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 RESPONSE TO BRIEF OF INTERVENOR SAN DIEGO COUNTY DISTRICT ATTORNEY

---

**PERKINS COIE LLP**
JAMES G. SNELL, SBN 173070
jsnell@perkinscoie.com
CHRISTIAN LEE, SBN 301671
clee@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304
tel: 650.838.4300, fax: 650.838.4350

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

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

*Attorneys for Petitioner Facebook, Inc.*

No. S245203

**IN THE SUPREME COURT OF THE STATE OF CALIFORNIA**

---

**FACEBOOK, INC.,**
*Petitioner,*

v.

**THE SUPERIOR COURT OF SAN DIEGO COUNTY,**
*Respondent;*

**LANCE TOUCHSTONE,**
*Real Party in Interest.*

---

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

---

# PETITIONER'S RESPONSE TO BRIEF OF INTERVENOR SAN DIEGO COUNTY DISTRICT ATTORNEY

---


**PERKINS COIE LLP**
JAMES G. SNELL, SBN 173070
jsnell@perkinscoie.com
CHRISTIAN LEE, SBN 301671
clee@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304
tel: 650.838.4300, fax: 650.838.4350

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

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

*Attorneys for Petitioner Facebook, Inc.*

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

Page(s)

### Cases

**TABLE OF AUTHORITIES** *(continued)*

Page(s)

## TABLE OF AUTHORITIES *(continued)*



### Statutes



### Other Authorities

## TABLE OF AUTHORITIES *(continued)*

Page(s)

## I. Introduction

The San Diego County District Attorney's ("DA") brief in intervention far exceeds the single issue on which they sought to intervene and that this Court permitted intervention: "whether the trial court can compel the District Attorney to seek a search warrant for records held by Facebook." (Mot. to Intervene at p. 1.) This Court should disregard all of the DA's other arguments because they are not properly before this Court.

With respect to the narrow issue on which the DA obtained leave, Facebook agrees with many of the points raised by the DA.[1] However, while Facebook agrees that a search warrant cannot issue without probable cause, nothing in the statutory framework prohibits a court from directing the People to issue a warrant where probable cause *does* exist. A warrant sought solely for impeachment purposes would not satisfy the Fourth Amendment, but one that sought to demonstrate evidence that a crime has been committed or that someone else committed a crime might, and would be entirely consistent with a prosecutor's solemn duty to seek justice by protecting the innocent and pursuing appropriate criminal charges only where justified.

If the Court elects to address the DA's novel and unsupported arguments that the Stored Communications Act ("SCA") does not protect most modern electronic communications content, it should reject them. The SCA applies to "electronic communications service" ("ECS") and

---

[1] Because Facebook agrees that Marsy's Law provides an independent basis to object to disclosure of witness/victim records, that Facebook is not part of the prosecution, and that Touchstone lacks a constitutional right to compel third parties to disclose content, Facebook does not respond to those arguments.

"remote computing service" ("RCS") providers, and Facebook qualifies as both.

Facebook clearly allows people to send and receive communications, and to store communications for future access and sharing, putting its services squarely within the definition of an ECS. Facebook is also an RCS because it provides storage and processing services. That Facebook can screen communications and support its free services by advertising does not remove SCA protection from those communications: Facebook's permissions to access stored communications are granted in connection with providing its storage and computer processing services. And while the DA refers to Facebook's use of "artificial intelligence" and "targeted advertising" as examples of why the SCA's privacy protections should not apply to Facebook accounts, these and other uses are part and parcel of the computer processing services offered by Facebook.

## II. Argument

### A. Courts can order the prosecution to assist the defense to the extent permitted by law.

As noted above, this Court granted the DA leave to intervene on a single narrow question: whether the trial court can compel the prosecution to seek a search warrant. (Mot. to Intervene at p. 1.) Facebook takes no position on whether a trial court may order the prosecution to issue a search warrant, but notes that the trial court has wide discretion to control the proceedings before it and has numerous ways to compel the prosecution to assist the defendant to obtain necessary evidence or to fashion ways to address the lack of necessary evidence. (See Ans. Br. at p. 36.) But, the DA draws the wrong conclusion—that courts can *never* compel the DA to

obtain a warrant—from the accurate statement that a search warrant cannot issue without an affidavit establishing probable cause.

### 1. A trial court does not violate the separation of powers doctrine by ensuring that the prosecution abides by its constitutional duties.

"A trial court has inherent as well as statutory discretion to control the proceedings to ensure the efficacious administration of justice." (*Juror Number One v. Superior Court* (2012) 206 Cal.App.4th 854, 866, quoting *People v. Cox* (1991) 53 Cal.3d 618, 700.) This discretion includes the authority to order the prosecution to abide by its constitutional duties, such as the duty to investigate and produce to the defense information in their possession that is favorable to the defendant. (See *Kyles v. Whitley* (1995) 514 U.S. 419, 437 ["[T]he individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case."].) *Brady v. Maryland* (1963) 373 U.S. 83, 87, restricts the prosecution from suppressing evidence and does not "provide the accused a right to criminal discovery," but also requires the prosecution to assist the defense when the evidence is available only to the prosecution and is otherwise permitted by law. (*People v. Morrison* (2004) 34 Cal.4th 698, 715; cf. *Evans v. Superior Court* (1974) 11 Cal.3d 617, 625 ["Should petitioner be denied his right of discovery the net effect would be the same as if existing evidence were intentionally suppressed."].)

Applying these principles, trial courts have ***required*** the prosecution to affirmatively assist the defense in discovery in a variety of circumstances. (See, e.g., *id.* [compelling the prosecution to order a pretrial lineup if a defendant needs one to pursue a false-identification defense]; *People v. Goliday* (1973) 8 Cal.3d 771, 779-782 [requiring prosecution to assist defense to locate witnesses because "the People's duty included not

only disclosure but also action to obtain information"]; *United States v. Stein* (S.D.N.Y. 2007) 488 F.Supp.2d 350, 363–364 [holding that government was obliged to obtain documents from a third-party that were material to the defense]; *United States v. Kilroy* (E.D. Wis. 1981) 523 F.Supp. 206, 215 [ordering government to use its "best efforts" to obtain from cooperating witness documents that defendant claimed were material to defense].)

In addition to ordering the prosecution to affirmatively assist the defendant, the trial court can also incentivize the prosecution to do so by imposing the appropriate sanction against the prosecution if the prosecution's inaction results in the defendant not having what he or she needs to mount a defense or proceed to trial. (See, e.g., *Kling v. Superior Court* (2010) 50 Cal.4th 1068, 1078 [noting that "a third party's refusal to produce documents requested by the defense can potentially result in sanctions being applied against the People"]; *People v. Brophy* (1992) 5 Cal.App.4th 932, 937 ["Dismissal is proper as a sanction for refusing to comply with a discovery order when the effect of such refusal is to deny defendant's right to due process."]; *Dep't of Corr. v. Superior Court* (1988) 199 Cal.App.3d 1087, 1093 ["Discovery proceedings involving third parties can potentially result in sanctions being applied against the People should the third party refuse to produce the documents requested."]; *Dell M. v. Superior Court* (1977) 70 Cal.App.3d 782 [issuing evidentiary sanction against prosecution when third party refused to produce records on privilege grounds].)

In short, the trial court has numerous tools to ensure that the prosecution upholds its constitutional obligations and for the defendant to have a fair trial, none of which violates the separation of powers doctrine and none of which causes Facebook to violate federal law.

### 2. A warrant must be supported by probable cause, which can include evidence helpful to defendant.

The DA correctly notes that a search warrant must be supported by probable cause (see Pen. Code, § 1546.1, subds. (a), (b); *United States v. Warshak* (6th Cir. 2010) 631 F.Supp.3d 266, 288) and must relate to "gathering of evidence that a crime has occurred or is about to occur" (Intervenor's Br. at p. 17), but then makes the unsupported inference that probable cause can never be based on "evidence which could be used to impeach a witness at trial, or for evidence to support an affirmative defense[.]" (Intervenor's Br. at p. 19.) As far as Facebook is aware, there is no support in the law for the DA's conclusion.

"[T]he traditional standard for review of an issuing magistrate's probable cause determination has been that so long as the magistrate had a 'substantial basis for ... conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." (*Illinois v. Gates* (1983) 462 U.S. 213, 236.) This evidence of wrongdoing need not be restricted to wrongdoing by the defendant. For example, if the prosecution had probable cause to believe that the charged crime was committed by someone other than the defendant, then the evidence sought would be both evidence of the other's crime and exculpatory evidence for the defendant.

The DA concludes that "[c]learly . . . the victim . . . [did not] commit[] a crime here, and no such required probable cause exists to support the issuance of a warrant." (Intervenor's Br. at p. 18.) Facebook does not take a position on the merits of the allegations, but notes that Touchstone's claims of self-defense may suggest there is evidence of a crime committed by another person. (See Facebook's Appendix of Exhibits to the Court of Appeal ("App'x") at p. 75.) As a non-party, Facebook does not have familiarity with the factual disputes in this case,

which are best left to the parties and the court and which is within "the broad discretion of the magistrate or trial judge" to consider the materiality of the information sought and availability of the evidence to the defense. (*Evans*, *supra*, 11 Cal.3d at p. 625.)

## B. The Court should decline to consider the People's SCA argument, which exceeds their right to permissive intervention.

The DA sought to intervene to address the issue in which the People have "a direct and immediate interest . . . namely, whether the trial court can compel the District Attorney to seek a search warrant for records held by Facebook." (Mot. to Intervene at p. 6.) The Court granted that limited request. The DA's brief, however, goes well beyond the narrow question of whether the court can compel a District Attorney to seek a search warrant. Indeed, the majority of the DA's brief—pages 4 through 15—addresses topics completely unrelated to the issue.

The DA obtained leave to intervene under Code of Civil Procedure section 387(d)(2), which allows intervention only when "(1) the intervenor has a direct and immediate interest in the litigation, (2) the intervention will not enlarge the issues in the case, and (3) the reasons for intervention outweigh opposition by existing parties." (*Hinton v. Beck* (2009) 176 Cal.App.4th 1378, 1383.)

The DA's motion for leave addressed only the first prong of this test: whether the DA had a direct and immediate interest in the litigation, which exists where the outcome "adds or detracts from [the DA's] legal rights without reference to rights and duties not involved in the litigation." (*Continental Vinyl Products Corp. v. Mead* (1972) 27 Cal.App.3d 543, 549.)

With respect to this prong, the DA noted "[o]ur office will be compelled to use its resources to seek a search warrant for the requested communications should this court find that the trial court has the inherent authority to order the District Attorney do so." (Mot. to Intervene at p. 3.) The DA also claimed it was not in Touchstone's or Facebook's interest to reveal statutory prohibitions on obtaining a search warrant without probable cause. (*Id.*) The DA did not address the second or third prongs of the test for intervention.

Facebook did not object to intervention because the DA's request was limited to a discrete question this Court asked the parties to address through supplemental briefing. (Mot. to Intervene at p. 1.) Touchstone also did not object, presumably for the same reasons.

But the brief the DA filed goes far beyond the narrow issue regarding a Court directing the District Attorney to obtain a search warrant, and instead seeks to enlarge the issues in this case. Indeed, this case was fully briefed prior to this Court's decision in *Facebook v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245, and ensuing order for supplemental briefing on the impact of *Hunter*. And as the DA concedes, Touchstone never disputed that Facebook's services are covered by the SCA. (Intervenor's Br., 5 [noting that Touchstone has "fail[e]d to contest [this issue] in the proceedings below."]) Moreover, in its motion for leave, the DA assumed the SCA applied. (Mot. to Intervene at p. 4.)[2]

---

[2] Amicus curiae California Attorneys for Criminal Justice ("CACJ") likewise takes the position that the SCA applies to the communications at issue in this case. (See CACJ Suppl. Br. at p. 8 ["In this *Touchstone* litigation, the Court is presented with a focused discussion of the dilemmas facing the accused in a criminal case in California where electronic communications covered by the SCA are at issue"].)

The DA now seeks to enlarge the issues in this case by injecting the threshold question of whether the SCA applies to Facebook. The DA presents no support or justification for adding another issue not raised in the request to intervene and implicitly admits that resolution of this new issue is irrelevant to the issue on which this court granted its motion to intervene. Indeed, the DA acknowledges that regardless of the SCA, California law still requires the People to obtain a warrant based on probable cause to acquire communications from Facebook (Intervenor's Br. at p. 18; Pen. Code, § 1546.1, subd. (b)), and that Marsy's Law, Cal. Const., art. I, § 28, subd. (c), par. 1, may independently prohibit Touchstone from obtaining the records he seeks. (Intervenor's Br. at p. 23.)

There is no reason to expand the issues in this case. Resolution of this manufactured issue changes nothing for the DA.[3] Facebook's concerns (outlined below) about injecting a new issue at this late date outweighs the DA's interest in extending the scope of its intervention. The Court should therefore strike pages 1-19, 22-34 of the DA's brief and disregard its novel SCA arguments.[4]

---

[3] The DA may want to revise the SCA to allow Facebook voluntarily to disclose communications to law enforcement, but that issue is a question for the legislative branch, not the judiciary. It also not properly before this Court, as it is not "a direct and immediate interest" raised by this case. But even if this Court were to change the law in California, providers would still be unable to disclose content to law enforcement voluntarily without risking a violation of federal law because the Ninth Circuit has defined "electronic storage" broadly to include the kind of storage at issue. (See *Theofel v. Farey Jones* (9th Cir. 2004) 359 F. Supp. 2d 1059, 1075; *infra* at p. 7.)

[4] For the same reasons, the Court should also deny the DA's concurrently-filed Motion to Augment the Record, which is not a vehicle to introduce new arguments. (See *People v. Landry* (1996) 49 Cal.App. 4th 785, 791-792 [motions to augment the record are valid "to support the theories ... articulated for reversal," but are not "vehicle[s] for deciding substantives

### C. In the alternative, the Court should find that the SCA protects Facebook user communications.

If the Court considers the People's SCA arguments, it should reject them. The plain text of the SCA leaves no dispute that Facebook is both an ECS and RCS, and that the SCA disclosure prohibitions apply to Facebook communications. Every court to consider this issue has so held.[5]

#### 1. Facebook is both an ECS provider and an RCS provider.

The SCA applies to two types of service providers: ECS providers and RCS providers. An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." (18 U.S.C. § 2510(15).) An RCS is "the provision to the public of computer storage or processing services by means of an electronic communications system." (18 U.S.C. § 2711(2).)

Facebook permits people to communicate with one another in multiple ways, including direct messages; audio or video calls, posts, and comments that can also include photos or videos and be visible to one or more people.[6] Facebook is an ECS because it "provides its users with the

---

issues on their merits."]; see also *People v. Silva* (1978) 20 Cal.3d 489, 493 [same].) The Court should not consider out-of-context, inaccurate characterizations of materials outside the record in this case.

[5] The DA suggests that Facebook failed to carry its "initial burden" of showing that the SCA applies to Facebook. (Intervenor's Br. at pp. 4-6.) This is wrong: Facebook's initial motion to quash cited to a litany of authority demonstrating that the SCA applies to Facebook. (App'x at pp. 7-8, 11.)

[6] (*See* Facebook Help Center, *Messaging* [available at https://www.facebook.com/help/1071984682876123?helpref=hc_global_nav]; *id.*, *Video Calling* [available at https://www.facebook.com/help/287631408243374/?helpref=hc_fnav]; *id.*,

ability to send and receive electronic communications, including private Facebook messages and wall posts." (*Ehling v. Monmouth-Ocean Hosp. Service Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 667 [holding that Facebook is an ECS provider]; *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F.Supp.2d 965, 982 [holding that subpoenas seeking content from Facebook are invalid under the SCA because "Facebook . . . is an ECS provider"].) Facebook is an RCS because it provides computer storage and processing services: users can store messages, notes, photos, videos and other content on Facebook, and Facebook offers myriad computer processing services to provide users with a "personalized experience." (Intervenor's Br. at p. 10; *Ehling*, *supra*, 961 F.Supp.2d at pp. 667-669 [Facebook user wall posts are covered by the SCA]; *In re Facebook, Inc.* (N.D. Cal. 2012) 923 F.Supp.2d 1204, 1206 [quashing subpoena seeking disclosure of content of deceased Facebook user based on the SCA]; *Crispin*, *supra*, 717 F.Supp.2d at pp. 989-990 [holding that Facebook is both and ECS and RCS under the SCA].) The People do not even address, let alone dispute, these threshold statutory and case authorities.

### 2. As an ECS provider, Section 2702(a)(1) applies to Facebook communications because they are maintained in electronic storage.

As an ECS provider, Facebook cannot disclose the content of electronic communications maintained in "electronic storage." (18 U.S.C. § 2702(a)(1).) "Electronic storage" includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic

---

*Share and Manage Posts on Your Timeline*
[https://www.facebook.com/help/1640261589632787/?helpref=hc_fnav].)

transmission thereof," *and* "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." (18 U.S.C. § 2510(17)(A),(B).) All Facebook accountholder communications are in electronic storage, because they are either pending receipt (and thus in temporary storage) or maintained in backup storage. (*Ehling*, *supra*, 961 F.Supp.2d at p. 668 ["Facebook wall posts are in electronic storage."])

First, Facebook maintains most communications in temporary and intermediate storage pending transmission. Indeed, nearly every post, comment, or update that a person puts on Facebook resides in temporary and intermediate storage because it awaits receipt and review by one or more intended recipients. (See *Theofel*, *supra*, 359 F.3d at p. 1075 [subsection 2510(17)(A) applies to "messages stored on an ISP's server pending delivery to their intended recipient"].) Not everyone reviews a Facebook communication immediately; if a communication is made visible to 50 people, it will necessarily be "pending transmission"—and thus in temporary storage—until *all* of those people have seen it. And it remains in temporary storage thereafter because the list of people who can view or review a profile or communication is dynamic; it can change if people change their privacy settings and add and delete friends.[7]

---

[7] Unlike emails that may be stored in two places (one copy in the sender's account, and one copy in the recipient's account), a Facebook post is stored only in the user's account and delivered and/or redelivered to the recipient each time the recipient wishes to view it. (See, e.g., Facebook Help Center, *Share and Manage Posts on Your Timeline* [available at https://www.facebook.com/help/1640261589632787/?helpref=hc_fnav] [explaining that when a user deletes on of their own posts, it is removed from Facebook entirely].)

Second, Facebook communications are also covered by Section 2510(17)(B), because they are also retained for backup protection. (*Ehling*, *supra*, 961 F. Supp. 2d at p. 668 [Because they are stored "for backup purposes," "Facebook wall posts are in electronic storage"].) The Ninth Circuit has held that Section 2510(17)(B) includes opened messages stored for later use. (*Theofel*, *supra*, 359 F.3d at p. 1075 [holding that emails stored by an ECS are in temporary, intermediate storage incidental to transmission; and that in the alternative, opened emails are stored for purposes of backup protection; "nothing in the [SCA] requires that the backup protection be for the benefit of the [provider] rather than the user"].)

In *Theofel*, the Ninth Circuit addressed a claim of unauthorized access under Section 2701(a) of the SCA, which, like the disclosure prohibitions of the SCA, applies only to communications maintained in "electronic storage." The plaintiffs in *Theofel* alleged that the defendant accessed their emails without authorization by using fraud to obtain them from the email provider, NetGate. The emails had already been opened; plaintiffs chose to retain them with NetGate. The defense, supported by the Department of Justice as *amicus curiae*, argued that the emails were not in "electronic storage." According to the defense, they were not in "temporary, intermediate storage pending transmission" because the plaintiffs had already opened them, and they were not stored for purposes of backup protection because plaintiffs chose to retain them with NetGate.

The Ninth Circuit rejected this argument, holding that opened communications can remain in "electronic storage regardless of whether they had been previously delivered." (*Theofel*, *supra*, 359 F.3d at p. 1077.) As the Ninth Circuit explained, messages that remain on a provider's server are maintained for purposes of backup protection "within the ordinary

meaning of those terms." (*Id.* at p. 1075). The court explained that "an obvious purpose" for such storage is to access it again later. (*Id.*)

Consistent with this view, courts have held that copies of opened Facebook messages "would plainly be for backup purposes," and therefore be in "electronic storage." (*Crispin*, *supra*, 717 F.Supp.2d at p. 987, fn. 46.) Indeed, every court to consider the issue has held that the SCA applies to opened Facebook communications; no court has ever held to the contrary. (See *id.* at pp. 989-990 [holding that the SCA would not permit Facebook to disclose content in response to a subpoena, noting that "Facebook [is an] ECS provider as respects wall postings and comments and that such communications are in electronic storage" and that in the alternative Facebook is an RCS provider]; see also *Doe v. City and County of San Francisco* (N.D. Cal. June 12, 2012, No. C10–04700 THE, 2012 WL 2132398, at *2 [applying the SCA to previously opened webmail messages]; *Suzlon Energy Ltd. v. Microsoft Corp.* (9th Cir. 2011) 671 F.3d 726, 730 [quashing a subpoena seeking content from Hotmail, a web-based email service, as invalid under the SCA].)

This is exactly what Congress intended. "Electronic storage" was meant to include opened messages that an accountholder leaves in storage on the service for later use:

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

(H.R.Rep. No. 99-647, 99th Cong., 2d Sess., p. 65 (1986).)

The DA ignores all this authority. Instead, it makes two unsupported and irrelevant arguments: first, that Facebook differs from the services that were in existence in 1986. (Intervenor's Br. at p. 10 ["Facebook operates in a vastly different manner" and contrasting it with "primitive email systems, which served as simple couriers of data"].) But Congress was prescient in drafting the SCA and expressly intended for it to be a forward-looking statute that would encourage, and apply to, future technological developments.[8] (See Sen.Rep. No. 99–541, 2d Sess., p. 19 (1986), reprinted in 1986 U.S. Code Cong. & Admin. News, p. 3599 [noting that the SCA was designed to allow for "innovative forms of telecommunications and computer technology"].)

Second, the DA argues that Facebook does not retain data for "backup" protection because "it is analyzed and used to provide users a 'personalized experience.'" (Intervenor's Br. at p. 10.) Not only is this a non-sequitur, but the DA misses the point. If a user chooses to retain Facebook content—whether a private message or otherwise—one of the purposes "would plainly be for backup purposes." (*Crispin*, *supra*, 717 F.Supp.2d at p. 987, fn. 46.)[9] And whether Facebook otherwise has authority to access this communication in connection with the service is a separate question, and one that is irrelevant to whether it is in electronic storage.[10]

---

[8] The People note that Facebook "possesses a license over the content users upload." (Intervenor's Br. at p. 10.) Of course it does: a license lets Facebook route communications to their recipients.

[9] As noted above, it may also be in intermediate storage awaiting delivery or redelivery to another user.

[10] The People also note that Facebook has a "Download Your Information tool," which allows accountholders to download their data. (Intervenor's Br. at p. 10.) But this proves the fact that Facebook communications are maintained in electronic storage, since it allows users to download copies of

### 3. Facebook is a covered RCS, and Section 2702(a)(2) applies because Facebook only provides accountholders with storage and computer processing services.

Facebook's services also qualify as a RCS in addition to an ECS. As an RCS, Section 2702(a)(2) prohibits Facebook from disclosing communications content maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer [ ] if the provider is not authorized to access the contents of any such communication for purposes of providing any services other than storage or computer processing." (18 U.S.C § 2702(a)(2)(A), (B).)

This provision has two requirements, both of which Facebook meets. First, Facebook must receive the communication from the user electronically, which it does. (18 U.S.C. § 2702(a)(2)(A); see also H.R.Rep. No. 99-647, 99th Cong., 2d Sess., p. 64 (1986) ["First, the affected communication must be on behalf of and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from) a subscriber or customer of such service."].) The DA does not dispute this.

Second, the communication must be "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than

---

their communications. (See *Theofel*, *supra*, 359 F.3d at p. 1075 ["An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user."].)

storage or computer processing." (18 U.S.C. § 2702(a)(2)(B); see also H.R.Rep. No. 99-647, 99th Cong., 2d Sess., p. 64 (1986) [stating that disclosure prohibition applies "so long as the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing"].) Facebook satisfies this requirement as well.

The statute does not limit the purposes for which Facebook can access a communication. It simply says that Facebook must receive authorization to access a communication in connection with its provision of storage and computer processing services. (See *Viacom Int'l Inc. v. YouTube Inc.* (S.D.N.Y. 2008) 253 F.R.D. 256, 264 fn. 8 [YouTube is an RCS provider notwithstanding the fact that it is authorized to access content for purposes of review, as such authorization "is granted in connection with [YouTube's] provision of alleged storage services."].) The DA argues that "the SCA only requires authority to access [data] in order to place a provider outside of the Act's protection," but this is only partially true. (Intervenor's Br. at p. 12.) To fall outside the SCA, the accountholder must grant Facebook authority to access data in connection with Facebook's provision of services other than storage and computer processing. In other words, it makes no difference if Facebook has authority to screen content to prevent malware, provide a "personalized experience," or for some other reason. (Cf. *Crispin v. Christian Audigier, Inc.*, *supra*, 717 F.Supp.2d at p. 990 [holding that Section 2702(a)(2)(B) prohibits Facebook, as an RCS, from disclosing communications, and holding that "the statute does not limit storage to retention for benefit of the user only"].) What matters is that Facebook's authorization to access content is granted as part of Facebook's storage and computer processing services, and not for purposes of providing other, unspecified services.

As the DA concedes, Facebook receives authorization to access communications entirely in connection with its provision of "user related services" – which are storage and computer processing. (Intervenor's Br. at p. 12.) The DA proves this point by noting that Facebook's Terms of Service and Data Policy provide Facebook with authorization to access content in order to screen communications for contraband (such as potential terrorist content or child exploitation), or to provide tailored suggestions to accountholders (such as what Pages to like or what products to buy). (Intervenor's Br. at p. 12.)[11] These Terms govern Facebook's provision of storage and computer processing services. Section 2702(a)(2) therefore applies to Facebook communications. (See *Viacom, Int'l Inc. v. YouTube Inc.*, *supra*, 253 F.R.D. at p. 264, fn. 7 [Section 2702(a)(2) applies when a provider has authorization to review content, if the authorization "is granted in connection with its provision of alleged storage services."].)

Moreover, even under a narrow reading of Section 2702(a)(2)(B), the statute allows "computer processing." Artificial intelligence, malware protection screening, and targeted advertising are all forms of "computer processing," which is an intentionally broad term that is not limited to processing for the benefit of the user. (*Low v. LinkedIn Corp.* (N.D. Cal. 2012) 900 F.Supp.2d 1010, 1023 [computer processing is "sophisticated processing" of information]; Sen.Rep. No. 99–541, 2d Sess., p. 3 (1986) [computer processing involves "processing of information"]; cf. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It* (2004) 72 Geo. Wash. L.Rev. 1208, 1230 ["Every

---

[11] The People's reference to *Juror No. One v. Superior Court* (2012) 206 Cal.App.4th 854, is misplaced. (Intervenor's Br. at p. 12.) That court's discussion of whether Facebook is an RCS is dicta that relies on the same misreading of the statute that the People rely on. The court declined to decide the issue. (*Juror No. One*, *supra*, 206 Cal.App.4th at p. 864.)

website processes information sent to it[.]"]; *Crispin v. Christian Audigier, Inc.*, *supra*, 717 F.Supp.2d at p. 990.) The use of this broad term was intentional: the SCA was designed to encourage technological development. A construction of the statute that would have its protections fall away when companies innovate would undermine its purpose. (H.R.Rep. No. 99-647, 99th Cong., 2d Sess., p. 19 (1986).) No court has adopted the People's argument that RCS content loses protection because the provider processes the data, because the statute expressly permits it. (See 18 U.S.C. § 2702(a)(2)(B).)

### 4. The Court should not adopt an interpretation of the SCA that is at odds with its text and purpose.

The plain text of the SCA demonstrates that it protects Facebook communications. However, if the Court believes there is any ambiguity, it should construe the statute to give effect to the intent of Congress.[12]

The SCA was intended to "shield private electronic communications from government intrusion" and "grant[] [electronic communications] protection against unwanted disclosure *to anyone.*" (See *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1445.) As Congress put it, the SCA was intended to address the following problems caused by legal uncertainty that existed at the time:

> First, [legal uncertainty] may unnecessarily discourage potential customers form using such systems, and encourage unauthorized users to

---

[12] Courts can consult legislative history to confirm that applying the plain meaning of the text leads to a result that is consistent with the intent of Congress. (*Immigration & Naturalization Servs. v. Cardoza-Fonseca* (1987) 480 U.S. 421.) Courts can also consult legislative history to avoid an absurd result (see *Green v. Bock Laundry Machine Co.* (1989) 109 S.Ct. 1981, 1995), or where applying the plain meaning would lead to a result contrary to legislative intent (*O'Gilvie v. United States* (1996) 519 U.S. 79).

> obtain access to communications to which they are not party. Lack of clear standards may also expose law enforcement officers to liability and endanger the admissibility of evidence.
>
> But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.

(H.R.Rep. No. 99-647, 99th Cong. 2d Sess., p. 19 (1986).) In other words, Congress sought to accomplish three goals: (1) to encourage the use and development of innovative communications technology; (2) to provide law enforcement with a clear framework to conduct investigations; and (3) to ensure the "continued vitality of the Fourth Amendment" by creating a statutory regime that extends a set of Fourth-Amendment like protections to electronic communications. (See *Hunter*, *supra*, 4 Cal.5th at p. 1263 [describing the "three themes" Congress sought to address as "(1) protecting the privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies"].)

The DA's view – in which the SCA does not apply to modern services like Facebook – would mean privacy has "erode[d] as technology advance[d]." It would leave most modern electronic communications unprotected by the statute because most online and web services conduct some form of proactive screening for contraband, malware, or virus protection.[13] If the Court adopts the DA's view, Providers would have to

---

[13] (See, e.g., Microsoft Office Help & Training, *Help Protect Your Outlook.com Email Account* [available at https://support.office.com/en-

choose between the security and integrity of their service, and the privacy of the communications maintained on that service. This is not what Congress intended.

These stark consequences would reach far beyond the circumstances presented by this case. If the SCA does not apply to a communication, then a subscriber has no remedy under Section 2701 if a malicious third party gains unauthorized access to their communications via the provider. A provider could choose to disclose a communication to anyone, for any reason or no reason at all. Many law enforcement agencies could compel a provider to disclose a communication with a mere subpoena,[14] and providers would remain free to disclose communications to governments without limitation or oversight.[15] Users would quickly lose confidence in

---

us/article/help-protect-your-outlook-com-email-account-a4f20fc5-4307-4ece-8231-6d4d4bd8a9ba] [explaining that Microsoft Outlook alerts a user if a certain message "contains something that might be unsafe" and advises the user not to open the message].)

[14] While the DA is correct that California law would still require a warrant even if the SCA did not apply to Facebook, (*see* Pen. Code, § 1546.1(b)), California law would not prohibit federal agencies inside or outside of California, or any state agencies outside California, from seeking such information through use of a mere subpoena. (But see *United States v. Warshak*, *supra*, 631 F.Supp.3d at p. 288 [the Fourth Amendment requires governmental entities to obtain a warrant before obtaining communications from providers].) Nor would California law restrict providers from disclosing content to anyone, since its prohibitions apply to governmental entities, not providers.

[15] The DA misleadingly suggests that the SCA cannot apply to Facebook because otherwise, Facebook would be unable to disclose content to the government when Facebook locates problematic content. (Intervenor's Br. at pp. 13-15.) But the DA omits that the SCA contains limited exceptions that show Congressional intent in determining when providers may disclose content. There are exceptions that allow some disclosures – for example, if Facebook uncovers child exploitation, the SCA permits disclosure "to the National Center for Missing and Exploited Children in connection with a report submitted thereto under section 2258A." (18 U.S.C. § 2702(b)(6).)

communications technology as their privacy rights disappear, undermining the stated intent of Congress in enacting the SCA.

In sum, no court has accepted the view advanced by the DA that the SCA does not apply to Facebook. It is contrary to the intent of Congress when it enacted the SCA. It has no support in the text of the SCA or the many court opinions interpreting the SCA. This Court should soundly reject it.

## III. Conclusion

Because the DA's brief in intervention far exceeds the single issue on which they sought to intervene and that this Court permitted intervention—whether a trial court can compel the prosecution to issue a search warrant—this Court should disregard all of the DA's other arguments.

This Court should also reaffirm that a trial court can order the People to assist the defense to the extent permitted by law.

DATED: August 8, 2018

Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP

---

And if Facebook believes in good faith that there is "an emergency involving danger of death or serious physical injury," it can disclose content to the government. (18 U.S.C. § 2702(b)(8).) If the DA wants to loosen the SCA's limitations further, it should direct its request to Congress rather than asking this Court to rewrite the statute. (See, e.g., *Henson v. Santander Consumer USA Inc.* (2017) 137 S.Ct. 1718, 1725 ["[I]t is never our job to rewrite a constitutionally valid statutory text under the banner of speculation about what Congress might have done had it faced a question that, on everyone's account, it never faced."]; *Baker Botts L.L.P. v. ASARCO LLC* (2015) 135 S.Ct. 2158, 2169 [noting that the Court "lack[s] the authority to rewrite" a statute].)

## 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 6240 words. I swear under penalty of perjury that the foregoing is true and correct.

DATED: August 8, 2018

Joshua S. Lipshutz

Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP

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

**PROOF OF SERVICE**

I, Teresa Motichka, declare as follows:

I am a citizen of the United States and employed in San Francisco County, California; I am over the age of eighteen years, and not a party to the within action; my business address is 555 Mission Street, Suite 3000, San Francisco, CA 94105-0921. On August 8, 2018, I served the within documents:

**PETITIONER'S RESPONSE TO BRIEF OF INTERVENOR SAN DIEGO COUNTY DISTRICT ATTORNEY**

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

**SEE ATTACHED SERVICE LIST**

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

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

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

Executed on August 8, 2018, at San Francisco, California.

Teresa Motichka

Teresa Motichka

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

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