No. S245203

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

FACEBOOK, INC.,
Petitioner,

v.

THE SUPERIOR COURT OF SAN DIEGO COUNTY,
Respondent;

LANCE TOUCHSTONE,
Real Party in Interest.

After Published Opinion by the Court of Appeal, Fourth Appellate District, Division One, No. D072171; Superior Court of San Diego County, No. SCD268262, Hon. Kenneth So, Presiding Judge

---

PETITIONER'S RULE 8.520(d) SUPPLEMENTAL BRIEF REGARDING *FACEBOOK, INC. V. WINT* (D.C. 2019) AND *FACEBOOK, INC. V. SUPERIOR COURT* ("*HUNTER III*") (2020)

PERKINS COIE LLP
JAMES G. SNELL, SBN 173070
jsnell@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304
tel: 650.838.4300, fax: 650.838.4350

GIBSON, DUNN & CRUTCHER LLP
*JOSHUA S. LIPSHUTZ, SBN 242557
jlipshutz@gibsondunn.com
555 Mission Street
San Francisco, CA 94105
tel: 415.393.8200, fax: 415.393.8306

MICHAEL HOLECEK, SBN 281034
mholecek@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071
tel: 213.229.7000, fax: 213.229.7520

Attorneys for Petitioner Facebook, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

Since briefing concluded in this appeal, two appellate courts have issued decisions that support Facebook's arguments. Both confirm that the Stored Communications Act ("SCA") precludes Defendant Lance Touchstone from subpoenaing social media records from Facebook without account holders' consent.

First, in *Facebook, Inc. v. Wint* (D.C. 2019) 199 A.3d 625, the D.C. Court of Appeals unanimously reversed an order requiring Facebook to produce records to a criminal defendant, holding that the defendant did not raise any "serious constitutional doubts" about the SCA. The court explained that the SCA furthers important privacy interests and rationally requires criminal defendants to direct their subpoenas to message senders and recipients—as Facebook argues here.

Further, *Wint* was briefed and decided during trial, where a criminal defendant's constitutional rights are at their zenith. This appeal, on the other hand, involves a *pretrial* subpoena, and this Court has repeatedly held that there is no general constitutional right to discovery, and certainly no constitutional right to pretrial discovery. In *Wint*, the United States submitted a brief supporting Facebook's arguments regarding the requirements of the SCA—an authoritative view of the federal executive branch that merits consideration by this Court as well.

Second, in *Facebook, Inc. v. Superior Court* (Feb. 13, 2020) 46 Cal.App.5th 109 ("*Hunter III*"), *certified for publication* Mar. 6, 2020, the California Court of Appeal held that trial courts must "adequately consider" whether a criminal defendant can obtain electronic communications through alternative means—such as from senders and

recipients—before even considering constitutional arguments to justify subpoenaing service providers like Facebook in violation of the SCA. (*Hunter III*, *supra*, at p. 118.) Similar to Touchstone, the defendants in *Hunter III* failed to show that it would be futile to subpoena message senders and recipients, and they improperly relied on speculation that a subpoena recipient would invoke the Fifth Amendment to avoid production.

This Court should affirm the decision below.

II. THE *WINT* AND *HUNTER III* DECISIONS

A. The *Wint* Decision

In *Wint*, defendant Daron Wint was charged with quadruple homicide. Wint subpoenaed Facebook for the social media records of a prosecution witness and the owner of an Instagram account. (See *Wint*, *supra*, 199 A.3d at p. 628.) The trial court found that the requested records were material to Wint's defense, and that it would be unconstitutional to interpret the SCA in a way that deprived Wint of the records. (*Ibid*.) The trial court therefore denied Facebook's motion to quash and held Facebook in civil contempt when it failed to produce records. (*Ibid.*)

Facebook filed an emergency appeal with the D.C. Court of Appeals. The court ordered notice to the U.S. Attorney General because the appeal implicated the SCA's constitutionality and invited the United States to file a brief and participate in oral argument. (*Ibid.*)

On January 3, 2019, the D.C. Court of Appeals unanimously reversed. The court began by holding that the plain language of the SCA precluded Facebook from complying with Wint's subpoena. (*Id.* at p. 629.) Indeed, "every court to consider the

issue has concluded that the SCA's general prohibition on disclosure of the contents of covered communications applies to criminal defendants' subpoenas." (*Ibid.*) The court also reviewed the SCA's legislative history, concluding that "the prohibition on disclosure was meant to be comprehensive." (*Id.* at p. 631.)

The court next rejected Wint's policy arguments, holding that "channeling such discovery to senders or recipients, rather than providers, increases the chances that affected individuals can assert claims of privilege or other rights of privacy before covered communications are disclosed to criminal defendants in response to subpoenas." (*Ibid.*) Enforcing the SCA as written "therefore advances a significant interest and does not lead to irrational or absurd results." (*Ibid.*, citing *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423.)

Finally, the court held that Wint did not establish "a serious constitutional doubt" warranting a different interpretation of the SCA. (*Id.* at p. 633.) "[T]he Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense," but the SCA does not preclude defendants from seeking the same communications from "entities other than providers, such as recipients and senders." (*Ibid.*)

B. The *Hunter III* Decision

The *Hunter* cases arise out of two criminal defendants' attempts to subpoena Facebook and Twitter, Inc. for a murder victim's and prosecution witness' social media communications. In *Facebook v. Superior Court* (2018) 4 Cal.5th 1245 ("*Hunter II*"), this Court held that the SCA protects privately configured social media content, even where the sender shares that content with a large group of friends and followers. (*Id.* at

pp. 1250-1251.) The Court remanded the case in part to permit the trial court 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," before even considering the defendants' "novel constitutional theory." (*Id.* at pp. 1275-1276.) On remand, though, and without fully weighing the availability of the evidence sought from other sources, the trial judge ordered Facebook and Twitter to produce private communications. (*Hunter III*, *supra*, at p. 117.) The *Hunter III* appeal followed.

In *Hunter III*, the Court of Appeal vacated the trial court's production order, holding that the trial court "did not adequately consider the appropriate factors, including alternatives that would avoid a constitutional conflict." (*Id.* at p. 118.)

Specifically, the Court of Appeal held that the trial court failed to adequately consider "options for obtaining materials from other sources" (*id.* at p. 119), including (1) whether the materials can be obtained from the witness herself, notwithstanding the defendants' "speculation" that she would plead Fifth Amendment privilege (*id.* at p. 121); (2) whether the trial court could order the witness "to consent to disclosure *by providers*" (*ibid.*); and (3) whether the defendants could obtain communications "directly from the *recipient*" under 18 U.S.C. § 2702(b)(3) (*ibid.*).

Finally, the Court of Appeal in *Hunter III* held that the trial court erred in failing to consider whether the defendants' needed the private content at issue once Facebook produced publicly configured content. (*Ibid.*)

III. APPLICATION TO *TOUCHSTONE*

A. *Wint* Confirms that the SCA's Plain Language Precludes Criminal Subpoenas Directed at Facebook.

The SCA broadly prohibits Facebook from disclosing the contents of electronic communications, stating that providers "shall not knowingly divulge to any person or entity" electronic communications, absent enumerated exceptions such as account-holder consent. (18 U.S.C. § 2702, subd. (a)(1).)

Like Wint, Touchstone offers counter-textual interpretations of the SCA to avoid its application—from claiming that he can issue a *prosecution* "trial subpoena" under section 2703(b)(1)(B)(i), to belatedly arguing that Facebook falls outside the SCA's broad definitions of electronic service providers. (Touchstone's Opening Br. p. 37; Touchstone's Suppl. Br. on *Hunter* pp. 9-11.) But as *Wint* held, there is no basis for rewriting the SCA to permit subpoenas on Facebook without account-holder consent. Rather, the SCA's text and structure demonstrate that Congress's "prohibition on disclosure was meant to be *comprehensive*," and Congress "did not intend to permit disclosure in response to criminal defendants' subpoenas." (*Wint*, *supra*, 199 A.3d at pp. 631-632.) While Touchstone and his amici argue that the SCA's language is outdated and inapplicable to social media, *Wint* held that the SCA "speaks with sufficient clarity" and applies to criminal subpoenas on Facebook. (*Ibid.*)

Further, applying the SCA to criminal subpoenas advances important policy goals, including protecting third-party privacy rights. The D.C. Court of Appeals observed that the SCA protects privacy by directing subpoenaing parties to message senders and

recipients. (*Id.* at p. 631.) Permitting defendants to bypass account holders and subpoena Facebook directly, in contrast, makes it more likely that a person will be "unaware of the subpoena for his personal or confidential information." (*Ibid.*)

Indeed, Touchstone asks this Court to go one step further and rewrite the SCA to permit in camera reviews without *any* notice to the account holder. (Touchstone's Opening Br. p. 23 [arguing that notifying the account holder may cause him to be uncooperative or raise privacy rights].) Touchstone seeks his victim's records to portray him as a violent drug user who carries guns and abuses women. (*Id.* at p. 28.) But this is precisely the reason why crime victims and other third parties *must* be given the opportunity to assert privacy rights before their private communications are divulged, and directing subpoenas toward the actual parties to the communications—senders and recipients—is the best way to ensure that opportunity. (*Wint*, *supra*, 199 A.3d at p. 632.)

B. The Stored Communications Act Is Constitutional.

Both *Hunter III* and *Wint* also rejected arguments that the SCA must require production by Facebook to avoid "curtailing criminal defendants' constitutional right[s]." (*Wint*, *supra*, 199 A.3d at p. 632.) Like Touchstone, Wint argued that his Fifth and Sixth Amendment rights required enforcing his subpoena on Facebook. (*Id.* at p. 633; *Hunter III*, *supra*, at p. 114.)

Wint held that there were no "serious constitutional doubt[s]" about the SCA's application to criminal subpoenas. (*Wint*, *supra*, 199 A.3d at p. 633.) The court explained that the Constitution guarantees a "meaningful opportunity to present a complete defense," but "[t]he compulsory-process right … is 'not unlimited.'" (*Ibid.*)

Far from depriving criminal defendants the opportunity to present a complete defense, the SCA prohibits defendants only from seeking electronic communications from one particular source—providers. The court in *Wint* explained that the same communications "can be sought through subpoenas directed at entities other than providers, such as recipients and senders." (*Ibid.*) That is the same way that criminal defendants have obtained records of communications for decades. As the D.C. Court of Appeals explained, "it would be far from irrational for Congress to conclude that one seeking disclosure of the contents of email, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message." (*Id.* at p. 631, quoting *O'Grady*, *supra*, 139 Cal.App.4th 1423.)

Like Touchstone, Wint argued that "direct subpoenas to providers are the easiest method for obtaining covered communications, and that other approaches are cumbersome, time-consuming, and more likely to be ineffective." (*Id.* at p. 633.) But, as the D.C. Court of Appeals affirmed, that does not mean that direct subpoenas on providers are constitutionally required. In fact, no court has ever permitted a criminal defendant to obtain evidence in violation of a federal statute based on speculation that other methods for obtaining the evidence might be ineffective or more cumbersome—and this Court should not be the first. The Court of Appeal in *Hunter III* rejected a similar argument, citing this Court's ruling in *Hunter II* and holding that courts *must* "consider[] alternative sources" before ordering an unlawful production from a third-party provider. (*Hunter III*, *supra*, at pp. 119-120.)

Further, both *Wint* and *Hunter III* upheld the SCA in the face of (actual or arguable) *trial subpoenas*. (See Ex. A, p. 3; *Hunter III*, *supra*, at pp. 116-117 [noting that the trial court considered the matter "as if it involved trial subpoenas [] even though new subpoenas had not been served" after the pretrial subpoenas].) In contrast, Touchstone seeks to enforce a *pretrial* subpoena, even though this Court has consistently held that there is "no general constitutional right to discovery," much less a constitutional right to *pretrial* discovery. (*Schaffer v. Superior Court* (2010) 185 Cal.App.4th 1235, 1243; *People v. Hammon* (1997) 15 Cal.4th 1117, 1125-1127.)

C. *Hunter III* and *Wint* Demonstrate Why Touchstone's Fifth Amendment and Witness-Cooperation Concerns Are Premature.

Touchstone has argued that subpoenaing the victim for his social media records could be ineffective because the victim might assert the Fifth Amendment or refuse to cooperate. The defendant in *Hunter III* made the same argument, but the court rejected it as conjecture: "[W]e reject Sullivan's assertion that it would be futile to try to obtain the communications from Lee because (Sullivan presumes) she will invoke the Fifth Amendment. This is speculation." (*Hunter III*, *supra*, at p. 121.) The court explained that because the defendant had neither "shown [a] recent effort to subpoena" the witness, nor exhausted other available methods of obtaining the records he sought, "the trial court abused its discretion in finding good cause to order providers to produce private content" that was protected by the SCA. (*Ibid.*)

Wint proved why this rule is correct. Like Touchstone and Hunter, Wint speculated that subpoenaing a witness might be ineffectual because the witness might

invoke the Fifth Amendment, and the trial court accepted that argument and ordered Facebook to produce records. (Ex. A, p. 4.) But at trial, Wint's fears proved baseless because the witness appeared at trial and gave straightforward answers to questions about his social media activity without invoking the Fifth Amendment. (Ex. B, pp. 154-156.)

The lesson from *Hunter III* and *Wint* is that courts should not order violations of the SCA and put third-party privacy at risk based on speculation that the proper subpoena targets—the account holder, message senders, and message recipients (see *Hunter III*, *supra*, at pp. 114-115)—*might* refuse to cooperate. Indeed, here, Touchstone has made little attempt to subpoena the victim, and the record includes no evidence that he attempted to subpoena message senders and recipients. As in *Hunter III*, that alone is dispositive. (*Id.* at p. 118 ["Because it did not adequately consider the appropriate factors, including alternatives that would avoid a constitutional conflict, the trial court abused its discretion when it found good cause to issue the [production] order"].)

D. The United States' Brief in *Wint* Supports Facebook.

Finally, the United States' brief in *Wint* provides additional support for Facebook's position in this appeal. Because the Attorney General prosecutes violations of the SCA and has extensive experience applying the SCA,[1] its interpretation of the statute "is entitled to respect by the courts." (*Mudd v. McColgan* (1947) 30 Cal.2d 463, 470; see also *Smith v. Mun. Court* (1959) 167 Cal.App.2d 534, 539 [because the attorney

[1] See, e.g., *U.S. v. Councilman* (1st Cir. 2005) 418 F.3d 67; *Warshak v. U.S.* (6th Cir. 2008) 532 F.3d 521.

general "is the officer charged by law with advising the officers charged with the enforcement of the law as to the meaning of it," his opinions deserve "great weight"].)

In *Wint*, the Attorney General argued that criminal defendants should not be permitted to subpoena Facebook for third-party communications, and in doing so announced several positions of the federal executive branch that are relevant to this appeal.

First, the Attorney General explained that "the SCA's general prohibition against disclosure does not raise serious constitutional concerns because a criminal defendant's constitutional rights to due process, compulsory process, and confrontation are not unlimited, and criminal defendants have alternate means of obtaining the content of communications from the sender or recipients of the communications, or from the account holder." (Ex. C, pp. 6-7.) The SCA is "not a categorical prohibition on a defendant's ability to obtain and introduce the content of electronic communications," but instead "limits the methods a defendant can use to obtain evidence by prohibiting *one source* – the service provider – from disclosing the content of communications absent consent." (*Id.* at p. 34.) Indeed, "'[t]he most effective methods of obtaining discovery of the contents of a party's social networking profile are propounding specific, well-tailored discovery requests to the party himself.'" (*Id.* at p. 25 fn. 17.)

Second, permitting criminal defendants to subpoena Facebook directly "would violate people's right to privacy and potentially jeopardize their safety by allowing defendants to obtain access to the contents of the electronic communications of a victim [or] witness." (*Id.* at p. 26.)

Third, the Attorney General addressed the trial court's myriad tools to assure criminal defendants a fair trial, including "requir[ing] the account-holder to consent to disclosure of the content," "preclud[ing] a witness from testifying or limit[ing] the witness's testimony if a witness refused to comply with such a subpoena," and "craft[ing] an instruction similar to the missing evidence instruction given when the government fails to produce evidence." (*Id.* at pp. 38-39.) "What a court should not do is order Facebook or another service provider to violate federal law." (*Ibid.*)

Fourth, the Attorney General explained that courts should not order violations of the SCA based on the "speculative possibility that the account holder 'could' assert [the] Fifth Amendment." (*Id.* at p. 39-40 fn. 24.) Rather, if a witness *actually* refuses to disclose exculpatory evidence, the trial court should "inform[] the government that it must make the choice between dismissal of the indictment or some other commensurate remedy which the court may fashion on Sixth Amendment and due process grounds, or affording use immunity to the crucial defense witness involved." (*Ibid.*, citing *Carter v. U.S.* (D.C. 1996) 684 A.2d 331, 343.)

IV. CONCLUSION

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

DATED: May 8, 2020

Respectfully Submitted,

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Joshua S. Lipshutz*
Joshua S. Lipshutz

Attorney for Facebook, Inc.

CERTIFICATE OF WORD COUNT

I, Joshua Lipshutz, certify that, according to the software used to prepare this brief, the word count of this brief is 2,799 words, which is fewer than the 2,800 words allowed for Supplemental Briefs under California Rule of Court 8.520(d)(2). I swear under penalty of perjury that the foregoing is true and correct.

DATED: May 8, 2020

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

Exhibit A

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
Criminal Division – Felony Branch

UNITED STATES	:	**Docket No. 2015 CF1 7047**
	:	**Hon. Judge Juliet McKenna**
v.	:	**Trial: September 5, 2018**
	:	
DARON WINT	:	**UNDER SEAL**

ORDER DENYING FACEBOOK, INC.'S MOTION TO VACATE ORDERS AND QUASH SUBPOENAS

Upon consideration of Facebook, Inc.'s Motion to Vacate Orders and Quash Subpoenas, the Court makes the following findings:

On August 20, 2018, the Court issued an Order authorizing defense counsel to subpoena Facebook, Inc. and Instagram, Inc. for information associated with Facebook accounts for "Jordan Wallace" *and* phone number [redacted] as well as information associated with the Instagram account associated with either username "racer_jordan" or "dreday7600," or phone number [redacted]. On August 30, 2018, Facebook filed a Motion to Vacate the Court's Order and Quash the Subpoenas. The Court granted Facebook's motion solely based on the information provided by Facebook that "there is no account associated with username 'Jordan Wallace and phone number [redacted]." The defense filed a Motion to Reconsider and provided further information that no check was run for an account with the username "Jordan Wallace" *or* phone number [redacted] and the Court reissued both subpoenas. Facebook subsequently filed a Renewed Motion to Vacate Orders and Quash Subpoenas arguing that the subpoenas should be quashed "because (1) the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, does not permit criminal defendants to use a subpoena or court order to compel a service provider to disclose the contents or communications; (2) the subpoenas do not

satisfy Rule 17 because any relevant records and content are otherwise procurable in ways that do not violate federal law; and (3) the subpoenas do not satisfy Rule 17 because Defendant is engaged in a "fishing expedition." Facebook Mot. to Renew at 1.[1]

Pursuant to the Stored Communications Act ("SCA"), electronic communication service providers, such as Facebook, Inc. and Instagram, are generally not permitted to disclose a record or other information regarding a subscriber, *see* 18 U.S.C. § 2702(a)(3), or the contents of a subscriber's electronic or wire communications, *see id.* § 2703(a)(1). The SCA provides an exception for disclosure to government entities, pursuant to a warrant, court order, or subpoena. *See* 18 U.S.C. § 2703 (a), (b).

The California Supreme Court recently considered the question of whether electronic communication service providers must produce publicly configured data in response to a defense subpoena seeking public and private data, including deleted information. *Facebook, Inc. v. Superior Court*, 417 P.3d 725 (Cal. 2018). The court held that, in configuring communications to be public, a social media user implicitly consented to disclosure and that such content fell within § 2702(b)(3)'s lawful consent exception. The court went on to find that a communication service provider may not refuse to disclose the content of public communications when served with a valid subpoena. *Id.* The Supreme Court of California, however, declined to answer the question presented here—whether a user revokes consent when he or she deletes content or changes his or her privacy settings. *Id.* at 754.

The Court finds that deletion of a post or modification of privacy settings does not necessarily constitute a revocation of consent. When a user posts public content, there is no

[1] In Facebook's initial Motion to Quash, it argued that "the Order's nondisclosure provision is not authorized by Rule 17 or the SCA." The Court did not address this argument here because in Facebook's renewed Motion to Quash, it stated, "Facebook understands from Defendant's Motion that the Orders' nondisclosure provisions are not intended [to] apply to Facebook." Facebook Mot. at 2 n.1.

reasonable expectation of privacy given that anyone viewing the public content could have screenshotted, saved, or forwarded the social media content to others and the subsequent deletion of that content by the user does not rescind or retract the original communication.

Regardless of whether the communications were configured as public or private, to read the SCA as prohibiting disclosure of such communications, in response to a court authorized subpoena, would violate the defendant's Fifth and Sixth Amendment rights. The primary purpose of the SCA is to balance the privacy interest of subscribers with the needs of the government and law enforcement agencies, not to restrict a criminal defendant's right to present a complete defense. The instant case is readily distinguishable from other cases in which courts have quashed pre-trial subpoenas because a criminal defendant's right to pretrial discovery is limited, s*ee id.* at 735. In this case, parties are in the midst of jury selection and trial is expected to commence immediately thereafter. Therefore, this is no longer a pretrial discovery request. The Supreme Court of California explained that the Court of Appeal's opinion rejecting the defense's argument that denying the subpoenas violated the defendant's Fifth and Sixth Amendment rights was "confined to *'this stage of the proceedings'* and limited to the 'pretrial context in which the trial court's order was made.'" *Id.* at 735 (original italics). Further, the California Supreme Court 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." *Id.* (original italics).

It has been long held that congressional statutes cannot abridge fundamental constitutional rights. *Marbury v. Madison*, 5 U.S. 137 (1803). Pursuant to the Fifth and Sixth Amendment, Mr. Wint now has the right to compulsory process, to effectively confront witnesses against him, and to cross examine those witnesses. In *Davis v. Alaska*, the United

States Supreme Court has held that a criminal defendant's constitutional right to cross-examine witnesses trumped a state law declaring juvenile records to be confidential and not to be disclosed to the public. 415 U.S. 308 (1974). Specifically, the trial judge prohibited defense counsel from questioning a witness about the latter's juvenile criminal record because a state statute made this information presumptively confidential. The Court found that this restriction on cross-examination violated the Confrontation Clause, despite Alaska's legitimate interest in protecting the identity of juvenile offenders. *See id.* at 318–320.

To read the SCA as prohibiting Facebook from disclosing information necessary to confront witnesses against Mr. Wint would similarly violate the Confrontation Clause and render the SCA unconstitutional. Therefore, the Court concludes that the SCA cannot prohibit such a disclosure. *See Clark v. Martinez*, 543 U.S. 371, 381–82 (2005) (explaining that when choosing between competing statutory interpretations, courts may "rest[ ] on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts").

The Court rejects Facebook's contention that these records are procurable in other ways. The defense cannot obtain these records via subpoena to the users or the government. Because the records requested may implicate Mr. Wallace in a criminal conspiracy, the records may conflict with Mr. Wallace's Fifth Amendment privileges against self-incrimination. Mr. Wint cannot subpoena the account holder for the account "dreday7600" because he has not been provided with the identity of this account holder. Even if the identity of the account holder was disclosed to the defense, that individual could also assert his Fifth Amendment privilege against self-incrimination.

The government cannot provide the records to the defense because the government chose to subpoena some, but not all of the relevant social media records, all of which the defense needs

to present a complete defense. Further, the government does not have an affirmative obligation to seek out information not held by the prosecution team. Additionally, the defense sought a subpoena on an *ex parte* basis because, at this juncture, the prosecution is not entitled to learn the details of Mr. Wint's defense through Rule 16 discovery or otherwise. See Bowman v. United States, 412 A.2d 10 (D.C. 1980). Therefore, the defense cannot obtain these records from the government, nor can the defense obtain the records from the account holders.

Finally, the Court is satisfied that this is not a "fishing expedition" by the defense. Jordan Wallace has been identified as a witness that the government intends to call at trial. Based upon prior *ex parte* representations by defense counsel, the information regarding Jordan Wallace's Facebook and Instagram accounts is material to Mr. Wint's defense in this case.

Therefore, it is this 10th day of September 2018, hereby,

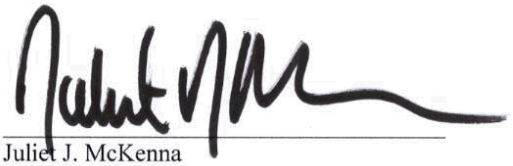
ORDERED that Facebook's Motion to Vacate Orders and Quash Subpoenas is DENIED; it is further

ORDERED the deadline for Facebook to comply with the subpoena is extended from September 4, 2018 to 9:30 am on Tuesday, September 11, 2018; it is further

ORDERED that, pursuant to Nellson v. Bayly, 856 A.2d 566, 567 (D.C. 2004), having found (1) that Mr. Wint has a compelling interest in having his defense theory, strategy, and investigation remain confidential, that (2) sealing would serve that interest, (3) that in the absence of sealing, that interest would be harmed, and (4) that there are no alternatives to sealing, the defense's Motion and this Order be placed UNDER SEAL; it is further

ORDERED that any subsequent filings related to this Motion or the related subpoenas be filed under seal without service or notice to the government; it is further

ORDERED that, because the Court finds that "exceptional circumstances" exist as contemplated by D.C. Superior Court Crim. Pro Rule 17(c)(3), the Court will not require notice of this Order to Jordan Wallace.



Juliet J. McKenna
Associate Judge
Superior Court for the District of Columbia

Exhibit B

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION

UNITED STATES OF AMERICA,	:	**(EXCERPT)**
versus	:	Criminal Action Number
DARON D. WINT,	:	2015-CF1-7047
Defendant.	:	

Washington, D.C.
Monday, September 17, 2018

The above-entitled action came on for a Jury Trial, before the Honorable JULIET J. MCKENNA, Associate Judge, in courtroom number 203, commencing at 11:50 a.m.

THIS TRANSCRIPT REPRESENTS THE PRODUCT OF AN OFFICIAL REPORTER, ENGAGED BY THE COURT, WHO HAS PERSONALLY CERTIFIED THAT IT REPRESENTS TESTIMONY AND PROCEEDINGS OF THE CASE AS RECORDED.

APPEARANCES:

On behalf of the Government:

LAURA R. BACH, Esquire
CHRISTOPHER BRUCKMANN, Esquire
Assistant United States Attorneys

On behalf of the Defendant:

JUDITH PIPE, Esquire
JEFFREY STEIN, Esquire
Washington, D.C.

Stacey E. Raikes, RMR, CRR (202) 879-1447
Official Court Reporter

TABLE OF CONTENTS
TRIAL
WITNESSES

On behalf of the Government:

JORDAN T. WALLACE

EXHIBITS

On behalf of the Government:

MISCELLANY

to be questioned?

A. No.

Q. No, because that wouldn't make any sense?

A. Correct.

Q. Right? So when you deleted that text message exchange with Ashley, it was after you found out you were going to be questioned?

A. Yes.

Q. Now, it's fair to say that the Savopouloses were extremely wealthy?

A. Yes.

Q. They owned, I think, five luxury cars, right?

A. Uh-huh.

Q. And including that Mosler that was one of three in the world?

A. Yes, sir.

Q. And it was -- I mean, it was genuinely impressive how successful they were, right?

A. Correct.

Q. And you, understandably, liked to talk about how wealthy your boss was, right?

A. Not necessarily, no.

Q. Well, and we'll talk about this more in a second, but you certainly posted a lot of photos of their cars, right?

A. I posted a few photos of their cars.

Q. On social media, right?

A. Yes.

Q. And --

A. But nothing of the outside of the vehicles, just of the inside, and I never once said whose cars they were.

Q. So the Savopouloses never -- well, Mr. Savopoulos, Savvas, never specifically or explicitly told you not to talk about his cars with anyone, right?

A. Correct.

Q. And he never specifically told you not to share information about your job with anyone, right?

A. Correct.

Q. You know, you had an understanding that you --

A. Yeah.

Q. -- you should respect his privacy?

A. Yes, sir.

Q. But he never ordered you, you know, you are not to share anything about your job with anyone, right?

A. Yes, sir.

Q. And you did post a lot of photos on social media, right?

A. What would you consider a lot?

Q. Well, you posted pictures of the Range Rover on Instagram, right?

A. I posted a picture of the interior of the Range Rover one time.

Q. Okay. And you -- on Instagram?

A. Yes, sir.

Q. Right? And, even before you started working for Savvas, you posted a picture of his Mosler on Facebook, right?

A. Yes.

Q. Because you had seen it at Autobahn?

A. Yeah, he encouraged me to do so.

Q. And --

A. He said more people need to see that car.

Q. And you would text your girlfriend and ask her things like did you see what I'm driving today, right?

A. Yeah.

Q. I'm sorry?

A. Yes, sir.

Q. And you also -- did you also have a Twitter account?

A. No.

Q. Okay. Your --

A. Or, if I did, I didn't use it.

Q. Okay. And then there's that picture that you sent your girlfriend of the $40,000 --

A. Correct.

CERTIFICATE OF REPORTER

I, Stacey E. Raikes, RMR, CRR, an Official Court Reporter for the Superior Court of the District of Columbia, do hereby certify that I reported, by machine shorthand, in my official capacity, the proceedings had and testimony adduced upon the Jury Trial in the case of the UNITED STATES OF AMERICA versus DARON D. WINT, Criminal Action Number 2015-CF1-7047, in said court on the 17th day of September, 2018.

I further certify that the foregoing 184 pages constitute the official transcript of said proceedings, as taken from my machine shorthand notes, together with the backup tape of said proceedings to the best of my ability.

In witness whereof, I have hereto subscribed my name, this 18th day of September, 2018.

Stacey E. Raikes, RMR, CRR
Official Court Reporter

Exhibit C

BRIEF FOR THE UNITED STATES

DISTRICT OF COLUMBIA
COURT OF APPEALS

No. 18-SS-958

IN RE FACEBOOK,

Appellant.

APPEAL FROM THE SUPERIOR COURT
OF THE DISTRICT OF COLUMBIA
CRIMINAL DIVISION

JESSIE K. LIU
United States Attorney

ELIZABETH TROSMAN
* LAUREN R. BATES
D.C. Bar #975461
Assistant United States Attorneys
* Counsel for Oral Argument
555 Fourth Street, NW, Room 8104
Washington, D.C. 20530
Lauren.Bates@usdoj.gov
(202) 252-6829

TABLE OF CONTENTS

TABLE OF AUTHORITIES*

Page

OTHER AUTHORITIES

ISSUES PRESENTED

I. Whether the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, et seq., prohibits service providers such as Facebook, Inc. ("Facebook") from producing the contents of communications in response to a criminal defendant's subpoena absent consent, where the plain language of Section 2702(a) sets forth a general prohibition against the disclosure of "the contents of a communication" by a service provider to "any person or entity," and none of the exceptions to this prohibition permit disclosure in response to a criminal defendant's subpoena absent consent of the sender, recipient, or account holder.

II. Whether, despite the SCA's plain-language prohibition on disclosure, this Court should adopt a reading of the SCA that allows service providers to disclose the content of communications in response to a criminal defendant's subpoena on the ground that a contrary interpretation would raise serious constitutional concerns, where the SCA's general prohibition against disclosure is neither ambiguous nor does it implicate serious constitutional concerns because a criminal defendant's Fifth and Sixth Amendment rights to due process, compulsory process, and confrontation are not unlimited and criminal

defendants have alternate means of obtaining the content of electronic communications.

DISTRICT OF COLUMBIA
COURT OF APPEALS

No. 18-SS-958

IN RE FACEBOOK,

Appellant.

APPEAL FROM THE SUPERIOR COURT
OF THE DISTRICT OF COLUMBIA
CRIMINAL DIVISION

BRIEF FOR THE UNITED STATES

COUNTERSTATEMENT OF THE CASE

This appeal arises from *ex parte* proceedings in a criminal prosecution that occurred before the Honorable Juliet J. McKenna. After hearing an *ex parte* proffer from appellee, Judge McKenna authorized appellee to serve subpoenas *duces tecum* on Facebook, Inc. ("Facebook") seeking "any and all information" from January 1, 2015, to the present, relating to any Facebook accounts associated with the name of a government witness or a specific phone number and two Instagram accounts, including "all photos, messenger calls, messages, wall posts,

friends, likes and status updates," as well as information relating to the "physical address," "GPS location," and "IP address" of the account holder(s) (Appx. 39, 43, 45).[1] These subpoenas were issued pursuant to Superior Court Rule of Criminal Procedure 17(c) in connection with a now-ongoing trial. The trial court issued the subpoenas on an *ex parte* basis, finding that the government was not entitled to learn the details of the defendant's defense.

Facebook moved to quash the subpoenas on the grounds that "(1) the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, does not permit criminal defendants to use a subpoena or court order to compel a service provider to disclose the contents of communications; (2) [the subpoenas] do not satisfy Rule 17 because any relevant records and content are otherwise procurable in ways that do not violate federal law; and (3) [the subpoenas] do not satisfy Rule 17 because Defendant is engaged in a fishing expedition" (Appx. 20). Facebook proffered that, although there was one "Facebook account associated with the specified

[1] "Appx." refers to the Appendix of Exhibits Required by Rule 4(c)(2)(B)(iv) filed by Facebook. A redacted copy of this appendix was provided to the United States on September 27, 2018.

phone number, it was created in 2017 – two years after the commission of the crime at issue in this trial" (Appx. 31). In addition, "a search for [the name of the specified government witness] on Facebook yields dozens of results" (*id.*).

On September 6, 2018, Judge McKenna issued a written order denying Facebook's motion to quash, finding that, although providers such as Facebook "are generally not permitted to disclose a record or other information regarding a subscriber, or the contents of a subscriber's electronic or wire communications," "to read the SCA as prohibiting disclosure of such communications, in response to a court authorized subpoena, would violate the defendant's Fifth and Sixth Amendment rights" (Appx. 52-54) (citing *Marbury v. Madison*, 5 U.S. 137 (1803), for the proposition that "[i]t has long been held that congressional statutes cannot abridge fundamental constitutional rights"). Judge McKenna further found that the requested records were not "procurable in other ways" because "the records requested may implicate [one of the account holders] in a criminal conspiracy, [and thus] the records may conflict with [the account holder's] Fifth Amendment privilege[ ] against self-incrimination" and because the identity of at least one of the account

holders was not known to the defense (Appx. 55). Finally, Judge McKenna explained that "the Court is satisfied that this is not a 'fishing expedition' by the defense. [One of the account holders] has been identified as a witness the government intends to call at trial" and "[b]ased upon prior *ex parte* representations by defense counsel, the information regarding [the requested] Facebook and Instagram accounts is material to [the] defense in this case" (Appx. 56).

Facebook subsequently "produced reasonably responsive, non-content, transactional information, including basic subscriber information, IP addresses, message headers, and device information" (Appx. 59). However, because Facebook "will not violate the SCA," it refused to provide the content of communications (*id.*). Accordingly, Facebook requested an order of civil contempt from the trial court so that it could appeal the trial court's order (Appx. 58). Pending appellate review, Facebook stated that it would "continue to preserve any information in its possession that is responsive" (Appx. 59).

After the trial court issued an order holding Facebook in civil contempt and assessing sanctions of $10,000 per day for failing to comply with the subpoenas (Appx. 70), Facebook noted the instant appeal on

September 12, 2018 (Appx. 72). Facebook filed a motion for summary reversal on September 17, 2018. Appellee filed an opposition on September 21, 2018, and Facebook filed a reply on September 25, 2018.

On September 24, 2018, this Court issued an Order "certify[ying] to the Attorney General of the United States that appellee in this emergency appeal has filed a motion that 'questions the constitutionality' of the Stored Communications Act" pursuant to D.C. App. R. 44(a); ordering the parties to provide redacted versions of the cross-motions for summary disposition to the United States Attorney's Office by 5:00 p.m. on Tuesday, September 25, 2018; and ordering that the United States has until 5:00 p.m. on Tuesday, October 2, 2018, within which to file a brief in this case. An oral argument is scheduled before this Court at 10:00 a.m. on Tuesday, October 9, 2018.

SUMMARY OF ARGUMENT

The SCA prohibits Facebook from disclosing the contents of electronic communications in response to appellee's subpoenas absent consent. The plain language of Section 2702(a) sets forth a general prohibition against the disclosure of "the contents of a communication" by a service provider to "any person or entity," and none of the exceptions to this prohibition permit disclosure in response to a criminal defendant's subpoena absent consent of the sender, recipient, or account holder. Although Section 2702 is broadly titled "[v]oluntary disclosure of customer communications or records," it is not limited to voluntary disclosures. The plain language of Section 2702(a)'s general prohibition against disclosure of the contents of communications is consistent with the legislative history and purpose of the SCA.

Because Section 2702(a) is not ambiguous, there is no basis for this Court to apply the canon of constitutional avoidance and adopt a reading of the SCA that allows service providers to disclose the content of communications in response to a criminal defendant's subpoena. Moreover, the SCA's general prohibition against disclosure does not raise serious constitutional concerns because a criminal defendant's

constitutional rights to due process, compulsory process, and confrontation are not unlimited, and criminal defendants have alternate means of obtaining the content of communications from the sender or recipients of the communications, or from the account holder.

ARGUMENT

I. The SCA Prohibits Service Providers From Disclosing the Contents of Electronic Communications In Response to a Defendant's Trial Subpoena Absent Consent.

A. The Stored Communications Act

The Stored Communications Act, 18 U.S.C. § 2701, *et seq*., was enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA"). *See* Pub. L. No. 99-508, 100 Stat. 1860 (Oct. 21, 1986). The Act sets forth statutory provisions, codified at 18 U.S.C. §§ 2701-2713, to protect the privacy of stored email and other stored electronic communications. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1218-22 (2004). The SCA governs how stored wire and electronic communications may and may not be lawfully disclosed by an "electronic communications service" or a "remote computing service,"

collectively referred to *infra* as "service providers." *See* 18 U.S.C. §§ 2701-2713.[2]

Section 2702 of the SCA restricts service providers that provide service to the public from disclosing communications and other records except in specified circumstances.[3] Captioned "Voluntary disclosure of customer communications or records," Section 2702 begins with general prohibitions on provider disclosure. First, it states that a service provider to the public "*shall not* knowingly divulge to any person or entity the *contents*" of specified communications. 18 U.S.C. §§ 2702(a)(1) and (2) (emphasis added). Second, it states that a service provider to the public "shall not knowingly divulge [*non-content information*]" to "any governmental entity." 18 U.S.C. § 2702(a)(3) ("a [service] provider . . .

---

[2] An "electronic communication service" "provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A "remote computing service" provides "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[3] Services are provided "to the public" if they are available to any member of the general population who accepts the terms of service and pays any required fees. For example, Facebook and Gmail are provided to the public, but a private company that provides email to its employees is not a service provider to the public. *See, e.g., Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998).

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").[4]

Section 2702 then sets forth a series of "[e]xceptions for disclosure of communications" whereby a service provider "may divulge the *contents of a communication*." 18 U.S.C. § 2702(b) (emphasis added). Specifically, a service provider "may divulge the contents of a communication": "(1) to an addressee or intended recipient of such communication or an agent of

---

[4] A "governmental entity" "means a department or agency of the United States or any State or political subdivision thereof" and is distinct from a "court of competent jurisdiction," which is defined separately 18 U.S.C. §§ 2711(3) and (4). Appellee does not contend that it is a "governmental entity." *See United States v. Wenk*, No. 17-cr-85, 2017 WL 9989882, at *1 (E.D. Va. Nov. 29, 2017) ("It is clear that courts do not qualify as 'governmental entities'" under the SCA); *United States v. Amawi*, 552 F. Supp. 2d 679 (N.D. Ohio 2008) ("the judiciary and its components, including the Federal Public Defender, cannot obtain a court order under § 2703(d)").

We refer to what is described in the SCA as "a record or other information pertaining to a subscriber [ ] or to a customer . . . (not including the contents of communications . . .)," generally as non-content information. 18 U.S.C. § 2702(a)(3). This non-content information includes, as is relevant to the instant appeal, "basic subscriber information, IP addresses, message headers, and device information" (Facebook Mot. at 8-9).

such addressee or intended recipient"; "(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title";[5] "(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"; "(8) to a governmental entity, if the provider, in good faith, believes that an

[5] As discussed *infra*, Section 2703 provides three mechanisms by which a service provider can be *required* to disclose certain information to the *government* about wire or electronic communications. 18 U.S.C. § 2703.

Section 2517 addresses "[a]uthorization for disclosure and use of intercepted wire, oral, or electronic communications," and Section 2511(2)(a) provides the circumstances where "[i]t shall not be unlawful . . . for an operator of a switchboard or an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication."

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." 18 U.S.C. §§ 2702(b)(1)-(9).

Section 2702 next sets forth a separate series of "[e]xceptions for disclosure of *customer records*" whereby a service provider "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))." 18 U.S.C. § 2702(c) (emphasis added). Specifically, a service provider "may divulge a record or other information" "(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." 18 U.S.C. §§ 2702(c)(1)-(7).

Section 2703 of the SCA, captioned "Required disclosure of customer communications or records," regulates how a governmental entity[6] can require a service provider to disclose information to the government. *See* 18 U.S.C. § 2703. Section 2703 provides three separate mechanisms for the government to acquire such information: a subpoena, a court order, or a warrant. *Id.* As explained below, the mechanism used by the government affects the type of information it can obtain: certain compelled disclosures require a more demanding showing.[7]

---

[6] *See supra* note 4.

[7] In addition, the mechanism used to compel disclosure of information from a service provider must comply with the Fourth Amendment, if implicated. For example, although the SCA allows use of a court order to compel disclosure of historical cell-site records, the Supreme Court held that a warrant must be used to compel disclosure of seven or more days of such records. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3, 2221 (2018).

First, the government may issue an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" to acquire basic subscriber information such as the subscriber's name and identifying information. 18 U.S.C. § 2703(c)(2). Under the SCA, a subpoena may also be used for contents in electronic storage with a provider for more than 180 days, or for other contents stored by a remote computing service. 18 U.S.C. §§ 2703(a), (b)(1)(B).[8]

Second, the government may obtain a court order, sometimes called a 2703(d) order, requiring disclosure of any records legally obtainable by subpoena and additional non-content information "pertaining to a subscriber." 18 U.S.C. §§ 2703(b)(1)(B)(ii) and (c)(1). For example, the government must obtain a 2703(d) order to obtain historical logs of email addressing information (*i.e.*, "header" information). The government may obtain a 2703(d) order only if it "offers specific and articulable facts

---

[8] When the government obtains contents with a subpoena, it must provide prior notice to the subscriber or comply with procedures that allow notice to be delayed. 18 U.S.C. §§ 2703(b)(1)(B) and 2705(a).

Although the SCA allows use of a subpoena to compel disclosure of the contents of communications that are more than 180 days old, the Sixth Circuit held that a warrant is required under the Fourth Amendment to compel disclosure of email contents from a commercial service provider. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

showing that there are reasonable grounds to believe that" the records sought are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Third, the SCA authorizes the government to "require the disclosure" by a service provider of electronic communications and other records by means of a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." 18 U.S.C. §§ 2703(a) and (b). Unlike with subpoenas and 2703(d) orders, the government may obtain the contents of communications stored by an electronic communication service for fewer than 181 days, 18 U.S.C. § 2703(a), and may demand the same records covered by a 2703(d) order without providing prior notice to a subscriber. 18 U.S.C. § 2703(b)(1)(A). To obtain a Section 2703 warrant, the government must satisfy a neutral judicial officer that there is probable cause to believe that the records to be disclosed contain evidence of a crime, and must describe those records with particularity. Fed. R. Crim. P. 41(d).

The SCA provides that any person "aggrieved" by a violation of the statute may recover actual and statutory damages from the person or

entity that committed the violation. 18 U.S.C. §§ 2707(a)-(c). Section 2707(e) provides a defense for service providers who relied in good faith on "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization . . . ."[9]

B. Standard of Review and Applicable Legal Principles

This Court reviews questions of statutory interpretation *de novo*. *Peterson v. United States*, 997 A.2d 682, 683 (D.C. 2010). In interpreting a statute, this Court looks to the statute's plain language to determine if it is "clear and unambiguous." *Id.* at 684 (internal quotation marks omitted). "[I]f it is clear and unambiguous and will not produce an absurd result, [this Court] will look no further." *Pixley v. United States*, 692 A.2d 438, 440 (D.C. 1997). If the statute's words are ambiguous, then the Court may turn to the statute's legislative history to determine its meaning. *See Hood v. United States*, 28 A.3d 553, 559 (D.C. 2011).

[9] Contrary to appellee's suggestion (at 12 n.11), Section 2707(e) does not include trial subpoenas or defense subpoenas in this list.

C. Discussion

The plain language of Section 2702(a) sets forth a broad prohibition against the disclosure of "the contents of a communication" by a service provider: a service provider "*shall not* knowingly divulge to any person or entity the contents of [a] communication." 18 U.S.C. §§ 2702(a)(1) and (2) (emphasis added). Every court to address this provision has held that the SCA presents a "general prohibition on disclosure" of the contents of communications. *See, e.g.*, *Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1249 (2018) (the SCA "declar[es] that as a general matter [service providers] may not disclose stored electronic communications except under specified circumstances"); *State v. Bray*, 363 Or. 226, 229-30 (2018) ("In simplified terms and subject to exceptions, section 2702 of the SCA prohibits providers . . . from knowingly divulging to any person or entity the contents of any communication carried or maintained in that service."); *Sines v. Kessler*, No. 18-mc-80080, 2018 WL 3730434, at *10 (N.D. Cal. Aug. 6, 2018) ("The SCA prohibits any 'person or entity providing an electronic communication service to the public' from 'knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service' without the

lawful consent of the sender or recipient of the communication. There are no exceptions for civil subpoenas, which are subject to SCA prohibitions." (quoting 18 U.S.C. § 2702(a), (b), and citing *In re Super Vitaminas, S.A.*, No. 17-mc-80125, 2017 WL 5571037, at *3 (N.C. Cal. Nov. 20, 2017))); *United States v. Wenk*, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017) ("The SCA prohibits service providers from knowingly divulging electronic communications stored under their control, subject to several exceptions."). Accordingly, absent an applicable exception, the SCA does not allow non-governmental entities, including criminal defendants, to obtain the contents of communications from a service provider pursuant to a subpoena. *See generally* 18 U.S.C. §§ 2702(b)(1)-(8) (enumerating eight exceptions to Section 2702(a)).[10]

Because the plain language of Section 2702(a) prohibits disclosure of the "contents of a communication" to anyone, 18 U.S.C. §§ 2702(a)(1), (2), this Court should look "no further." *Pixley*, 692 A.2d at 440 (a court first looks to statute's plain language to determine if it is "clear and

[10] Courts throughout the country have found that subpoenas from criminal defendants seeking disclosure of the contents of communications from Facebook and similar service providers are unlawful under the SCA. For a collection of opinions and orders, see Facebook's Appendix at 22-23.

unambiguous," if it is "and will not produce an absurd result, [the court] will look no further").

Appellee, however, contends (at 7-8) that Section 2702 "addresses voluntary disclosures, and not compelled ones" such that the prohibition on disclosure "does not encompass court-ordered disclosures to criminal defendants pursuant to Rule 17(c)" subpoenas. Appellee does not point to any word or phrase in Section 2702 that is ambiguous. Rather, appellee's argument relies on the title of Section 2702 – "Voluntary disclosure of customer communications or records" – in arguing that the text of the statute means something other than what it states.[11] But, "the title of a

---

[11] This title was added in 2001 as part of the USA PATRIOT Act, Pub. L. No. 107-56, § 212, 115 Stat. 284. Prior to 2001, the title of Section 2702 was "Disclosure of contents." The title of Section 2703 was also changed from "Requirements for governmental access" to "Required disclosure of customer communications or records." *Id.*

The 2001 amendments moved part of what was contained in Section 2703 to Section 2702. For example, Section 2702 added subsection 2702(a)(3) – the prohibition against disclosure of non-content information to any governmental entity – and subsection 2702(c) – the "[e]xceptions for disclosure of customer records." Prior to the 2001 amendments, Section 2703(c)(1)(A) included language permitting a service provider to disclose non-content information "to any person other than a governmental entity" (*i.e.,* what is now one of the exceptions in Section 2702(c)).

The 2001 amendments *did not* alter the requirement that a service provider "*shall not* knowingly divulge to *any person or entity* the contents

statute cannot limit the plain meaning of the text. For interpretive purposes, it is of use only when it sheds light on some ambiguous word of phrase." *Pennsylvania Dep't of Corr. v. Yeskey*, 524 U.S. 206, 212 (1998) (citation, brackets, ellipsis, and some alterations omitted); *accord Cherry v. District of Columbia*, 164 A.3d 922, 928 (D.C. 2017) (recognizing that this Court has "cautioned" that "'[t]he significance of the title of [a] statute should not be exaggerated'") (quoting *Freundel v. United States*, 146 A.3d 375, 381 (D.C. 2016)); *see also Carter v. United States*, 530 U.S. 255, 267 (2000). The text of Section 2702 is not ambiguous. The requirement that a service provider "*shall not* knowingly divulge to *any person or entity* the contents of a [stored] communication," 18 U.S.C. §§ 2702(a)(1)-(2), could not be clearer. There is thus no basis to consider Section 2702's title, let alone rely on it to read ambiguity into an otherwise unambiguous statutory prohibition.

Moreover, as we explain below, although Section 2702 is broadly titled "[v]oluntary disclosure of customer communications or records," it

---

of a [stored] communication" in 18 U.S.C. §§ 2702(a)(1)-(2). Accordingly, the fact that Congress changed the title of Section in 2702 in 2001, 15 years after the SCA was enacted, cannot alter the plain meaning of the statutory language.

clearly is not limited only to voluntary disclosures as it addresses circumstances when a service provider is *required* to disclose pursuant to a subpoena or court order.

The "[p]rohibitions" set forth in Section 2702(a)(1) and (2) apply broadly to prohibit disclosure of the contents of communications to "any person or entity." The exceptions to this broad prohibition against disclosure do not apply solely to voluntary disclosures – *i.e.*, circumstances where a service provider has discretion to determine whether it will or will not make a voluntary disclosure. Rather, numerous exceptions apply to mandatory disclosures. For example, Section 2702(b) provides an exception for disclosure "as otherwise authorized in" Section 2703. 18 U.S.C. § 2702(b)(2). As noted above, Section 2703 sets forth the mechanisms by which the government can *require* disclosure of the contents of communications pursuant to a warrant. 18 U.S.C. § 2703. In addition, Section 2702(b) provides an exception that permits disclosure to the National Center for Missing and Exploited Children ("NCMEC") in connection with a report submitted thereto under 18 U.S.C. § 2258A. 18 U.S.C. § 2702(b)(6). Section 2258A, in turn, *requires*, in certain specified circumstances, a service provider to disclose information to

NCMEC. 18 U.S.C. § 2258A(a)(1) (requiring that a service provider "*shall*, as soon as reasonably possible" provide certain information) (emphasis added). Thus, Section 2702's reach is not limited to only voluntary disclosures by service providers.[12] Rather, read as a whole, Section 2702 prohibits the disclosure of the "contents of any communication" unless an exception permitting voluntary disclosure *or* one requiring mandatory disclosure applies.[13]

---

[12] This Court should avoid concluding that Section 2702 applies only to voluntary disclosures as appellee suggests because such a reading of the statute would fail to give effect to the exceptions for required disclosures authorized by Section 2703 and Section 2258A. *See generally Zhou v. Jennifer Mall Rest., Inc.*, 699 A.2d 348, 353 (D.C. 1997) ("We interpret statutory provisions so as to give effect to all the statutory language."); *see also United States v. Alaska*, 521 U.S. 1, 59 (1997) ("The Court will avoid an interpretation of a statute that renders some words altogether redundant."); *In re Z.B.*, 131 A.3d 351, 355 (D.C. 2016) ("The courts are to construe statutes in a manner which assumes that [the legislature] has acted logically and rationally.").

[13] Appellee notes (at 9) that Section "2702(d) specifically describes two of the enumerated exceptions in § 2702(b) and (c) as 'voluntary disclosures.'" The two exceptions – "voluntary disclosures under subsection (b)(8)" and "voluntary disclosures under subsection (c)(4)" – do not include the exceptions for required disclosures pursuant to Section 2703, 18 §§ U.S.C. 2702(b)(2) and (c)(1), or mandatory disclosures to the NCMEC pursuant to Section 2258A, 18 U.S.C. §§ 2702(b)(6) and (c)(5). Moreover, the fact that Section 2702(d) refers to certain specified exceptions as "voluntary disclosures," reinforces the conclusion that not all of the exceptions are voluntary disclosures.

Although this Court need "look no further," *Pixley*, 692 A.2d at 440, the plain language of the SCA is consistent with its purpose and history. *See* H.R. Rep. No. 99-647, at 64 (1986) (Section 2702 is a "general prohibition[] on the disclosure of contents" and a "provision [that] is aimed at proscribing the disclosure of stored . . . communications" subject only to the specified "exceptions to this general rule"); *id.* at 65 (the SCA "generally prohibits the provider . . . from knowingly divulging the contents of any communication . . . to any person other than the addressee or intended recipient"). As Facebook notes (at Reply 7-8), "Congress was not only concerned with government access to electronic communications, but *any* third-party access."

To be sure, Congress had a specific concern with protecting individual's electronic communications from governmental surveillance.[14] This concern is addressed by the specific provisions

[14] *See, e.g.*, S. Rep. No. 99-541, at 2 (1986) (the SCA seeks to strike "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies" by "ensur[ing] the continued vitality of the fourth amendment"); H.R. Rep. No. 99-647, at 18-19 (noting that "the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm").

limiting the circumstances under which a service provider may disclose content or other information to the government. *See, e.g.*, 18 U.S.C. § 2703 (requiring a subpoena, court order, or warrant, depending on the type of information sought). It does not follow from Congress's desire to limit the government's access to electronic communications, however, that Congress intended to allow unlimited disclosure to criminal defendants or other non-governmental individuals or entities. Rather, Congress struck the following careful balance between individual privacy rights and disclosure: with respect to *non-content information* such as subscriber information, service providers may voluntarily disclose "to any person other than a governmental entity," 18 U.S.C. § 2702(c)(6), while a governmental entity must generally obtain disclosure pursuant to a subpoena or court order. 18 U.S.C. § 2703(c).[15] Congress afforded much greater protection to the content of communications, however. Section 2702(b) does not include an exception that permits a service provider to disclose the contents of communications "to any person other than a

[15] The exception permitting disclosure "to any person other than a governmental entity" shows that Congress knew how to word the statute to permit non-governmental entities to obtain certain types of information.

governmental entity." *Compare* 18 U.S.C. §§ 2702(b)(1)-(9) *with* 18 U.S.C. § 2702(c)(6). Rather, the SCA permits the disclosure of the *contents* of communications to anyone who obtains the "lawful consent of the originator or addressee . . . or the subscriber," 18 U.S.C. § 2702(b)(3), and to the government pursuant to a warrant. 18 U.S.C. §§ 2703(a) and (b).[16]

Thus, contrary to appellee's suggestion (at 11), the SCA provides a "mechanism" for non-governmental litigants to obtain the disclosure of both the records and content of electronic communications. A non-governmental litigant can subpoena *non-content* information from the service provider under the provision permitting voluntary disclosure "to any person other than a governmental entity." 18 U.S.C. § 2702(c)(6). The non-governmental litigant who wishes to obtain *content* of communications may either (1) issue a subpoena to the account holder for the content of communications, or (2) obtain consent and issue a subpoena to the service provider under the provision permitting

[16] As Facebook notes (at 10), this appeal does not raise the question of whether the fact a communication or post is configured such that it is viewable by the public satisfies the "consent" exception in Section 2702(b)(3) because "the parties agreed that the subpoenaed records were not public" (Appx. 50).

disclosure of the contents of communications "with the lawful consent of the originator or an addressee or intended recipient . . . or the subscriber." 18 U.S.C. § 2702(b)(3).[17]

It would be illogical to conclude that Congress intended to allow non-governmental litigants to obtain the content of communications simply by issuing a subpoena to the service provider, while at the same time requiring that the government obtain a warrant supported by

---

[17] Appellee contends (at 18) that "it would be cumbersome, time-consuming, and likely ineffective to try to obtain social media information directly from account holders whose identities are known to the defense." However, there is no support for appellee's contention because, despite Facebook providing subscriber information in response to appellee's subpoenas and the fact that at least one of the relevant account holders appeared at trial and testified "about his social media activity without invoking the Fifth Amendment" (Facebook Reply at 9 n.4 and 10 n.5), appellee apparently has made no efforts to subpoena the account holders or obtain consent from the account holders. As Facebook explains (Appendix at 29), "Facebook and Instagram accountholders can go directly to their accounts to download or print content, or they can use the online tools provided by each service to obtain content and records." *See* Instagram Help Center, "How do I access or review my data on Instagram?," *available at* https://help.instagram.com/181231772500920; Facebook Help Center, "Accessing Your Facebook Data," *available at* http://www.facebook.com/help/405183566203254; *see also* John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU Sci. & Tech. L. Rev. 465, 473 (2011) ("The most effective methods of obtaining discovery of the contents of a party's social networking profile are propounding specific, well-tailored discovery requests to the party himself . . . .")

probable cause. Such a conclusion would run counter to the Supreme Court's recognition of individuals' privacy interests in their own electronically stored data and information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (extending the Fourth Amendment to require that the government obtain a warrant to obtain location data from cell-phone providers because "[t]hese location records hold for many Americans the privacies of life" and can be accessed "at practically no expense" "[w]ith just the click of a button") (internal quotation and citation omitted); *Riley v. California*, 134 S. Ct. 2473, 2485, 2489-91, 2493 (2014) (holding that the Fourth Amendment requires that police obtain a warrant before searching an individual's cell phone and recognizing the "vast quantities of personal information" stored on phones and cloud storage). Moreover, as Facebook notes (at 14 and Reply 1), appellee's suggested reading of the SCA "would violate people's right to privacy and potentially jeopardize their safety" by allowing defendants to obtain access to the contents of the electronic communications of a victim, witness, or even an individual who shares the same name as victim or witness. Rather, the framework established by the SCA balances individual privacy interests with the need to obtain evidence from service

providers and comports with the long-established methods by which the government and criminal defendants may obtain evidence.

The fact that the SCA permits the government to obtain the contents of communications pursuant to a warrant, but does not provide similar access to other non-governmental entities including criminal defendants, is not surprising. Within the criminal justice system, other statutes and rules also provide for one-sided access to the government. For example, the search warrant provisions of Federal Rule of Criminal Procedure 41(b) and the wiretap application provisions of 18 U.S.C. § 2516(1) both provide a means for the government to obtain evidence without a mechanism for defendants to do so. Similarly, only the government, not the defendant, has the ability to utilize a grand jury to gather evidence related to the commission of a criminal offense. This framework is consistent with the presumption of innocence, which places the burden of proof beyond a reasonable doubt on the government and mandates that a defendant does not have to prove himself innocent.[18]

---

[18] Appellee argues (at 13-15) that this "interpretation of the SCA . . . implicitly curtains criminal defendants' Rule 17(c) subpoena power" and that such "[r]epeals by implication are not favored." To the extent that the SCA limited the type of information a defendant may obtain from a

II. A Contrary Reading of the SCA is Not Constitutionally Mandated.

Despite the plain language of the SCA, appellee contends (at 17-18) that this Court should adopt a reading of the SCA that "leaves in place criminal defendants' constitutionally grounded right to compel favorable and material evidence for use at trial" because the contrary interpretation advanced by Facebook and the United States would "raise serious questions about [the SCA's] validity under the Fifth and Sixth Amendments." This argument is without merit.

---

particular source, a criminal defendant's Rule 17(c) subpoena power was not "repealed." Moreover, as Facebook notes (at Reply 5), the Supreme Court rejected this argument in *Baldrige v. Shapiro*, 455 U.S. 345 (1982) (holding that the "unambiguous language of the confidentiality provisions" in a statute directing the Department of Commerce not to "permit anyone" to examine raw census data precluded discovery of that data via subpoena). *See also Cazorla v. Koch Foods of Mississippi, L.L.C.*, 838 F.3d 540, 551 (5th Cir. 2016) ("as a purely textual matter, it is unclear why a provision broadly barring *any* 'disclosure' would have to specify 'including in discovery' in order to have effect"); *In re England*, 375 F.3d 1169, 1177-78 (D.C. Cir. 2004) (holding that federal statute prohibiting disclosure "to any person" extended to all contexts, including judicial proceedings even when not specifically mentioned by the statute). Appellee's reliance (at 14) on *Freeman v. Seligson*, 405 F.2d 1326 (D.C. Cir. 1968), is misplaced. *Freeman* dealt with a statute that barred the "publish[ing]" of certain records, not a statute like the SCA that prohibited the disclosure of information or records (*see* Facebook Reply at 6).

As an initial matter, "the canon of constitutional avoidance 'is an interpretive tool, counseling that ambiguous statutory language be construed to avoid serious constitutional doubts.'" *Mack v. United States*, 6 A.3d 1224, 1233-34 (D.C. 2010) (quoting *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009)). "It is intended as 'a means of giving effect to congressional intent, not of subverting it.'" *Id.* (quoting *Clark v. Martinez*, 543 U.S. 371, 382 (2005)). As this Court has explained, "[w]e do not needlessly pit a statute against the Constitution." *Gay Rights Coalition of Georgetown Univ. Law Center v. Georgetown Univ.*, 536 A.2d 1, 16 (D.C. 1987) (en banc) (plurality opinion). Here, the SCA's broad prohibition against disclosure is not ambiguous. *See supra* Section I. The canon of constitutional avoidance thus plays no role in this Court's interpretation of the SCA. But, even assuming *arguendo* that there was more than one plausible interpretation of the SCA, the interpretation advanced by Facebook and the United States does not "provoke a confrontation with the Constitution." *Mack*, 6 A.3d at 1234.[19]

[19] Appellee bears a heavy burden in persuading this Court that the SCA's broad prohibition against disclosure is unconstitutional – Acts of Congress receive a "strong presumption of constitutionality." *United States v. Watson*, 423 U.S. 411, 416 (1976); *see also Mistretta v. United*

"Whether rooted directly in the Due Process Clause . . ., or in the Compulsory Process or Confrontation clauses of the Sixth Amendment, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *Crane v. Kentucky*, 476 U.S. 683, 690 (1986) (internal quotations and citations omitted). However, as both the Supreme Court and this Court have recognized, "the constitutional right to present a defense is not absolute and does not allow the defendant to introduce all evidence that may be helpful." *Blackson v. United States*, 979 A.2d 1, 10 n.9 (D.C. 2009) (citing *Crane*, 476 U.S. at 690); *see also United States v. Scheffer*, 523 U.S. 303, 308 (1998) ("[S]tate and federal rulemakers have broad latitude under the Constitution to establish rules excluding evidence from criminal trials. Such rules do not abridge an accused's right to present a defense so long as they are not 'arbitrary' or 'disproportionate to the purposes they are designed to serve.'") (quoting *Rock v. Arkansas*, 483 U.S. 44, 56 (1998)).

For example, "a defendant's right to cross-examination is not unlimited," *Coles v. United States*, 808 A.2d 485, 489 (D.C. 2002), as the

---

States, 488 U.S. 361, 384 (1989) (a court may invalidate an Act of Congress for only "the most compelling constitutional reasons").

Confrontation Clause "guarantees an opportunity for effective cross-examination, not cross-examination that is effective in whatever way, and to whatever extent, the defense may wish," *Hart v. United States*, 863 A.2d 866, 871 (D.C. 2004) (citing *Delaware v. Fensterer*, 474 U.S. 15, 20 (1985)). Similarly, although the Compulsory Process Clause "guarantees a criminal defendant a fair and meaningful opportunity to present a complete defense," *McDonald v. United States*, 904 A.2d 377, 380 (D.C. 2006), "it is not unlimited," *Grady v. United States*, 180 A.3d 652, 657 (D.C. 2018). A defendant's right to produce relevant evidence may "bow to accommodate other legitimate interests in the criminal trial process." *Chambers v. Mississippi*, 410 U.S. 284, 295 (1973); *see also Taylor v. Illinois*, 484 U.S. 400, 410 (1988) ("The accused does not have an unfettered right to offer testimony that is incompetent, privileged, or otherwise inadmissible under the rules of evidence."). To establish a violation of the right to compulsory process, a fair trial or due process, a defendant "must show a denial of fundamental fairness: 'In order to declare a denial of [fundamental fairness] we must find that the absence of that fairness fatally infected the trial; the acts complained of must be of such quality as necessarily prevents a fair trial.'" *Richmond v. Embry*,

122 F.3d 866, 872 (10th Cir. 1997) (quoting *United States v. Valenzuela-Bernal*, 458 U.S. 858, 872 (1982)).

Applying these precepts, courts have upheld categorical prohibitions on a defendant's right to obtain or introduce certain types of evidence. *See, e.g.*, *Scheffer*, 523 U.S. at 317 (upholding rule prohibiting defendant from introducing polygraph evidence, finding that the rule "serves several legitimate interests in the criminal trial process," "is neither arbitrary nor disproportionate in promoting these ends," and does not "implicate a sufficiently weighty interest of the defendant to raise a constitutional concern under our precedents"); *United States v. Stewart*, 433 F.3d 273, 310-11 (2d Cir. 2006) (upholding procedural and evidentiary rules that limit the introduction of expert testimony on the basis that the rules serve "'legitimate interests in the criminal trial process,' and the resulting restrictions on the presentation of evidence are neither arbitrary nor disproportionate to those purposes" (quoting *Rock*, 483 U.S. at 55); *Commonwealth v. Aultman*, 602 A.2d 1290, 1297 (Pa. 1992) (defendant was not entitled to disclosure of victim's records held by a rape crisis center where those records were protected by an absolute statutory privilege; "the existence of a statutory privilege is an

indication that the legislature acknowledges the significance of a particular interest and has chosen to protect that interest"); *cf. Minder v. Georgia*, 183 U.S. 559, 562 (1902) (defendant was not deprived of "due process of law, on account of not having the benefit of the testimony of witnesses who are beyond the jurisdiction of the court, when the lawmaking power of the state is powerless to make any provision which would result in the compulsory attendance of the witnesses, and the use of depositions in such cases is directly contrary to the usages, customs, and principles of the common law").[20]

Like these limitations on a defendant's right to obtain or introduce evidence, the SCA's general prohibition against the disclosure of "the *contents* of a communication" by a service provider to "any person or entity" serves a "legitimate interest" – protecting the privacy of stored email and other stored electronic communications – and is "neither arbitrary nor disproportionate in promoting these ends." *Scheffer*, 523 U.S. at 317. This is because the SCA only prohibits unconsented-to

[20] The issue presented in *Minder* has since been addressed by a uniform act to secure the presence of witnesses adopted by the vast majority of states.

disclosure by a service provider, not by others with access to the communications, such as the originator or recipients. Service providers may disclose the content "with the lawful consent of" the originator, an addressee or recipient, or subscriber and of non-content to "any person other than a governmental entity." 18 U.S.C. §§ 2702(b)(3) and (c)(6). Accordingly, the SCA's prohibition against the disclosure of "the contents of a communication" by a service provider, 18 U.S.C. §§ 2702(a)(1) and (2), does not "implicate a sufficiently weighty interest of the defendant to raise a constitutional concern," *Scheffer*, 523 U.S. at 317.[21]

Important to this conclusion is a recognition that the SCA is not a categorical prohibition on a defendant's ability to obtain and introduce the content of electronic communications. Rather, it limits the methods a defendant can use to obtain evidence by prohibiting *one source* – the service provider – from disclosing the content of communications absent consent or another applicable exception. This type of limitation on the

[21] We note that when the government obtains the content of communications under Section 2703 pursuant to a warrant, the government's discovery obligations might require it to disclose some or all of that information to the defense. *See, e.g.*, Super. Ct. R. Crim. P. 16; *Giglio v. United States*, 405 U.S. 150 (1972); *Brady v. Maryland*, 373 U.S. 83 (1963).

methods and sources a defendant can use to obtain evidence is routine. *See, e.g.*, 18 U.S.C. § 2510, *et seq.* (defendant may not obtain evidence of a conversation by wiretapping or otherwise unlawfully recording it, but no limitation on ability to obtain evidence from a party to the conversation); *United States v. Recognition Equip. Inc.*, 720 F. Supp. 13, 14 (D.D.C. 1989) (criminal defendant cannot obtain third-party tax returns from U.S. government unless they are in the U.S. attorney's possession).[22]

Indeed, where, as here, a defendant has an alternative means of obtaining evidence, courts routinely uphold privileges and non-disclosure provisions in the face of constitutional challenges. *See, e.g.*, *Anderson v. United States*, 607 A.2d 490, 497-99 (D.C. 1992) (upholding government's qualified privilege to withhold location of observation post against claim of denial of accused's right to confront and cross-examine prosecution witnesses where defendant did not show that there were "no alternative means of getting at the same point"); *United States v. Poindexter*, 727 F.

[22] Similarly, criminal unlawful entry and burglary statutes prohibit a defendant from entering a witness's home to gather evidence absent consent; rather a defendant must seek the evidence via consent or pursuant to a subpoena *duces tecum*.

Supp. 1501, 1509 (D.D.C. 1989) (upholding executive privilege because the President "need not produce these answers because they are available from another source"); *State v. Boiardo*, 414 A.2d 14, 21 (N.J. 1980) ("Legislature clearly contemplated . . . a balancing of the interests served by compulsory process in criminal cases against those served by the protection of a newsperson's confidential sources and information, once the strengths of the competing interests had been demonstrated through a showing of relevance, materiality and necessity to the defense, in addition to nonavailability through a less intrusive source"); *cf. United States v. Prantil*, 756 F.2d 759, 763 (9th Cir. 1985) ("We recognize that a defendant has an obligation to exhaust other available sources of evidence before a court should sustain a defendant's efforts to call a participating prosecutor as a witness.").

Thus, at a minimum, absent a showing that there are no alternative means of obtaining the content of the communications appellee seeks, there is no serious constitutional question presented here. Because appellee has not made any attempt to obtain the communications from the sender, recipient, or account holder, even after receiving subscriber information from Facebook and having the opportunity to question the

Facebook account holder (a government witness) at trial regarding his social media activity, appellee cannot show that there are no alternative means of obtaining the content he seeks (Facebook Mot. at 8-9; Facebook Reply at 10 n.5).[23]

---

[23] Super. Ct. Crim. R. 17(c) requires that a party seeking a subpoena *duces tecum* demonstrate: (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable . . . by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production . . . and (4) that the application is made in good faith and is not intended as a 'fishing expedition.'" *Tyer v. United States*, 912 A.2d 1150, 1156 (D.C. 2006).

Because the trial court based its conclusion that the requested subpoenas satisfied the requirements of Rule 17(c) on *ex parte* representations by appellee, neither Facebook nor the United States has the ability to fully assess the trial court's conclusions. However, based on the record as it stands, it is difficult to conceive of a proffer that would demonstrate that subpoenas that seek "any and all information" for a period of over three years from dozens of Facebook accounts associated with a particular name and two Instagram accounts meet this standard, especially where appellee has not made any attempt to limit the scope of the subpoenas after receiving subscriber information from Facebook. *See, e.g., In re Grand Jury Subpoena*, 828 F.3d 1083 (9th Cir. 2016) (holding that subpoena for the contents of former governor's email account was overly broad); *Margoles v. United States*, 402 F.2d 450 (7th Cir. 1968) (subpoena for any and all equipment logs relating to electronic eavesdropping equipment during one-and-a-half year period was too broad); *United States v. Wilmington Trust Corp.*, 321 F.R.D. 100 (D. Del. 2017) (subpoenas seeking broad array of internal Federal Reserve documents did not comport with limited purpose of rule governing subpoenas for production of documents – to allow defendants access to "identified evidence"). What is clear, however, is that appellee cannot show that the

Appellee's arguments (at 18-19) to the contrary are unpersuasive. In response to a subpoena *duces tecum*, Facebook and Instagram accountholders can go directly to their accounts to download or print content, or they can use the online tools provided by each service to obtain content. *See supra* note 14. If they were unable to access content responsive to the subpoena, the trial court could, in appropriate circumstances, require the account-holder to consent to disclosure of the content by the service provider. *See Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008). If an account-holder refused to produce content in response to a subpoena, the defendant could seek to compel compliance or move the court to hold the account-holder in contempt of court. *See*

---

materials he seeks "are not otherwise procurable . . . by exercise of due diligence" because he has not made any attempt to obtain the communications from the sender, recipient, or account holder.

For these same reasons, appellee cannot show the SCA's prohibition on disclosure of the contents of communications by service providers "implicate[s] a sufficiently weighty interest of the defendant to raise a constitutional concern," *Scheffer*, 523 U.S. at 317. Courts often engage in a case-by-case balancing of the defendant's need for the privileged or statutorily proscribed information and the interest served by the privilege or statute. Here, the breadth of the defendant's request and the fact that the defendant did not seek the information either with more specificity or from the account holder itself suggests that any balance favors the legitimate interest in protecting individuals' privacy.

Super. Ct. R. Crim. P. 17(g) ("Failure by any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of the court."). The trial court could also preclude a witness from testifying or limit the witness's testimony if a witness refused to comply with such a subpoena, *see United States v. Nobles*, 422 U.S. 225, 241 (1975); craft an instruction similar to the missing evidence instruction given when the government fails to produce evidence, *see generally Tyer v. United States*, 912 A.2d 1150, 1164-66 (D.C. 2006); or, in appropriate cases, permit the defense to comment in closing argument on the absence of the evidence, *see Greer v. United States*, 697 A.2d 1207, 1210 (D.C. 1997). The government, faced with these possibilities, could also elect to obtain the content directly from the service-provider pursuant to 18 U.S.C. § 2703. What a court should not do is order Facebook or another service provider to violate federal law.[24]

---

[24] As Facebook notes (at Reply 9 n.4), appellee has not pressed on appeal the argument raised below and relied on by the trial court that if confronted with a subpoena, the subscriber might invoke the Fifth Amendment. This is understandable given that this Court has a long-recognized procedure for addressing the "tension between the accused's Sixth Amendment right of compulsory process to obtain witnesses in aid of a defense, and a witness' Fifth Amendment right against self-incrimination. *See Carter v. United States*, 684 A.2d 331, 334-35, 341, 343

CONCLUSION

WHEREFORE, the government respectfully submits that the judgment of the Superior Court should be reversed.

Respectfully submitted,

JESSIE K. LIU
United States Attorney

ELIZABETH TROSMAN
Assistant United States Attorney

/s/
LAUREN R. BATES
D.C. Bar #975461
Assistant United States Attorney
555 Fourth Street, NW, Room 8104
Washington, D.C. 20530
Lauren.Bates@usdoj.gov
(202) 252-6829

(D.C. 1996) (en banc) (where "the testimony of a crucial defense witness" is "(a) material, (b) exculpatory, (c) not cumulative, and (d) unobtainable from any other source," and "the government does not submit to the court a reasonable basis for not affording use immunity to the crucial witness in order to procure the vital defense testimony, then the trial court would be justified in informing the government that it must make the choice between dismissal of the indictment or some other *commensurate remedy* which the court may fashion on Sixth Amendment and due process grounds, or affording use immunity to the crucial defense witness involved"). Thus, to the extent the trial court relied on the speculative possibility that the account holder "could" assert his Fifth Amendment privilege against self-incrimination in finding the information sought by appellee not "procurable in other ways," the trial court erred by not following the *Carter* procedures. 684 A.2d at 343 (Appx. at 55).

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that I have caused the foregoing Brief for the United States to be served by email on counsel for appellant, Joshua Lipshutz, Michael Holecek, Thomas Cochrane, John Roche, and Hayley Berlin, and counsel for appellee, Samia Fam, Jaclyn Frankfurt, and Mikel-Meredith Weidman, on this 2nd day of October, 2018.

/s/
LAUREN R. BATES
Assistant United States Attorney

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

PROOF OF SERVICE

I, Thomas Cochrane, declare as follows:

I am a citizen of the United States and employed in San Francisco County, California; I am over the age of eighteen years, and not a party to the within action; my business address is 333 South Grand Ave., Los Angeles, CA 94105-0921. On May 8, 2020, I served the within documents:

PETITIONER'S RULE 8.520(d) SUPPLEMENTAL BRIEF REGARDING *FACEBOOK, INC. V. WINT* (D.C. 2019) AND *FACEBOOK, INC. V. SUPERIOR COURT* ("*HUNTER III*") (2020)

On the parties stated below, by the following means of service:

SEE ATTACHED SERVICE LIST

☑ **BY UNITED STATES MAIL**: I caused a true copy to be placed in a sealed envelope or package addressed to the persons as indicated above, on the above-mentioned date, and placed the envelope for collection and mailing, following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited with the U.S. Postal Service in the ordinary course of business in a sealed envelope with postage fully prepaid. I am aware that on motion of party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing set forth in this declaration.

I am a resident or employed in the county where the mailing occurred. The envelope or package was placed in the mail at San Francisco, California.

☑ I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on May 8, 2020 at Los Angeles, California.

/s/ Thomas Cochrane
Thomas Cochrane

SERVICE LIST FOR *Facebook, Inc. v. Superior Court of San Diego*
CALIFORNIA SUPREME COURT CASE NO. S245203

Superior Court of San Diego County: Respondent	Superior Court of San Diego County Central – Downtown Courthouse P.O. Box 122724 San Diego, CA 92112
Court of Appeal, Fourth District, Div. 1	Clerk of the Court Court of Appeal, Fourth District, Div. 1 750 B Street, Suite 300 San Diego, CA 92101
Lance Touchstone: Real Party in Interest	Katherine Ilse Tesch Office of the Alternate Public Defender 450 B Street, Suite 1200 San Diego, CA 92101
San Diego County District Attorney: Intervenor	Summer Stephan, District Attorney Mark Amador, Deputy District Attorney Linh Lam, Deputy District Attorney Karl Husoe, Deputy District Attorney 330 W. Broadway, Suite 860 San Diego, CA 92101
Apple Inc., Google Inc., Oath Inc., Twitter Inc., and California Chamber of Commerce: Attorneys for Amici Curiae	Jeremy B. Rosen Stanley H. Chen Horvitz & Levy LLP 3601 West Olive Avenue, 8th Floor Burbank, California 91505-4681
California Public Defenders Association and Public Defender of Ventura County: Attorneys for Amici Curiae	Todd Howeth, Public Defender Michael C. McMahon, Senior Deputy Office of the Ventura County Public Defender 800 S. Victoria Avenue, Suite 207 Ventura, CA 93009
California Attorneys for Criminal Justice: Attorneys for Amici Curiae	Donald E. Landis The Law Office of Donald E. Landis, Jr. P.O. Box 221278 Carmel, CA 93922

California Attorneys for Criminal Justice: Attorneys for Amici Curiae	Stephen Kerr Dunkle Sanger Swysen & Dunkle 125 East De La Guerra Street, Suite 102 Santa Barbara, CA 93101
California Attorneys for Criminal Justice: Attorneys for Amici Curiae	John T. Philipsborn Law Offices of J.T. Philipsborn Civic Center Building 507 Polk Street, Suite 350 San Francisco, CA 94102
San Francisco Public Defender's Office: Attorneys for Amici Curiae	Jeff Adachi, Public Defender, City and County of San Francisco Matt Gonzalez, Chief Attorney Dorothy Bischoff, Deputy Public Defender 555 Seventh Street San Francisco, CA 94103

STATE OF CALIFORNIA
Supreme Court of California

PROOF OF SERVICE

STATE OF CALIFORNIA
Supreme Court of California

Case Name: **FACEBOOK v. S.C. (TOUCHSTONE)**
Case Number: **S245203**
Lower Court Case Number: **D072171**

1. At the time of service I was at least 18 years of age and not a party to this legal action.

2. My email address used to e-serve: **tcochrane@gibsondunn.com**

3. I served by email a copy of the following document(s) indicated below:

Title(s) of papers e-served:

Filing Type	Document Title
BRIEF	Touchstone_Supp Br re Hunter

Service Recipients:

Person Served	Email Address	Type	Date / Time
John Philipsborn Law Offices of J.T. Philipsborn 83944	JPhilipsbo@aol.com	e-Serve	5/8/2020 2:53:41 PM
Soolean Choy Gibson, Dunn & Crutcher LLP 318750	schoy@gibsondunn.com	e-Serve	5/8/2020 2:53:41 PM
Donald Landis The Law Office of Donald E. Landis, Jr. 149006	don@donlandislaw.com	e-Serve	5/8/2020 2:53:41 PM
Stephen Dunkle Sanger Swysen & Dunkle 227136	sdunkle@sangerswysen.com	e-Serve	5/8/2020 2:53:41 PM
Eric Boorstin Horvitz & Levy LLP 253724	eboorstin@horvitzlevy.com	e-Serve	5/8/2020 2:53:41 PM
James Snell Perkins Coie LLP 173070	JSnell@perkinscoie.com	e-Serve	5/8/2020 2:53:41 PM
Karl Husoe Office of the District Attorney 261097	karl.husoe@sdcda.org	e-Serve	5/8/2020 2:53:41 PM
Michael Mcmahon Office of the Ventura County Public Defender 71909	michael.mcmahon@ventura.org	e-Serve	5/8/2020 2:53:41 PM
Dorothy Bischoff Office of the Public Defender 142129	dorothy.bischoff@sfgov.org	e-Serve	5/8/2020 2:53:41 PM
Joshua Lipshutz Gibson, Dunn & Crutcher LLP	jslipshutz@gmail.com	e-Serve	5/8/2020 2:53:41 PM

Todd Howeth Todd W. Howeth, Ventura County Public Defender 110714	todd.howeth@ventura.org	e-Serve	5/8/2020 2:53:41 PM
Katherine Tesch Office of the Alternate Public Defender 284107	Kate.Tesch@sdcounty.ca.gov	e-Serve	5/8/2020 2:53:41 PM
Donald Landis The Law Office of Donald E. Landis, Jr. 149006	admin@donlandislaw.com	e-Serve	5/8/2020 2:53:41 PM
Michael Holecek Gibson Dunn & Crutcher, LLP	mholecek@gibsondunn.com	e-Serve	5/8/2020 2:53:41 PM
Christian Lee Perkins Coie LLP 301671	clee@perkinscoie.com	e-Serve	5/8/2020 2:53:41 PM
Raeann Diamond Horvitz & Levy LLP	rdiamond@horvitzlevy.com	e-Serve	5/8/2020 2:53:41 PM
Stanley Chen Horvitz & Levy LLP 302429	schen@horvitzlevy.com	e-Serve	5/8/2020 2:53:41 PM
Thomas Cochrane Gibson, Dunn & Crutcher LLP 318635	tcochrane@gibsondunn.com	e-Serve	5/8/2020 2:53:41 PM

This proof of service was automatically created, submitted and signed on my behalf through my agreements with TrueFiling and its contents are true to the best of my information, knowledge, and belief.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

5/8/2020

Date

/s/Thomas Cochrane

Signature

Cochrane, Thomas (318635)

Last Name, First Name (PNum)

Gibson, Dunn & Crutcher LLP

Law Firm