witness to consent to disclosure by a provider, subject to in camera review and any appropriate protective or limiting conditions; and (2) whether a trial court may compel the prosecution to issue a search warrant under the Act, on behalf of a defendant.

Finally, yet another matter, not discussed in the parties' briefs, may require consideration on remand. As alluded to *ante*, part I.F., after the trial court confirmed its production ruling, counsel for defendant Sullivan asked that providers be ordered to preserve all data at issue in this case. The court stated that it would not immediately issue an oral preservation order because it wanted the parties to first work out among themselves language addressing the providers' preservation obligations, and stated: "You will have to draft something and submit it, and see if you can reach an agreement. And if you get competing orders, we will have to have another hearing about that." The record before us, however, contains no preservation order; no mention of such an order appears in the briefs; and the superior court docket for each case, as to which we have taken judicial notice, reflects no such order. (See, e.g., *Williams v. Russ* (2008) 167

IV. CONCLUSION AND DISPOSITION

We vacate the Court of Appeal's decision and direct that court to remand the matter to the trial court for proceedings consistent with this opinion.

CANTIL-SAKAUYE, C. J.

WE CONCUR:

CHIN, J.
CORRIGAN, J.
LIU, J.
CUÉLLAR, J.
KRUGER, J.
YEGAN, J.[*]

Cal.App.4th 1215, 1223 [addressing a party's "failure to preserve evidence for another's use in pending or future litigation" and corresponding sanctions].)

[*] Associate Justice of the Court of Appeal, Second Appellate District, Division Six, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

Name of Opinion Facebook, Inc. v. Superior Court

Unpublished Opinion
Original Appeal
Original Proceeding
Review Granted XXX 240 Cal.App.4th 203
Rehearing Granted

Opinion No. S230051
Date Filed: May 24, 2018

Court: Superior
County: San Francisco
Judge: Bruce E. Chan

Counsel:

Perkins Coie, Christian Lee, James G. Snell, Eric D. Miller, John R. Tyler, Sunita Bali; Gibson, Dunn & Crutcher, Joshua S. Lipshutz and Michael J. Holecek for Petitioners.

Mayer Brown and Donald M. Falk for Google LLC as Amicus Curiae on behalf of Petitioners.

No appearance for Respondent.

Jose Pericles Umali for Real Party in Interest Derrick D. Hunter.

Susan B. Kaplan and Janelle E. Caywood for Real Party in Interest Lee Sullivan.

Jeff Adachi, Public Defender (San Francisco), Matt Gonzalez, Chief Attorney, and Dorothy Bischoff, Deputy Public Defender, as Amici Curiae on behalf of Respondent and Real Parties in Interest.

Stephen P. Lipson, Public Defender (Ventura) and Michael C. McMahon, Chief Deputy Public Defender, for California Public Defenders Association and Public Defender of Ventura County as Amici Curiae on behalf of Real Parties in Interest.

David M. Porter; Law Offices of Donald E. Landis, Jr., Donald E. Landis, Jr.; Law Offices of J.T. Philipsborn and John T. Philipsborn for California Attorneys for Criminal Justice and National Association of Criminal Defense Lawyers as Amici Curiae on behalf of Real Parties in Interest.

APPENDIX E

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

U.S. Const. amend. V.

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

U.S. Const. amend. VI.

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

18 U.S.C. § 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents

of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B)Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(6) to any person other than a governmental entity; or

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

18 U.S.C. § 2703. Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communica-

tions received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute

or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

(1) DEFINITIONS.—In this subsection—

(A) the term "qualifying foreign government" means a foreign government—

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) MOTIONS TO QUASH OR MODIFY.—(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to

quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) DISCLOSURE OBLIGATIONS DURING PENDENCY OF CHALLENGE.—A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT.—(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

18 U.S.C. § 2707. Civil action

(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the

court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3), section 2702(b)(9), or section 2702(c)(7) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) IMPROPER DISCLOSURE.—Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

APPENDIX F

Examples of cases in which criminal defense subpoenas were issued to Facebook or Instagram since 2017:

- *California v. Beverly*, No. XCNBA437706-01 (Cal. Super. Ct.—Los Angeles Cty.)
- *California v. Collins*, No. 13033957 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Cudjo*, No. XNVA746168-01 (Cal. Super. Ct.—Los Angeles Cty.)
- *California v. Flores*, No. CN374531 (Cal. Super. Ct.—San Diego Cty.)
- *California v. Gobbo*, No. 18CR-04433 (Cal. Super. Ct.—Santa Cruz Cty.)
- *California v. Hale*, No. 17005770 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Harris*, No. 17-CR-017349-A (Cal. Super. Ct.—Alameda Cty.)
- *California v. Harris*, No. 19012702 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Hayward*, No. SCR-695353 (Cal. Super. Ct.—Sonoma Cty.)
- *California v. Jackson*, No. 19014356 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Maldonado*, No. CR18-4729 (Cal. Super. Ct.—Yolo Cty.)

- *California v. Moreno-Silva*, No. SCR-702878 (Cal. Super. Ct.—Sonoma Cty.)
- *California v. Neal*, No. 17FE002616 (Cal. Super. Ct.—Sacramento Cty.)
- *California v. O'Neill*, No. SC083016 (Cal. Super. Ct.—San Mateo Cty.)
- *California v. Pablo*, No. 18-CR-006161 (Cal. Super. Ct.—Alameda Cty.)
- *California v. Pohlman-Minor*, No. J44044 (Cal. Super. Ct.—Solano Cty.)
- *California v. Robinson*, No. 16FE020033 (Cal. Super. Ct.—Sacramento Cty.)
- *California v. Rocha*, No. 18018907 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Shubov*, No. 4004178 (Cal. Super. Ct.—Stanislaus Cty.)
- *California v. Stone*, No. 1190175739 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Sullivan*, No. 221448 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Touchstone*, No. SCD268262 (Cal. Super. Ct.—San Diego Cty.)
- *California v. Warshaw*, No. 17004548 (Cal. Super. Ct.—San Francisco Cty.)
- *California v. Young*, No. 18012547 (Cal. Super. Ct.—San Francisco Cty.)
- *City of Shoreline v. Weaver*, No. 617025315 (Wash. Dist. Ct.—King Cty.)

- *Colorado v. Mannix*, No. 18CR3875 (Colo. Dist. Ct.—El Paso Cty.)
- *District of Columbia v. Smith*, No. 2018 CFI 009266 (D.C. Super. Ct.)
- *District of Columbia v. Williams*, No. 2018 DEL 217 (D.C. Super. Ct.)
- *District of Columbia v. Wint*, No. 2015 CF1 7047 (D.C. Super. Ct.)
- *Florida v. Kline*, No. 16-2018-cf-0174 (Fla. Cir. Ct.—4th Cir.)
- *Georgia v. Davis*, No. 19sm001970A (Cal. Super. Ct.—San Mateo)
- *Georgia v. Hall*, No. 18SC158617 (Ga. Super. Ct.—Fulton Cty.)
- *Georgia v. Johnson*, No. SUCR2019000160P (Ga. Super. Ct.—Bulloch Cty.)
- *Illinois v. Ontiveros*, No. 17CR16700 (Ill. Cir. Ct.—Cook Cty.)
- *Indiana v. Herron*, No. 49G05-1803-F1-009772 (Ind. Super. Ct.—Marion Cty.)
- *Louisiana v. Short*, No. 527-600 (La. Dist. Ct.—Orleans Parish)
- *Massachusetts v. Hurney*, No. 17-CR-1682 (Mass. Dist. Ct.—Somerville)
- *Massachusetts v. Martinez*, No. 1749-2203 (Mass. Dist. Ct.—Framingham)
- *Massachusetts v. Tavera*, No. 1617CR003451 (Mass. Dist. Ct.—Holyoke)

- *Massachusetts v. Tremblay*, No. 1833CR004085 (Mass. Dist. Ct.—New Bedford)
- *Missouri v. Carter*, No. 1416-CR00254-01 (Mo. Cir. Ct. – Jackson Cty.)
- *New Jersey v. Rodriguez*, No. FJ-02-708-17B (N.J. Super. Ct – Bergen Cty.)
- *Texas v. Fojtasek*, No. 154349601010-3 (Tex. Dist. Ct. – Travis Cty.)
- *United States v. Nix*, No. 14-CR-06181-EAW (W.D.N.Y.)
- *United States v. Pepe*, No. 2018 CF1 018581 (D.C. Super. Ct.)
- *United States v. Raynor*, Nos. 2018 CF2 16148, 2019 CF2 16148 (D.C. Super. Ct.)