

STAY REQUESTED

No. S286267

IN THE SUPREME COURT OF CALIFORNIA

SNAP, INC.,
Petitioner,

vs.

THE SUPERIOR COURT OF THE STATE OF CALIFORNIA,
FOR THE COUNTY OF SAN DIEGO,
Respondent,

ADRIAN PINA et al.,
Real Parties in Interest.

META PLATFORMS, INC.,
Petitioner,

vs.

THE SUPERIOR COURT OF THE STATE OF CALIFORNIA,
FOR THE COUNTY OF SAN DIEGO,
Respondent,

ADRIAN PINA et al.,
Real Parties in Interest.

After a Decision by the Court of Appeal,
Fourth Appellate District, Division 1, Case Nos. D083446,
D083475
San Diego Superior Court, Dept. 21, Case Nos. SCN429787,
SCN429787
Honorable Daniel F. Link, Judge Presiding, (760) 201-8021

PETITION FOR REVIEW
IMMEDIATE STAY REQUESTED OF THE SUPERIOR
COURT'S AUGUST 2, 2024 *EX PARTE* ORDER TO PRODUCE
SUBPOENAED RECORDS *IN CAMERA* BY AUGUST 5, 2024

*Orin S. Kerr (CSB No. 319808) orin@orinkerr.com
LAW OFFICE OF ORIN S. KERR
334 Law Building, Berkeley, CA 94720 Telephone: 510.664.5257

David W. Feder (*application for admission pro hac vice pending*)
dfeder@fenwick.com
FENWICK & WEST LLP
902 Broadway, 18th Floor
New York, NY 10010-6035
Telephone: 212.430.260

Tyler G. Newby (CSB No. 205790)
tnewby@fenwick.com
Ryan Kwock (CSB No. 336414)
rkwock@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300

Janie Yoo Miller (CSB No. 312715)
jmiller@fenwick.com
Esther Galan (CSB No. 335763)
egalan@fenwick.com
FENWICK & WEST LLP
730 Arizona Avenue, 1st Floor
Santa Monica, CA 90401
Telephone: 310.554.5400

Brian A. Sutherland
(CSB No. 248486)
brian.sutherland@calg.com
Greg Wolff (CSB No. 78626)
greg.wolff@calg.com
COMPLEX APPELLATE
LITIGATION GROUP LLP
96 Jessie Street
San Francisco, CA 94105
Telephone: 415.649.6700

Attorneys for Petitioner
SNAP INC.

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	5
ISSUE PRESENTED FOR REVIEW	9
INTRODUCTION	9
STATEMENT OF THE CASE	13
I. THE STORED COMMUNICATIONS ACT.....	13
II. FACTUAL BACKGROUND AND PROCEDURAL HISTORY	16
A. Snapchat.....	16
B. Real Party In Interest Adrian Pina.	17
C. Procedural History.....	18
WHY REVIEW IS WARRANTED	20
I. THE COURT OF APPEAL’S ERRONEOUS INTERPRETATION WILL HAVE SIGNIFICANT PUBLIC CONSEQUENCES.....	21
A. The Decision Guts the Primary Federal Statute that Shields Private Electronic Communications from Disclosure.	21
B. If This Court Does Not Grant Review, California Courts Will Be Deluged with Subpoenas.	25
C. The Court of Appeal’s Decision Undermines Platform Safety and User Security.....	27
II. CALIFORNIA COURTS NEED IMMEDIATE GUIDANCE IN APPLYING THE BUSINESS MODEL THEORY	29

**TABLE OF CONTENTS
(Continued)**

	Page
III. THE COURT OF APPEAL’S SHARP DEPARTURE FROM PRIOR PRECEDENT WARRANTS THIS COURT’S REVIEW.....	31
A. The Court of Appeal’s Interpretation of The SCA’s ECS Protections Conflicts with Precedent from the Ninth and Fourth Circuits.	31
B. The Court of Appeal’s “Business Model” Theory Is a Novel Departure from Prevailing Understandings of the SCA.	34
IV. THE COURT OF APPEAL’S DECISION IS WRONG.....	36
A. Snap Is Prohibited from Disclosing Content Held in Electronic Storage, even if Snap Accesses the Same Content for an Unenumerated Purpose.	36
B. Snap Is Prohibited from Disclosing Content Stored on Behalf of Its Users.	39
A STAY IS WARRANTED.....	40
CONCLUSION.....	41
CERTIFICATE OF WORD COUNT.....	42
PROOF OF SERVICE	43

TABLE OF AUTHORITIES

	Page(s)
FEDERAL CASES	
<i>Andersen Consulting v. UOP</i> (N.D.Ill. 1998) 991 F.Supp.1041	26
<i>Anzaldua v. Northeast Ambulance and Fire Protection District</i> (8th Cir. 2015) 793 F.3d 822.....	31
<i>Hately v. Watts</i> (4th Cir. 2019) 917 F.3d 770	15, 33, 36
<i>In re U.S.</i> (D.Or. 2009) 665 F.Supp.2d 1210	25
<i>Konop v. Hawaiian Airlines, Inc.</i> (9th Cir. 2002) 302 F.3d 868.....	38
<i>Theofel v. Farey-Jones</i> (9th Cir. 2004) 359 F.3d 1066.....	32, 33, 36, 38
<i>United States v. Bychak</i> (S.D.Cal., May 12, 2022, No. 18-CR-4683-GPC) [2022 WL 1524736]	24
<i>United States v. Peterson</i> (W.D.Mo., July 18, 2023, No. 22-00196-01-CR-W-DGK) [2023 WL 5920869], <i>report and recommendation adopted</i> (W.D.Mo., September 11, 2023, No. 4:22-CR-0166-DGK-02) [2023 WL 5918310].....	30
<i>United States v. Warshak</i> (6th Cir. 2010) 631 F.3d 266.....	24
CALIFORNIA CASES	
<i>Facebook, Inc. v. Superior Court (Hunter)</i> (2018) 4 Cal.5th 1245 [233 Cal.Rptr.3d 77, 417 P.3d 725].....	<i>passim</i>

**TABLE OF AUTHORITIES
(Continued)**

	Page(s)
<i>Facebook, Inc. v. Superior Court (Touchstone)</i> (2020) 10 Cal.5th 329, 361 [233 Cal.Rptr.3d 77, 471 P.3d 38].....	<i>passim</i>
<i>Hassell v. Bird</i> (2018) 5 Cal.5th 522 [234 Cal.Rptr.3d 867, 420 P.3d 776].....	16
<i>In re Brandy R.</i> (2007) 150 Cal.App.4th 607 [58 Cal.Rptr.3d 456]	40
<i>Juror Number One v. Superior Court</i> (2012) 206 Cal.App.4th 854 [142 Cal.Rptr.3d 151]	38
<i>Negro v. Superior Court</i> (2014) 230 Cal.App.4th 879 [179 Cal.Rptr.3d 215]	29
<i>Ng v. Superior Court</i> (1992) 4 Cal.4th 29 [13 Cal.Rptr.2d 856, 840 P.2d 961].....	40
<i>People v. Lewis</i> (2021) 11 Cal.5th 952 [281 Cal.Rptr.3d 521, 491 P.3d 309].....	37
<i>Stewart v. Hurt</i> (1937) 9 Cal.2d 39 [68 P.2d 726].....	41
<i>Unzipped Apparel, LLC v. Bader</i> (2007) 156 Cal.App.4th 123 [67 Cal.Rptr.3d 111]	24
 OTHER STATE CASES	
<i>State v. Johnson</i> (Tenn. Crim. App. 2017) 538 S.W.3d 32.....	30

**TABLE OF AUTHORITIES
(Continued)**

	Page(s)
FEDERAL STATUTES	
18 U.S.C.	
§ 2510(15)	14
§ 2510(17)	15
§ 2510(17)(A)-(B)	36
§ 2523.....	35
§§ 2701-2712.....	11
§ 2702(a)(1).....	<i>passim</i>
§ 2702(a)(2).....	13, 15, 38, 39
§ 2702(b)(8).....	35
§ 2702(c)(6)	18
STATE STATUTES	
Code Civ. Proc., § 1985.6	24
Penal Code, § 1326, subd. (c).....	26
OTHER AUTHORITIES	
2 LaFave et. al., <i>Criminal Procedure</i> (4th ed. 2020)	
§ 4.8(b)	15, 25, 34
Carr & Bellia, <i>Law of Electronic Surveillance</i>	
(1st ed. 2024) § 4:97	34
<i>Information for Law Enforcement, Privacy, Safety, and</i>	
Policy Hub < https://bit.ly/46ARWge >	
[as of Aug. 2, 2024].....	23
Jeffrey Gottfried, <i>Americans' Social Media Use,</i>	
(Jan. 31, 2024) Pew Research Center	
< http://bit.ly/4d5B5od > [as of Aug. 2, 2024].....	10
Kerr, <i>Computer Crime Law</i> (5th ed. 2022)	34
<i>Learn About How Snap Uses Data</i> , Snapchat Support	
< https://bit.ly/3AasstM > [as of Aug. 2, 2024]	28

TABLE OF AUTHORITIES
(Continued)

	Page(s)
<i>Privacy By Product</i> , Privacy, Safety, and Policy Hub < https://bit.ly/3WuPyTq > [as of Aug. 2, 2024]	22, 23
<i>Privacy Policy</i> (Feb. 26, 2024) Privacy, Safety, and Policy Hub < https://bit.ly/46wZFvw > [as of Aug. 2, 2024]	17, 23
Sen. Rep. No. 99-541, 2d Sess.	13, 14
Snap Inc. Form 10-Q (Aug. 2, 2024) < https://bit.ly/3SAwBxA >, pp. 28-29 [as of Aug. 2, 2024].....	10, 22
Snap Inc. Terms of Service (Feb. 26, 2024) < https://bit.ly/3yA5HyV > [as of Aug. 2, 2024].....	17
<i>Snapchat Ads Transparency</i> , Privacy, Safety, and Policy Hub < https://bit.ly/4dum3YI > [as of Aug. 2, 2024]	27
<i>Testimony of Evan Spiegel Co-Founder and CEO, Snap Inc.</i> (January 2023), Hearing before the United States Senate Committee on the Judiciary < https://bit.ly/3YACvTj > [as of Aug. 2, 2024].....	28
Woods & Swire, <i>The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems</i> (Feb. 6, 2018)	35

**TO THE HONORABLE CHIEF JUSTICE GUERRERO AND
ASSOCIATE JUSTICES OF THE CALIFORNIA SUPREME
COURT:**

Petitioner Snap Inc. (“Snap”) respectfully petitions this Court for review of the published opinion of the Court of Appeal, Fourth Appellate District, Division One, in *Snap, Inc. et al. v. Superior Court of San Diego County* (July 23, 2024, No. D083446) (hereafter “Opinion” or “Opn.”), a copy of which is attached as Attachment A. Snap had no opportunity to petition the Court of Appeal for a rehearing because its Opinion was issued with immediate finality. (Opn. at p. 45.) As explained below, Snap requests a stay of trial court proceedings pending this Court’s review.

ISSUE PRESENTED FOR REVIEW

Are the contents of electronic communications maintained by a service provider such as Petitioner Snap Inc. protected from disclosure under the privacy protections of the Stored Communications Act, (18 U.S.C. § 2702(a)), or does the service provider’s “business model” eliminate those privacy protections?

INTRODUCTION

The specific issue in this case was expressly left open by a prior decision of this Court. (See *Facebook, Inc. v. Superior Court (Touchstone)* (2020) 10 Cal.5th 329, 361 [233 Cal.Rptr.3d 77, 471 P.3d 38].) In her *Touchstone* concurrence, Chief Justice Cantil-Sakauye introduced a “business model theory” of the federal Stored Communications Act (“SCA”), under which the contents of communications held by electronic communications providers

were exempt from the ban on disclosure under Section 2702(a). (18 U.S.C. § 2702(a).) The Court unanimously recognized that the issues raised by the business model theory are “important” and “unresolved.” (*Touchstone, supra*, 10 Cal.5th at pp. 338, 361.) Justice Cuéllar added that, “in the appropriate case, courts ought to take up” the “crucial matter of how broadly to read the SCA.” (*Id.* at p. 373 (conc. opn. of Cuéllar, J.).)

The Court of Appeal accepted this Court’s “invitation” to consider the business model theory of the SCA—and essentially adopted it in its entirety. (Opn. at p. 37.) In so doing, the Court misconstrued the SCA to negate its privacy protection for most electronic communications in the United States. For the majority of Americans who use services like Facebook, Instagram, and Snap’s platform Snapchat—and related services, like email and text messaging—the SCA’s crucial privacy protections have just evaporated by judicial interpretation.

This case is about the privacy of those electronic communications. According to the Pew Research Center, approximately 27% of adults in the United States use Snapchat, 68% of adults use Facebook, and 47% of adults use Instagram.¹ As of August 2, 2024, Snapchat has 432 million global daily active users, with approximately 100 million users in North America.² But nothing in the Court of Appeal’s Opinion limits

¹ (Jeffrey Gottfried, *Americans’ Social Media Use*, (Jan. 31, 2024) Pew Research Center <<http://bit.ly/4d5B5od>> [as of Aug. 2, 2024].)

² (Snap Inc. Form 10-Q (Aug. 2, 2024) <<https://bit.ly/3SAwBxA>>, pp. 28-29 [as of Aug. 2, 2024].)

the application to only these providers—the ruling will also eviscerate privacy protections for other services like web-based email and text messaging.

The SCA, (18 U.S.C. §§ 2701-2712), is the federal law that protects the privacy of electronic communications containing personal messages, photos, and videos. It does two main things. First, the SCA prevents the government from compelling access to contents of electronic communications or non-content records without proper legal process—including, in some cases, requiring a search warrant. (See *id.* § 2703.) Second, the SCA blocks providers from disclosing the contents of users’ communications unless a specific exception to the disclosure bar applies. (See *id.* § 2702.)

These two parts of the SCA work together, protecting our virtual spaces just like our physical ones. As with physical homes, the government cannot force its way in without a warrant. And the companies that hold our communications must protect them from outside access unless specific exceptions apply, like a warrant. Put simply, the SCA provides the legal walls that keep our internet accounts private. (See generally *Facebook, Inc. v. Superior Court (Hunter)* (2018) 4 Cal.5th 1245, 1262-63 [233 Cal.Rptr.3d 77, 417 P.3d 725].)

Review is justified for four reasons.

First, whether the business model theory is viable has statewide and national importance. Adopting the theory would eliminate the core privacy protection that most Americans rely on for their electronic communications. Although Congress enacted

the SCA in 1986 and amended it several times since, the business model theory entered the realm of judicial consideration for the first time in 2020 with Chief Justice Cantil-Sakauye's *Touchstone* concurrence. No court has ever adopted it as binding law until now. And its consequences are vast—resetting the existing balance between privacy protection, on the one hand, and platform integrity and public safety, on the other. This Court should determine whether the business model theory is viable, not the court below.

Second, this Court should not wait for a future opportunity to rule on the business model theory. The scope of the Court of Appeal's ruling is unclear. Does it apply only to Meta and Snap? What about email services like Gmail or Yahoo? Or messaging platforms like WhatsApp and Discord? Can providers avoid the ruling by changing their terms of service, and if so, what new language is needed? By failing to provide clear answers about how far the business theory extends, the Court of Appeal's ruling leaves trial courts, providers, and the public unable to determine the SCA's basic privacy rules.

Third, the Court of Appeal's reasoning departs sharply from the prevailing judicial understanding of the SCA. It conflicts with federal precedent articulating an expansive understanding of when the SCA protects the content of electronic communications from disclosure. And the appellate court dispatches, in a single footnote, numerous decisions where the question of whether content held by providers is protected by the SCA was so settled and unexceptional that it did not warrant

analysis. (Opn. at p. 39, fn.17.) This includes *Hunter*, where this Court said it had “no reason to question” that Facebook was subject to the SCA. (*Hunter, supra*, 4 Cal.5th at p. 1268.) Now, nearly 40 years after the SCA’s enactment and decades of legal scrutiny, the Court of Appeal effectively says these decisions were wrong.

Fourth, the business model theory is wrong as a matter of statutory interpretation. The Opinion misconstrues the plain language of one provision, (18 U.S.C. § 2702(a)(2)), and invents a limitation not found in the text of the other, (18 U.S.C. § 2702(a)(1)). This is logically inconsistent and contrary to the overarching privacy-protection purpose of the SCA.

STATEMENT OF THE CASE

I. THE STORED COMMUNICATIONS ACT

Congress enacted the SCA in 1986 “to protect privacy interests in personal and proprietary information,” while also providing avenues for law enforcement to access such information when needed. (Sen. Rep. No. 99-541, 2d Sess., p. 3-5.). The Senate Judiciary Committee report urging enactment recognized that “computers are used extensively today for the storage and processing of information.” (*Id.* at p. 3). It reasoned that, when individuals store their private information and communications on computers managed by third-party providers, they should not lose the Fourth Amendment protections that would apply to physical records stored at home. (See *ibid.*) “Congress was concerned that ‘the significant privacy protections that apply to homes in the physical world may not apply to “virtual homes” in

cyberspace,’ and hence ‘tried to fill this possible gap with the SCA.’” (*Hunter, supra*, 4 Cal.5th at p. 1263, citation omitted.) To avoid rapid obsolescence, Congress designed the SCA to apply prospectively to advancements in communications technology. (Sen. Rep. No. 99-541, 2d Sess., p. 5.)

In *Hunter*, this Court reviewed the SCA’s legislative history and discerned three major themes “repeatedly emphasized by the bill authors”:

- (1) protecting the privacy expectations of citizens,
- (2) recognizing the legitimate needs of law enforcement, and
- (3) encouraging the use and development of new technologies (with privacy protection being the primary focus).

(*Hunter, supra*, 4 Cal.5th at p. 1263.)

Congress prohibited two types of providers from disclosing the contents of their users’ communications. The first type of provider is an “electronic communication service” (“ECS”), which is any service that enables users to send or receive electronic communications. (18 U.S.C. § 2510(15).) The second is a “remote computing service” (“RCS”) which is the “provision to the public of computer storage or processing services by means of an electronic communications system.” (*Id.* § 2711.) An ECS provides messaging or communications; an RCS provides storage and processing. Both types of providers hold private electronic communications on customers’ behalf; under the SCA, neither may disclose them, subject to enumerated exceptions.

The prohibitions, however, differ between the two. An ECS cannot divulge “the contents of a communication while in electronic storage by that service.” (18 U.S.C. § 2702(a)(1).)

“Electronic storage” is “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” and “any storage of such communication by an [ECS] for purposes of backup protection.” (18 U.S.C. § 2510(17).) An RCS cannot disclose “the contents of any communication which is carried or maintained on that service” “solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.” (*Id.* § 2702(a)(2).)

When the SCA was enacted in 1986, providers typically were an ECS *or* an RCS. Now, providers generally allow users to store large amounts of their personal messaging data on the servers of internet providers. Accordingly, it is common for user contents to be protected under both the ECS *and* RCS rules of statutory privacy protection. (See *Hately v. Watts* (4th Cir. 2019) 917 F.3d 770, 789-93.) If a particular communication is protected under either the ECS or RCS rules—or both—then Section 2702(a) prohibits disclosure of user communications unless a specific exception to the disclosure in Section 2702(b)-(c) applies.³

For decades, providers and their customers depended on these provisions to safeguard privacy interests in communications by protecting them from disclosure. Congress has not amended the SCA to supersede judicial decisions

³ (See 2 LaFave et. al., *Criminal Procedure* (4th ed. 2020) § 4.8(b).)

upholding the SCA’s default nondisclosure provisions. And, before the Court of Appeal’s Opinion, no court had ever held that the SCA’s protections hinge on a provider’s particular business model. This judicial track record and congressional acquiescence is telling, see *Hassell v. Bird* (2018) 5 Cal.5th 522, 547 [234 Cal.Rptr.3d 867, 420 P.3d 776], and has engendered reliance, including by Snap. This Court should confirm which understanding of the SCA controls.

II. FACTUAL BACKGROUND AND PROCEDURAL HISTORY

A. Snapchat.

Snapchat is a camera and electronic communications application designed for people aged 13 and over. Snapchat users primarily use the app to communicate with close friends and family by sending and receiving messages, photos, and short videos. Snapchat is at heart a visual messaging application, designed for private communications, that encourages creative interactions with friends and family. It is, in many ways, an updated, dynamic version of text messaging.

Snapchat messages auto-delete by default. Users may choose to save communications sent or received through the “Chat” functionality—such as text, photos, videos, and audio notes (“Chats”). Users may also save photos or videos taken with the in-app “Camera” functionality (“Snaps”). Snap maintains saved content on its servers. If a user does not save Chats or Snaps within a certain timeframe, Snap deletes the content. In general, Snap retains content after the default-delete period only if the user chooses to save it.

Snap does not mine, analyze, or share the content of its users’ private communications to provide targeted advertising.⁴ However, Snapchat users grant Snap permission to access their communications for other reasons. They agree Snap may access and review their content “at any time and for any reason,” including to identify “content [that] violates [Snapchat’s] Terms or any applicable law,” “protect the safety of [Snapchat] users, and others,” “investigate, remedy, and enforce potential Terms violations,” and “detect and resolve any fraud or security concerns.”⁵ Users also permit Snap to store, use, and analyze content to improve its services and research and develop new ones.⁶

B. Real Party In Interest Adrian Pina.

Real Party in Interest Adrian Pina (“Pina”) is charged with murder, attempted murder, and felony possession of a firearm, arising from two shootings on December 26, 2021. (Opn. at p. 4.) Pina’s brother Samuel Pina died during one of them. (*Id.* at p. 2.) Pina plans to argue he acted in self-defense and seeks to prove his brother’s violent propensity through content in his brother’s stored communications. (*Id.* at p. 15.)

⁴ (*Privacy Policy* (Feb. 26, 2024) Privacy, Safety, and Policy Hub <<https://bit.ly/46wZfvw>> [as of Aug. 2, 2024].)

⁵ (Snap Inc. Terms of Service (Feb. 26, 2024) <<https://bit.ly/3yA5HyV>> [as of Aug. 2, 2024].)

⁶ (*Id.*)

C. Procedural History.

In October 2023, Snap received a subpoena from Pina seeking “[a]ny and all account information, including posts, photos, and messages” in Samuel Pina’s Snapchat account. (Opn. at p. 5.) Snap responded by letter the same day, objecting, among other things, that the SCA prohibited disclosure of content in response to a defense subpoena. The trial court held a hearing on Snap’s objections to the subpoena, but Snap had no notice of the hearing and did not appear.

Snap thereafter received a second subpoena from Pina and an order from the trial court directing Snap to produce “[a]ll records” in Samuel Pina’s Snapchat account (“Production Order”). (Opn. at p. 5.) The Production Order required Snap to produce the subpoenaed records before or appear at a status conference on January 8, 2024. The Production Order explained the Superior Court had determined at the prior hearing that Pina had good cause for the subpoenaed records.

Snap timely produced responsive non-content records, as the SCA has an explicit exception allowing disclosure of non-content records to non-government entities. (See 18 U.S.C. § 2702(c)(6).) Snap withheld the contents of electronic communications, however. Snap moved to modify the Production Order and quash in part the subpoena, objecting, among other grounds, that the SCA prohibited disclosure of content.

Just hours before the hearing, the Deputy Public Defender representing Pina emailed an opposition brief to Snap, which

raised the business model theory and Chief Justice Cantil-Sakauye's *Touchstone* concurrence.

At the January 2024 status conference, Pina did not raise the business model theory. The trial court recognized Pina had briefed the theory but asked no questions about it or about Snap's business functionality. The trial court ordered Snap to comply with the Production Order in full. It found the Public Defender's Office qualified as a "governmental entity" under the SCA. It also found "probable cause, specifically[,] that this is relevant information." It rejected Snap's SCA arguments, concluding that "all the other arguments and constitutional protections fall by the wayside once . . . a court finds probable cause, which I have." The trial court did not consider the business model theory at all in reaching its conclusion.

Following this ruling, Snap filed a petition for writ of mandate in the Court of Appeal to challenge the Production Order and the Court of Appeal stayed all trial court proceedings. Thus, Snap has not produced the subpoenaed contents. The Court of Appeal consolidated Snap's writ proceeding with one initiated by Meta Platforms Inc. ("Meta"). After briefing by the parties, the Court of Appeal heard the writ petition on July 11, 2024.

In its Opinion issued a few weeks later, the Court of Appeal upheld the Production Order. It endorsed the business model theory, holding that Snap's and Meta's "business models," "under which they access their customer's data for their own business purposes, excludes them from the limitations imposed on the

disclosure of information by the [SCA].” (Opn. at p. 2.) The Court of Appeal ordered: “Let a peremptory writ issue directing respondent court to set aside its order of January 8, 2024, and issue a modified order directing petitioners to produce the subpoenaed information in camera to the respondent court for it to determine whether the material should be produced to Pina’s defense counsel.” (*Id.* at p. 45.)

WHY REVIEW IS WARRANTED

It is difficult to overstate what is at stake here: whether the primary federal statute that protects billions of private electronic communications will continue to deliver the privacy protections the vast majority of Americans depend on. In *Touchstone*, this Court recognized the importance of deciding whether the SCA prohibits providers from disclosing their customers’ communications to third parties. It recognized this issue was not resolved in *Hunter, supra*, 4 Cal.5th 1245, and expressly left it unresolved in *Touchstone, supra*, 10 Cal.5th at p. 361. In her concurrence, Chief Justice Cantil-Sakauye declared this issue “deserves to be addressed when a similar issue arises in analogous future litigation.” (*Touchstone, supra*, 10 Cal.5th at p. 373.) Justice Cuéllar similarly urged that “courts ought” to take up “the crucial matter of how broadly to read the SCA” in a future case. (*Id.* at p. 373 (conc. opn. of Cuéllar, J.)) *This* is that future case.

I. THE COURT OF APPEAL'S ERRONEOUS INTERPRETATION WILL HAVE SIGNIFICANT PUBLIC CONSEQUENCES.

The Court of Appeal's erroneous interpretation of the SCA threatens to: (a) upset the privacy expectations of millions of consumers; (b) burden the courts; and (c) imperil public safety. Congress did not intend these outcomes, which are inconsistent with the SCA's text and purpose. Review is necessary to avoid the adverse consequences of the Court of Appeal's statutory interpretation.

A. The Decision Guts the Primary Federal Statute that Shields Private Electronic Communications from Disclosure.

Americans' personal electronic communications remain private in large part because of Section 2702's disclosure bar. Section 2702 is the linchpin of electronic communications privacy law because it prevents providers from disclosing user contents absent a specific exception.

By enacting the SCA in 1986, Congress recognized the public's privacy interests in then-emerging forms of electronic communications. It established a default prohibition on the disclosure of private communications, Section 2702(a), subject to the exceptions enumerated in Section 2702(b). As technology advanced, this prohibition was universally understood to apply to newer forms of communication, like email, text messages, and social media posts. Congress did not disturb that prevailing understanding in subsequent amendments to the SCA.

The Court of Appeal's re-interpretation of the SCA exposes billions of private communications to compelled production by

mere subpoena—including civil subpoenas. Users entrusted those communications to providers with the understanding they would be held subject to protections from disclosure to third parties. This Court should decide whether those users did so under a mistaken interpretation that the SCA, as commonly understood, would protect them.

Snapchat allows users to securely and privately transmit and store electronic communications with other users, precisely the type of electronic service Congress envisioned the SCA would cover. Millions of Californians use Snapchat every day.⁷

Snapchat users generally expect their communications will remain private. User privacy and agency are central tenets of Snapchat. As Snap’s “Privacy By Product” web page explains:

Saving Snaps was designed with privacy in mind. You control whether your Snaps can be saved within Snapchat. Set the Snap time to no time limit to allow a Snap to be saved. You can always delete any message you’ve sent, including Snaps that have been saved in Chat. Just press and hold to unsave. When you save a Snap, either before or after sending, it can become part of your Memories. When your friend saves a Snap you send them, it can become part of their Memories. Check out the Memories section below for more detailed information about Memories.⁸

It also provides:

Snaps and Chats are private and delete by default, including Voice and Video Chats between you and your friends — meaning we don’t scan their content to

⁷ (Snap Inc. Form 10-Q (Aug. 2, 2024) <<https://bit.ly/3SAwBxA>>, pp. 28-29 [as of Aug. 2, 2024].)

⁸ (*Privacy By Product*, Privacy, Safety, and Policy Hub <<https://bit.ly/3WuPyTq>> [as of Aug. 2, 2024].)

personalize your experience, make recommendations, or show you ads. This means we don't know what you're Chatting or Snapping except in limited, safety-related circumstances (for example, if we receive a report of content that is flagged for violating our Community Guidelines, or to help keep spammers from sending you malware or other harmful content) or unless you ask us to (for example, if you use our Voice Chat Transcription feature).⁹

Snap informs its users that it will “share information about your activity as necessary” to “comply with any valid legal process, governmental request, or applicable law, rule, or regulation.”¹⁰ It explains disclosure “is generally governed by the [SCA],” which “mandates that we disclose certain Snapchat account records only in response to specific types of legal process, including subpoenas, court orders, and search warrants.”¹¹ Snap honors its commitment to user privacy by following its non-disclosure obligations under the SCA, including by challenging subpoenas from private litigants seeking user content. If the decision stands, and stored communications lack protection under Section 2702(a), Snap would be compelled to comply with third-party requests and disclose user content without user consent—and in many cases without the user even having the opportunity to object to the wide scale production of their content.

⁹ (*Id.*)

¹⁰ (*Privacy Policy* (Feb. 26, 2024) Privacy, Safety, and Policy Hub <<https://bit.ly/46wZFvw>> [as of Aug. 2, 2024].)

¹¹ (*Information for Law Enforcement, Privacy, Safety, and Policy Hub* <<https://bit.ly/46ARWge>> [as of Aug. 2, 2024].)

The Opinion’s effects on user privacy are not confined to Snap users in California. As a California corporation, Snap requires domestication of subpoenas seeking records for actions outside California. (Code Civ. Proc., § 1985.6.). The Opinion will govern those subpoenas too, because any motion to quash will be filed in California court and litigated under California law. (See *Unzipped Apparel, LLC v. Bader* (2007) 156 Cal.App.4th 123, 128-30 [67 Cal.Rptr.3d 111] (applying California law to adjudicate out-of-state subpoena domesticated in California, because “California law governs discovery disputes that arise in [California] courts”).)

This Court should clarify when and in what circumstances users relinquish their privacy interests in stored communications. The Court of Appeal held that, “[i]f Snap’s users allow it to use their content for other purposes, they do not have the expectation of privacy contemplated by the SCA.” (Opn. at p. 41.) But courts have held users do not forfeit Fourth Amendment privacy protections by authorizing providers to access their communications. (See *United States v. Warshak* (6th Cir. 2010) 631 F.3d 266, 287 (explaining court was “convinced that some degree of routine access is hardly dispositive with respect to the privacy question”); *United States v. Bychak* (S.D.Cal., May 12, 2022, No. 18-CR-4683-GPC) [2022 WL 1524736, at *6] (“limited monitoring does not alone defeat a privacy expectation in some materials”).) Congress passed the SCA to “expand”—not diminish—“the protections of the Fourth Amendment to new forms of communication and data storage.”

(*In re U.S.* (D.Or. 2009), 665 F.Supp.2d 1210, 1220.) Users deserve consistency to make informed choices about where and how they store communications they intend to keep private.

The Court of Appeal's decision throws into flux the privacy expectations of millions of Snapchat users, contrary to the plain language, stated purpose, and prior prevailing understanding of the SCA. This Court should determine quickly whether it is correct.

B. If This Court Does Not Grant Review, California Courts Will Be Deluged with Subpoenas.

The crucial role of Section 2702 is readily seen in the context of civil litigation. Imagine a typical lawsuit. The parties, bitter at each other, now have the subpoena power. Many litigants would be eager to direct subpoenas to providers used by their opponents to access their emails, text messages, pictures, and videos. The statutory bar of Section 2702 traditionally prevents this. Because communications are protected under the ECS and RCS rules, providers invoke the Section 2702 bar to refuse compliance with civil discovery subpoenas,¹² and the litigants must seek the records elsewhere. Under the business model theory, however, the default privacy wall erected by Section 2702 would be torn down, and California's courts will be burdened by the litigation of countless subpoena disputes.

This is only the tip of the privacy iceberg. Consider the privacy practices of network providers exempt from the

¹² (See LaFave, *supra*, § 4.8(h) (citing cases).)

Section 2702 bar, like those that do not make services available to the public. For example, in *Andersen Consulting v. UOP* (N.D.Ill. 1998) 991 F.Supp.1041, a private company hired consultants and gave them email accounts on its private email server. When the relationship soured, the company contacted the press and released embarrassing emails the consultants had written. The emails were soon splashed across the pages of the *Wall Street Journal*. The disclosure was legal, a court ruled, because Section 2702 expressly exempts providers that do not provide services to the public. (See *id.* at pp. 1042-43.)

Traditionally, the Section 2702 bar has prevented service providers from making disclosures such as those in *Andersen Consulting*. Under the business model theory, however, that would no longer be true as a matter of law. Of course, Snap is committed to protecting the privacy of its users. But not every provider is as scrupulous about protecting its users' privacy as Snap. And an enforceable subpoena would leave Snap with no choice, putting it in an impossible position.

The Court of Appeal's decision will open the subpoena floodgates in civil and criminal litigation. California courts should expect a substantial increase in time devoted to third-party subpoenas in prosecutions. Criminal defendants with little incentive *not* to subpoena providers will trigger motions to quash and good cause hearings. If providers are compelled to produce, the lower courts will more regularly act as evidentiary gatekeepers under Penal Code § 1326, subd. (c). (*Touchstone*, 10 Cal.5th at p. 344.) They will receive often-voluminous account

contents and review them to determine which portions to provide to the issuer. California’s lower courts, already overburdened, will be even more taxed by increased production review.

C. The Court of Appeal’s Decision Undermines Platform Safety and User Security.

The Court of Appeal’s decision provides that if service providers store messages for any reason other than merely backup, then the provider is outside the scope of the SCA. Many providers’ terms of service, including Snap’s, permit providers to access those communications for important safety purposes—such as scanning messages to catch transmission of child sexual abuse material. This Opinion below therefore forces providers to choose between (1) accessing content to remove bad actors and protect their communities, and (2) *not* accessing content to preserve the application of the SCA’s disclosure bar. The effect may be to drive bad actors to platforms that choose the latter, secure in the knowledge the provider will *not* access their communications to detect wrongdoing. The Opinion sends the wrong message on safety, precisely when providers face intense scrutiny about whether and how they should protect their users and the public.

Snap’s public safety program illustrates what hangs in the balance. Snap does not monetize private user content or communications, or sell or share user data with third parties for advertising purposes.¹³ Snap accesses private user content and communications only to enforce its Terms of Service and

¹³ (See *Snapchat Ads Transparency, Privacy, Safety, and Policy Hub* <<https://bit.ly/4dum3YI>> [as of Aug. 2, 2024].)

Community Guidelines by identifying, preventing, and responding to wrongdoing.¹⁴ For example, Snap scans image and video uploads to Snapchat for known child sexual abuse material and reports such content to the National Center for Missing and Exploited Children. Snap identifies and responds to reports of content involving unlawful drug activities, disables offending accounts, bans associated devices, and makes law enforcement referrals.¹⁵ Snap also responds to reports of content involving terror threats, bullying, and other problematic behavior in violation of Snap’s Community Guidelines. In 2023 alone, Snap made over 690,000 reports of suspected child sexual abuse material to the appropriate authorities, resulting in more than 1,000 arrests, and “removed more than 2.2 million pieces of drug-related content, disabled the 705,000 related accounts, and blocked the devices associated with those accounts from using Snapchat.”¹⁶ Virtually all other commercial electronic communications providers do some version of the same activity to secure their platforms, remove wrongdoers, and protect their users and the public.

The Court of Appeal’s decision forces providers to abandon such efforts or otherwise face liability under the SCA for

¹⁴ (*Learn About How Snap Uses Data*, Snapchat Support <<https://bit.ly/3AasstM>> [as of Aug. 2, 2024].)

¹⁵ (*Testimony of Evan Spiegel Co-Founder and CEO, Snap Inc.* (January 2023), Hearing before the United States Senate Committee on the Judiciary <<https://bit.ly/3YACvTj>> [as of Aug. 2, 2024].)

¹⁶ (*Id.*)

protecting user content against disclosure. This Court should decide now whether the SCA genuinely compels that choice to be made.

II. CALIFORNIA COURTS NEED IMMEDIATE GUIDANCE IN APPLYING THE BUSINESS MODEL THEORY

The Court of Appeal's endorsement of the business model theory embarks on a tectonic shift after nearly 40 years without a business model theory of the SCA. But the Opinion also leaves the scope and application of this novel theory surprisingly unclear—impacting countless providers and the users they serve. If the business model theory is to be the law in California courts, this Court should grant review to provide much-needed guidance to the California courts on how to interpret and apply it.

The Court of Appeal's decision is frustratingly ambiguous as to its scope and application. We know, by its holding, that its reasoning applies to Snap and Meta, as long as they retain their current terms of service. But the decision does not say what steps Snap can take, especially in terms of changing its terms of service going forward, to restore the privacy protections that the Court of Appeal's decision eliminates.

The Court of Appeal's decision also leaves open how it applies to the endless array of other services and providers that make up the modern internet economy. Before the decision, it was well understood that the SCA applied to providers of email services and online messaging platforms. (See, e.g., *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 889 [179 Cal.Rptr.3d 215] (applying the SCA to private messaging services (email));

State v. Johnson (Tenn. Crim. App. 2017) 538 S.W.3d 32, 69 (“[T]he SCA is applicable to communications shared on social media websites.”); *United States v. Peterson* (W.D.Mo., July 18, 2023, No. 22-00196-01-CR-W-DGK) [2023 WL 5920869, at *7], *report and recommendation adopted*, (W.D.Mo., September 11, 2023, No. 4:22-CR-0166-DGK-02) [2023 WL 5918310] (generally describing Snap as an ECS in confirming that the SCA applies to Snap).) Under the Court of Appeal’s decision, however, email, text, and other private content held by these providers would no longer be covered under the SCA.

The Opinion is also unclear about what conduct nullifies SCA protection under the business model theory. It states only that “maintain[ing] that content for their own business purposes” or “their own profit-driven purposes” took Snap and Meta outside the SCA’s disclosure bar. (Opn. at p. 38-39.) That provides no clarity to providers and users about what “purposes” comply with the SCA. Although the Court of Appeal’s decision appears grounded against “profit-driven purposes,” (see *Id.* at p. 39) that leaves unclear what non-profit-driven purposes providers can pursue while maintaining protection against disclosure under the SCA.

As Chief Justice Cantil-Sakauye’s concurrence in *Touchstone* suggests:

It would seem that protection against malware and viruses, etc., might be viewed as reasonably necessary to ensure the safety and integrity of any computer system, and in that sense, such monitoring and resulting measures to counteract malware might well be found to fall within a narrower definition of

‘computer processing,’ even if that same term would not broadly encompass the sharing with third party advertisers of mined and analyzed information about content.

(*Touchstone, supra*, 10 Cal.5th 329, 372 fn.14 (conc. opn. of Cantil-Sakauye, C.J.)) With that in mind, this Court should provide immediate guidance about agreements between providers and their users, and how authorization affects protection under the SCA.

By failing to provide any clear answer to how far the business model theory extends, the Court of Appeal’s ruling leaves the Superior Courts, providers, and the public unable to determine the basic rules of internet privacy under the SCA. Clarification by this Court is necessary to understand the effect of this major shift.

III. THE COURT OF APPEAL’S SHARP DEPARTURE FROM PRIOR PRECEDENT WARRANTS THIS COURT’S REVIEW.

The Court of Appeal’s ruling conflicts with preexisting understandings of the SCA in two ways. First, its reasoning that there is no ECS protection for the subpoenaed content conflicts with Ninth Circuit and Fourth Circuit precedent. Second, and more broadly, its reasoning as to Section 2702(a) protections is a novel departure from settled understandings of the SCA.

A. The Court of Appeal’s Interpretation of The SCA’s ECS Protections Conflicts with Precedent from the Ninth and Fourth Circuits.

There is a significant body of caselaw in federal and state courts on the scope of the SCA’s ECS protections. (See *Anzaldua v. Northeast Ambulance and Fire Protection District* (8th Cir.

2015) 793 F.3d 822, 840-42 (summarizing caselaw).) The key question is the meaning of the phrase “for purposes of backup protection of such communication” in Section 2510(17)(B). This interpretation is crucial because a provider holding a communication “for purposes of backup protection” protects that communication under the ECS rules, prohibiting disclosure under Section 2702(a)(1) because it is in “electronic storage.” But whose “purpose” matters—the provider’s or the user’s? And how do the protections apply if there are multiple purposes?

In *Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, the Ninth Circuit adopted a broad view of the SCA’s ECS protections by ruling that either party’s purpose is sufficient to protect the communication under the “electronic storage” definition. The issue in *Theofel* was whether previously opened emails stored with an internet service provider were in “electronic storage” because they were held “for purposes of backup protection” under Section 2510(17)(B). (See *id.* at p. 1075, citation omitted.) The Ninth Circuit concluded that they were. The ordinary meaning of “backup protection,” the Ninth Circuit ruled, covers “any backup purpose.” (*Id.* at p. 1076.) This broad view of the SCA’s protections was justified, the Ninth Circuit reasoned, because “nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user.” (*Id.* at p. 1075.)

Under the Ninth Circuit’s reasoning in *Theofel*, all stored messages held by a service provider in an internet account are ordinarily protected under the ECS rules. (See *Theofel, supra*, at pp. 1075-76.) Because a user’s purpose in keeping a backup

triggers the “electronic storage” definition, the Section 2702 bar applies and prevents disclosure of messaging contents unless a specific exception applies. (See *ibid.*)

The Fourth Circuit agreed with the Ninth Circuit, adopting a similarly broad view of the phrase “for purposes of backup protection,” in *Hately, supra*, 917 F.3d 770. *Hately* ruled that emails held in storage by a web-based email provider are stored for purposes of backup protection “because that is a feature users desire.” (*Id.* at p. 794.) Specifically, storing email “afford[ed] the user a place to store messages the user does not want destroyed.” (*Id.* at 793.) Because the purpose of email storage was for the user’s backup, it was stored for purposes of backup protection under the statute. (*Ibid.*)

In its Opinion below, the Court of Appeal below took a very different approach. It reasoned that a provider storing contents for “profit-driven purposes” eliminates the SCA’s protection. This was so, the Court of Appeal reasoned, because a company’s purpose to store user contents “for their own business purposes” has the effect of “bring[ing] the content outside the SCA’s plain definition of ECS provider.” (Opn. at p. 39.) In other words, the only purpose that matters, in determining what counts as “purposes of backup protection,” Section 2510(17)(B), is the *provider’s* purpose. And if a company has multiple purposes in storing the data, the existence of a business purpose—among other purposes—eliminates protection. The result is a very narrow interpretation of ECS protections, in which a provider’s

business purpose eliminates the statute’s protections for content messages. (*Id.* at pp. 38-39.)

The difference is stark. Under the Fourth Circuit and Ninth Circuit rule, contents held by an ECS provider are broadly protected from disclosure. Under the ruling below, the same contents are not protected.

B. The Court of Appeal’s “Business Model” Theory Is a Novel Departure from Prevailing Understandings of the SCA.

The “business model” theory is a novel development. It is so novel that it has not even been part of the rich legislative debates over the SCA. Prominent treatises and casebooks that detail the SCA at length, and which cover the specific rules of the Section 2702 bar, do not even mention it.¹⁷ As the Court of Appeal recognized, whether content held by providers is protected by the SCA has been considered so settled in the affirmative that it did not warrant analysis. (*Opn.* at p. 39, fn.17.) This includes *Hunter*, where this Court said it had “no reason to question” that Facebook was subject to the SCA. 4 Cal. 5th at 1268.

Notably, Congress recently enacted major legislation amending the SCA that would have been redundant under the Court of Appeal’s interpretation. The Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 creates a specific exception to the Section 2702 bar that allows providers to comply with foreign court orders if a country has been pre-approved by the Attorney

¹⁷ (See, e.g., LaFave, *supra*, § 4.8; Carr & Bellia, *Law of Electronic Surveillance* (1st ed. 2024) § 4:97; Kerr, *Computer Crime Law* (5th ed. 2022) pp. 712-56.)

General. (See 18 U.S.C. § 2702(b)(8)) (permitting disclosure “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 [S]ection 2523”); (18 U.S.C. § 2523) (providing the procedure for Attorney General certification).)

As the extensive debate over the CLOUD Act shows, these provisions were enacted because Section 2702 was understood to block U.S. providers from complying with foreign government court orders.¹⁸ The CLOUD Act offered a limited, nuanced, and carefully-drafted way around the Section 2702 bar on disclosure.¹⁹ Under the Court of Appeal’s ruling, however, this important legislation was not actually needed. The Section 2702 bar did not apply in the first place. But, as far as Snap can discern, no one involved in the passage of the CLOUD Act ever mentioned this possibility in any of the debates over the need for this new exception.

¹⁸ (See Woods & Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, (Feb. 6, 2018) Lawfare <<https://bit.ly/3LQWKES>> [as of Aug. 2, 2024] [noting that the law “removes a number of blocking features—those provisions of American law that prevent American providers from complying with lawful foreign law enforcement requests, which are the sources of enormous frustration for American providers and foreign law enforcement alike”].)

¹⁹ (See *id.*)

IV. THE COURT OF APPEAL'S DECISION IS WRONG

A. Snap Is Prohibited from Disclosing Content Held in Electronic Storage, even if Snap Accesses the Same Content for an Unenumerated Purpose.

The Court of Appeal interpreted Section 2702(a)(1) to apply very narrowly as a bar to disclosure by ECS providers. Under its ruling, an ECS provider is barred from disclosing user contents only when it stores contents for the sole purpose of temporary or backup storage. (Opn. at pp. 38-39.) This limitation does not exist in the statute. And the Court of Appeal cites no precedent for its novel limiting construction.

Section 2702(a)(1) provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” The statute defines “electronic storage” as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) 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).)

As cases like *Theofel* and *Hately* recognize, the phrase “for purposes of backup protection” is broad. Americans routinely use the internet to store their most private communications. They store their messages and photos in the cloud, or with social media services, because they want to be able to access a copy of those files should they need it. In other words, they store that copy “for backup purposes.” (*Hately, supra*, 917 F.3d at p. 793 (holding

that web-based email is in “electronic storage” because it gives users “a place to store messages the user does not want destroyed”).)

The Court of Appeal invented a new limit on the SCA’s protections: If a provider holds user contents at least in part for “their own profit-driven purposes,” then those contents are not being held for purposes of backup protection. (Opn. at p. 39.) But this test is unworkable. Providers covered by the Section 2702 bar—the commercial providers that provide services “to the public”—are mostly for-profit companies. Most are public companies with publicly-traded stock. Trying to divine the true purpose of a corporation’s storing of a user’s file, and eliminating privacy protection if the corporation is acting to turn a profit, does not align with the purpose of the SCA to protect user privacy.

The Court of Appeal’s rationale also has no support in the plain language of the statute. The SCA sets no limit on the number of reasons an ECS provider might hold content before it loses SCA coverage. The only textual requirement in Section 2702(a)(1) is that the provider must hold the communications in electronic storage—meaning, temporary or backup storage. It does not say “solely” or “only” electronic storage. Congress plainly knew how to insert that type of limiting language. It did so in the very next subsection: Section 2702(a)(2) contains the limiter “solely.” The inconsistent interpretive methodology alone commends review by this Court. (See *People v. Lewis* (2021), 11 Cal.5th 952, 961-62

[281 Cal.Rptr.3d 521, 491 P.3d 309], citation omitted (“statutory sections relating to the same subject must be harmonized, both internally and with each other”).)

The Court of Appeal relied on *Juror Number One v. Superior Court*, (2012) 206 Cal.App.4th 854 [142 Cal.Rptr.3d 151]. (Opn. at p. 38.) There, the Third District said, “only copies of electronic communications held by the ECS pending initial delivery to the addressee or held thereafter for backup purposes are protected.” (*Id.* at p. 861.) That formulation is consistent with the statute: *only* content held in electronic storage is protected by the SCA. But that is very different from the Court of Appeal’s construction: content that is held by providers for *only* non-profit purposes is protected by the SCA.²⁰

The Court of Appeal also cites *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002) 302 F.3d 868, 875, which held “Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards.” This general observation from the Ninth Circuit is uncontroversial. But the more important point is that, two years after *Konop*, the Ninth Circuit interpreted “electronic storage” in *Theofel v. Farey-Jones*, and that interpretation is inconsistent with the Opinion’s interpretation. (See, *supra*, Part III.A.) In addition, the Court of Appeals overlooks that, unlike Section

²⁰ To the extent the Court of Appeal and the *Touchstone* concurrences seem animated primarily by a concern about targeted advertising, this Court should consider in deciding whether to grant review that Snap does not access *private user content or communications* for advertising purposes.

2702(a)(2), protection under § 2702(a)(1) does not turn on “authorization.” (See Opn. at p. 39.) It turns on the type of storage the content is actually in. Whether its users *authorize* Snap to access their content for purposes other than electronic storage is irrelevant under Section 2702(a)(1).

B. Snap Is Prohibited from Disclosing Content Stored on Behalf of Its Users.

This Court should also review the Court of Appeal’s interpretation of Section 2702(a)(2), which eliminates SCA protection of communications stored by an RCS authorized by its users to access their content for purposes other than storage and processing. (Opn. at p. 40-41.) As with its treatment of Section 2702(a)(1), the court offers no authority supporting its novel reading of Section 2702(a)(2), the effect of which is to strip privacy protections from stored communications.

According to the Court of Appeal, “under the plain language of Section 2702(a)(2), because Snap and Meta are not maintaining communications ‘solely for the purpose of providing storage or computer processing services’ to their users, the SCA does not preclude them from disclosing the material sought by Pina’s subpoenas.” (Opn. at p. 40.)

The key issue is the interpretation of Section 2702(a)(2)(B), which the Court of Appeals recognized was “not ‘a model of clarity.’” (Opn. at p. 41) (citing *Touchstone, supra*, 10 Cal.5th at p. 365 (conc. opn. of Cantil-Sakauye, C.J.)). Yet, rather than proceed with caution, it announced a sweeping new interpretation that removes SCA protection from billions of stored communications. And it did so without citing any

precedent or grappling with interpretive questions raised by the parties. Among other things, the court misconstrued Snap’s textual reading as saying content held solely for storage or processing is subject to the SCA only if the user *does* authorize access for other purposes. (Opn. at p. 40.) Snap’s position was just the opposite. It also ignored the argument that accessing content for platform integrity and trust and safety is inherent in providing storage and computer processing, and so not a separate purpose at all.

A STAY IS WARRANTED

This Court should grant a stay to ensure that trial court proceedings remain stayed pending review in this Court. The trial court ordered the production of subpoenaed documents by January 18, 2024. The Court of Appeal granted a stay of the order compelling production of subpoena documents, but then stated in its disposition that “[t]he stay issued by this court on January 24, 2024 is vacated on August 2, 2024 and this decision is final forthwith.” (Opn. at p. 45.) Although the peremptory writ of mandate has not issued and is not effective until proceedings in this Court conclude (*Ng v. Superior Court* (1992) 4 Cal.4th 29, 33-35 [13 Cal.Rptr.2d 856, 840 P.2d 961]), the trial court entered an *ex parte* Order on August 2, 2024, a copy of which is attached as Attachment B, ordering Snap to “produce the subpoenaed records *in camera*” to the court by “August 5, 2024.”

If the trial court concludes that the Court of Appeal has vacated the stay of trial proceedings and that a writ petition does not otherwise stay proceedings (*In re Brandy R.* (2007)

150 Cal.App.4th 607, 609-610 [58 Cal.Rptr.3d 456]), it may conclude that it has inherent authority to revisit its order, even if the peremptory writ has not issued, and then compel production for *in camera* inspection. This would impede and interfere with review by this Court, given that Snap claims that such production would violate federal law, and the trial court would have compelled such violation before this Court had an opportunity to review the question presented.

Thus, to preserve appellate jurisdiction (see *Stewart v. Hurt* (1937) 9 Cal.2d 39, 41 [68 P.2d 726]), avoid confusion, and prevent irreparable harm arising from the production of private electronic communications, this Court should stay proceedings in the trial court pending the completion of this Court's review.

CONCLUSION

Based on the importance of questions presented, as well as authorities discussed in the foregoing which show a need for consideration by this Court, Snap respectfully seeks review.

Dated: August 5, 2024

LAW OFFICE OF ORIN S. KERR

By: /s/ Orin Kerr

Orin Kerr

FENWICK & WEST LLP

By: /s/ David W. Feder

David W. Feder (*pro hac vice*
application pending)

Attorneys for Petitioner
SNAP INC.

CERTIFICATE OF WORD COUNT

In accordance with California Rules of Court Rule 8.504(d)(1), I certify that exclusive of this certification and the other exclusions reference in Rule of Court 8.204(c)(3), this PETITION FOR REVIEW contains 7,918 words, including footnotes, as determined by the word count of the computer used to prepare this brief.

Dated: August 5, 2024

LAW OFFICE OF ORIN S. KERR

By: /s/ Orin Kerr

Orin Kerr

FENWICK & WEST LLP

By: /s/ David W. Feder

David W. Feder (*pro hac vice
application pending*)

Attorneys for Petitioner
SNAP INC.

PROOF OF SERVICE

I certify that on August 5, 2024, I electronically filed **PETITIONER SNAP INC.'S PETITION FOR REVIEW** with the Clerk of the Court using the TrueFiling system which will be served by operation of the Court's electronic filing system to all parties below:

Summer Stephan
District Attorney
Linh Lam
Deputy District Attorney
Chief, Appellate & Training
Division
Karl Husoe
Deputy District Attorney
330 W. Broadway, Suite 860
San Diego, CA 92101
Email: karl.husoe@sdcca.org
*Counsel for The People,
Real Party in Interest*

Paul Rodriguez
Public Defender
Office of the Primary Public
Defender
Troy A. Britt
451 A. Street, Suite 900
San Diego, CA 92101
Email:
troy.britt@sdcounty.ca.gov
*Counsel for Real Party in
Interest
Adrian Pina*

David Jarman
Office of San Diego County
District Attorney
North County Regional Center
325 S. Melrose Drive, Suite 5000
Vista, CA 92081
Email: david.jarman@sdcca.org
*Counsel for The People,
Real Party in Interest*

Nadine Valdecini
San Diego County Department of
the Public Defender
451 A Street, Suite 900
San Diego, CA 92101
Email:
nadine.valdecini@sdcounty.ca.gov
*Counsel for Real Party in Interest
Adrian Pina*

Julie Schwartz
Ryan Mrazik
John R. Tyler
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Email:
jschwartz@perkinscoie.com
namlani@perkinscoie.com
rmrazik@perkinscoie.com
rtyler@perkinscoie.com

Natasha Amlani
Perkins Coie LLP
1888 Century Park East
Suite 1700
Los Angeles, CA 90067

*Counsel for Petitioner
Meta Platforms, Inc.*

Joshua S. Lipshutz
Gibson, Dunn & Crutcher LLP
One Embarcadero Center, # 2600
San Francisco, CA 94111
Email:
jlipshutz@gibsondunn.com

Michael J. Holecek
Gibson, Dunn & Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071
Email:
mholecek@gibsondunn.com

Natalie J. Hausknecht
Gibson, Dunn & Crutcher LLP
1801 California Street
Suite 4200
Denver, CO 80202
Email:
nhausknecht@gibsondunn.com

*Counsel for Petitioner
Meta Platforms, Inc.*

Additionally, a copy of **PETITIONER SNAP, INC.’S PETITION FOR REVIEW** will be served by U.S. Mail to the following addresses:

Honorable Daniel Link
Superior Court of California
County of San Diego
325 S. Melrose Drive
Department 21
Vista, CA
Email: appeals.central.sdcourt.ca.gov

Court of Appeal, Fourth Appellate
District, Division One
750 B Street, Suite 300
San, Diego, CA 92101

Dated: August 5, 2024

LAW OFFICE OF ORIN S. KERR

By: /s/ Orin Kerr
Orin Kerr

FENWICK & WEST LLP

By: /s/ David W. Feder
David W. Feder (*pro hac vice*
application pending)

Attorneys for Petitioner
SNAP INC.

Attachment A

CERTIFIED FOR PUBLICATION

COURT OF APPEAL, FOURTH APPELLATE DISTRICT

DIVISION ONE

STATE OF CALIFORNIA

SNAP, INC.,

Petitioner,

v.

THE SUPERIOR COURT OF SAN
DIEGO COUNTY,

Respondent;

ADRIAN PINA et al.,

Real Parties in Interest.

D083446

(San Diego County
Super. Ct. No. SCN429787)

META PLATFORMS INC.,

Petitioner,

v.

THE SUPERIOR COURT OF SAN
DIEGO COUNTY,

Respondent;

ADRIAN PINA et al.,

Real Parties in Interest.

D083475

(San Diego County
Super. Ct. No. SCN429787)

ORIGINAL PROCEEDINGS on petitions for writs of mandate.

Daniel F. Link, Judge. Relief denied in part and granted in part, peremptory writ issued modifying order.

Fenwick & West, Tyler G. Newby, Janie Yoo Miller, Esther D. Galan, and David W. Feder for Petitioner Snap, Inc.

Perkins Coie, Julie E. Schwartz, Natasha Amlani, Michel C. Bleicher, and Ryan Mrazik for Petitioner Meta Platforms, Inc.

Paul Rodriguez, Public Defender, Troy A. Britt, Deputy Public Defender, for Real Party in Interest Adrian Pina.

Summer Stephen, District Attorney, Linh Lam and Karl Husoe, Deputy District Attorneys for Real Party in Interest The People.

This writ proceeding presents a question of first impression that was raised but not decided by the California Supreme Court in *Facebook, Inc. v. Superior Court* (2020) 10 Cal.5th 329 (*Touchstone*): Whether the business models of social media companies like Meta, Inc. (Meta) and Snap, Inc. (Snap), under which they access their customer's data for their own business purposes, excludes them from the limitations imposed on the disclosure of information by the Stored Communications Act (18 U.S.C. § 2701 et seq., SCA or the Act¹). As we shall explain, we conclude that the companies' ability to access and use their customers' information takes them outside the strictures of the Act.

Adrian Pina, real party in interest, was charged with the murder of his brother, Samuel, and the attempted murder of another man, and currently awaits trial on the charges. Last September, Pina's defense counsel issued

¹ All further section citations are to title 18 of the United States Code unless otherwise indicated.

criminal defense subpoenas to Snap, the corporation which operates Snapchat, and Meta, the corporation that operates Facebook and Instagram, seeking social media posts and other communications made by Samuel on those platforms in the two years prior to his death. Pina seeks this material because he believes it may contain information relevant to his defense, specifically showing Samuel's violent character.

After Snap sent a letter to Pina's counsel indicating it would not provide the requested information and Meta ignored the initial subpoena, the trial court issued an order directing compliance by a hearing set for January 8, 2024. This prompted Snap to file a motion to quash the subpoena, asserting its compliance with it was precluded by the SCA. Meta filed a motion to quash during the January 8, 2024 hearing. At the conclusion of that hearing, the court denied both motions.

Snap and Meta promptly petitioned this court for writs of mandate staying the trial and vacating the trial court's order. In response, we issued an order to show cause, stayed the trial court proceedings, and consolidated the two petitions. Among other arguments, Snap and Meta assert the trial court's order requiring them to disclose the requested communications and data to Pina is precluded by the SCA and that the trial court failed to make the good cause findings required for this pretrial discovery under *Touchstone*.

We agree with Pina that the trial court conducted a sufficient analysis of good cause, that the facts presented by Pina supported the court's determination that good cause existed, and that because the business models of Snap and Meta provide them with the ability to access and use the information sought by Pina, the SCA does not foreclose production of that information. However, we agree with Pina that the material should not be disclosed directly to him. Rather, under Penal Code section 1326,

subdivision (d), the material should first be produced to the trial court in camera for the court to determine whether the material is relevant to Pina's defense and if it should be produced to him.

FACTUAL AND PROCEDURAL BACKGROUND

Pina is charged with murder (Pen. Code, § 187), attempted murder (*id.*, §§ 664, 187), and possession of a firearm by a felon (*id.*, § 29800). The murder and firearm charges relate to the shooting death of Samuel that took place on December 26, 2021. The attempted murder charge relates to a shooting incident involving another victim that is alleged to have occurred earlier the same day. During the preliminary hearing on December 7, 2022, Samuel's girlfriend testified that Samuel and Pina shared the gun used in his murder. She also stated she had posted a picture of Samuel with another gun on her Snapchat account, and that the photo might be saved in her "Snapchat memories."

During pretrial discovery, the prosecution provided Pina's defense counsel with an extraction of data from Samuel's cell phone. According to Pina's counsel, the extraction contained over 100,000 PDF pages and was not in a format that allowed for viewing of the raw data or navigation through the phone's contents. On October 20, 2023, defense counsel brought a partially successful motion to compel, and was permitted to view the phone at the Oceanside Police Department. The phone contained videos of fights and suggested gang affiliation, and showed there was data on the phone that was not previously provided to Pina's defense counsel. This resulted in an additional court order to "re-extract" Samuel's cell phone data and provide the full contents, including its raw data, to Pina's counsel. The defense received the data on November 16, 2023.

The information defense counsel viewed on the cell phone also prompted Pina’s counsel to believe that Samuel’s social media accounts might contain relevant evidence to support Pina’s defense. On September 26 and 28, 2023, respectively, Pina issued subpoenas duces tecum to Snap and Meta to compel the corporations to bring to court or produce to the defense the contents of Samuel’s social media accounts on or by October 20, 2023. The subpoena to Snap called for the production of “any and all account information, including posts, photos, and messages” The subpoena to Meta called for the production of “[a]ll records associated with Samuel’s account including basic subscriber records as well as stored contents of the account, including timeline posts, messages, phone calls, videos, location information, and information from 1/1/2020 to December 31, 2021.”

In response to the subpoena, on October 16, 2023, Snap sent a letter to defense counsel objecting and stating it would not produce any records. Meta did not respond to the subpoena. On December 8, 2023, the trial court signed an order directing both corporations to produce the records, which, on December 12, 2023, defense counsel served on Snap and Meta with new versions of the subpoenas.² The production was ordered by January 8, 2024, and a hearing was set for the same date.

On December 29, 2023, Snap filed a motion to modify in part, and quash in part the subpoena. Snap agreed to produce basic subscriber information, but asserted it could not provide any additional information because doing so was prohibited by the SCA. Meta did not file any response

² The subpoena to Snap was updated to request: “(1) All records associated with Samuel Pina’s account, including basic subscriber records as well as stored (2) contents of the account including posts, photos, messages, phone calls, videos, location information, and (3) information from 1/1/2020 to December 31, 2021.” The subpoena to Meta was unchanged.

to the subpoena before the January 8, 2024 hearing date, but did submit a motion to vacate, modify, or quash Pina's subpoena during the hearing. Like Snap, Meta asserted the communications and data sought by Pina were protected by the SCA, as well as the Revised Uniform Fiduciary Access to Digital Assets Act (Prob. Code, § 870 et seq.). Meta also argued that Pina had not shown good cause for the requested information. Specifically, it argued Pina had not shown any relationship between the requested information and his defense, or that he could not obtain the information from other sources. Finally, Meta argued it was deprived of due process because it had no record of receiving Pina's first subpoena and thus had no opportunity to object.

Also on the date of the hearing, Pina filed an opposition to Snap's motion to quash. Pina, citing *Touchstone, supra*, 10 Cal.5th 329, asserted Snap did not fall within the purview of the SCA because its terms of service require users to agree to allow Snap to retain and use the information they put on Snapchat for its own business purposes. Pina also asserted his right to prepare his defense, specifically to show Samuel's violent nature, outweighed any privacy concern of Samuel.

At the hearing, the trial court indicated it was inclined to deny both Snap's and Meta's motions. The court noted Snap's and Meta's arguments, and Pina's assertion that the communications at issue were not protected by the SCA because the corporations "mine data" and use it for profit. The court was also concerned with the lopsided nature of Snap and Meta's position, noting "the problem I'm having ... let's say that this subpoena came from the prosecution or ... from a law enforcement agency, hypothetically [the] San Diego Police Department, or just this court ... would you have filed a motion to quash?" Snap's and Meta's counsel both responded they would have

complied with a valid search warrant for the same information. The prosecutor stated she did not oppose Pina's request for this information. She also stated, however, that she was not willing to seek the information herself because the "Oceanside Police Department ha[d] conducted [its] investigation," the prosecution had the evidence it needed and was ready to proceed to trial, and Pina was conducting a "fishing expedition" to try to paint Samuel "in a negative light, as a violent person."

The court then stated it had already determined by its prior order compelling the production that the information sought was relevant and that there was probable cause for the information. Snap's counsel responded that probable cause was not the proper standard for the court to consider, and instead the court was required to assess good cause under the factors set forth in *Touchstone*. The court agreed and then specifically discussed those factors, finding the material sought was not publicly available, there was no other way for Pina to obtain the material, and that Pina had shown a plausible justification for the material based on the information he submitted from Samuel's cell phone, which had been provided to the defense by the Oceanside police. Pina's counsel noted that Snap had not argued that good cause for the subpoena was lacking in its motion to quash, instead relying entirely on the SCA, and that the information submitted by Pina in support of his opposition to the motion showed good cause.

Meta's counsel then requested a continuance of the hearing to allow it to receive opposition to its motion filed that day, which Pina's counsel had yet to receive. Like Snap, Meta also argued the SCA precluded it from providing the communications and data sought by Pina. The trial court stated it understood counsel's arguments, but was finding sufficient probable cause existed and denied both motions to quash. The court ordered the production

of the information by January 18, 2024. On January 12, 2024, Snap filed a motion to stay the production pending the resolution of its forthcoming petition for a writ of mandate. The court granted the motion extending the deadline to produce the information to February 2, 2024.

Snap filed its petition for writ of mandate in this court on January 17, 2024, and Meta filed its petition on January 19, 2024. We then issued an order staying the proceedings in the trial court and requesting informal responses from real parties in interest Pina and the District Attorney. After receiving the informal responses, we consolidated the two cases, issued an order to show cause, and set deadlines for the filing of the real parties' return and the petitioners' reply briefs.

DISCUSSION

In their petitions, both Snap and Meta argue that the trial court's order denying their motions to quash was flawed because Pina did not establish good cause for the subpoenaed material. The District Attorney sides with the corporate third parties, asserting the court failed to conduct an adequate analysis under *Touchstone*. Pina argues that the court's analysis was sufficient, and the court did not err in finding he established good cause for the material, which he argues may contain information helpful to his defense.

Snap and Meta also assert that the production of the requested material is precluded by the SCA. The District Attorney responds that these entities are not covered by the SCA in this case, and they have presented insufficient evidence to establish they constitute electronic communication service (ECS), or remote computing service (RCS) providers as defined by that law. Pina also asserts that Snap and Meta do not qualify as ECS or RCS providers and, therefore, the SCA does not prevent production of the requested material. He also contends that the SCA would be

unconstitutional if it were applied in this case because it would violate his equal protection, due process, and fair trial rights.

I

Law Governing a Motion to Quash a Subpoena Duces Tecum

Touchstone, supra, 10 Cal.5th 329, provides a helpful starting point. There, the Supreme Court set forth the relevant statutes and case law that relate to the issuance of criminal subpoenas.³ “Under Penal Code section 1326, subdivision (a), various officials or persons—including defense counsel, and any judge of the superior court—may issue a criminal subpoena duces tecum, and, unlike civil subpoenas, there is no statutory requirement of a “‘good cause’” affidavit before such a subpoena may be issued. [Citations.] It is important to note, however, that such a criminal subpoena does not command, or even allow, the recipient to provide materials directly to the requesting party. Instead, under subdivision [(d)] of section 1326, the sought materials must be given *to the superior court* for its in camera review so that it may ‘determine whether or not the [requesting party] is entitled to receive the documents.’ (Pen. Code, § 1326, subd. [(d)]; see also *People v. Blair* (1979) 25 Cal.3d 640, 651 [such materials cannot legally be given directly to the requesting party].)” (*Touchstone*, at pp. 343–344.)

“Although no substantial showing is required to *issue* a criminal subpoena duces tecum, as explained below, in order to *defend* such a

³ Meta argues that because the California Electronic Communication Privacy Act (Pen. Code, § 1546 et seq., CalECPA) requires *the government* to obtain a search warrant in order to compel it to turn over content, that statute entirely forbids a defendant in a criminal trial from obtaining such information. This is not an accurate assertion of the law. Rather, as we shall discuss, criminal defendants have the opportunity to obtain discovery of relevant information to their defense through the procedure set forth in Penal Code section 1326.

subpoena against a motion to quash, the subpoenaing party must at that point establish good cause to acquire the subpoenaed records. In other words, as we have observed, at the motion to quash stage the defendant must show ‘some cause for discovery other than “a mere desire for the benefit of all information.” ’ ” (*Touchstone, supra*, 10 Cal.5th at p. 344; see also *People v. Madrigal* (2023) 93 Cal.App.5th 219, 256 (*Madrigal*) [“To acquire the materials, the defendant must make a showing of good cause—that is, specific facts justifying discovery.”].) “ “[T]he good cause requirement embodies a ‘relatively low threshold’ for discovery.” ’ ... An accused is entitled to any “pretrial knowledge of any unprivileged evidence, or information that *might lead to the discovery of evidence*, if it appears reasonable that such knowledge will assist him in preparing his defense...” ’ ” (*Id.*, at pp. 256–257, italics added.)

To determine whether good cause has been established, the *Touchstone* court looked to the seven factors set forth in *City of Alhambra v. Superior Court* (1988) 205 Cal.App.3d 1118 (*Alhambra*). “ [T]he trial court ... must consider and balance’ [these seven factors] when ‘deciding whether the defendant shall be permitted to obtain *discovery* of the requested material.’ ”⁴ (*Touchstone, supra*, 10 Cal.5th at p. 344.) First, the defendant must show a “ “plausible justification” ’ for acquiring documents from a third party [citations] by presenting specific facts demonstrating that the subpoenaed documents are admissible or might lead to admissible evidence that will reasonably “assist [the defendant] in preparing his defense.” ’ ” (*Touchstone*, at p. 345.) The defendant is not permitted to go on “an impermissible

⁴ “For convenience,” the *Touchstone* court referred “to these seven considerations as the ‘*Alhambra* factors.’ ” (*Touchstone, supra*, 10 Cal.5th at p. 347.) We do the same.

“fishing expedition.”” (*Ibid.*) This factor is the “most significant” of the seven. (*Id.* at p. 345, fn. 6.)

Second, the material sought must be “adequately described and not overly broad.” (*Touchstone, supra*, 10 Cal.5th at p. 346.) Third, the court must consider if “the material [is] ‘reasonably available to the ... entity from which it is sought (and *not* readily available to the defendant from other sources).” (*Ibid.*) Fourth, the court must consider whether “production of the requested materials violate a third party’s ‘confidentiality or privacy rights’ or intrude upon ‘any protected governmental interest.’” (*Ibid.*) Fifth, the request must be timely, and not premature. (*Id.* at p. 347.) Sixth, the court must consider whether “the ‘time required to produce the requested information ... [would] necessitate an unreasonable delay of defendant’s trial.’” (*Ibid.*) And finally, the court must assess whether “‘production of the records containing the requested information ... place[s] an unreasonable burden on the [third party].’” (*Ibid.*)

We review the trial court’s decision denying a motion to quash a criminal subpoena for abuse of discretion. (*Pitchess v. Superior Court* (1974) 11 Cal.3d 531, 534.)

II

The Trial Court Did Not Abuse Its Discretion by Finding Good Cause

A

Snap’s and Meta’s Due Process Rights Were Not Violated

As an initial matter, we reject Snap’s and Meta’s assertions that their due process rights were violated by the trial court’s denial order. In its petition, Snap takes issue with the trial court’s December 8, 2023 order requiring it to comply with Pina’s subpoena and argues the court erred by proceeding *ex parte*. After receiving the initial subpoena, dated September

26, 2023, calling for a response or production of the requested information by October 20, 2023, Snap sent a letter to Pina’s counsel indicating it would not comply. Snap, however, did not file a motion to quash the subpoena, the only available method to avoid compliance, prior to the December 8, 2023 hearing. (See Code Civ. Proc., § 1987.1 [setting forth procedure to quash subpoena *duces tecum*]; *City of Los Angeles v. Superior Court* (2003) 111 Cal.App.4th 883, 888 [“In general, the procedural remedy against a defective subpoena *duces tecum* ... is a motion to quash, vacate, recall, or modify the subpoena.”].) Thereafter, Snap filed its motion to quash and was provided with opportunity to argue its position at the January 8, 2024 hearing.

Meta also contends that the trial court impinged on its due process rights by not affording it the opportunity to provide further briefing on a shortened briefing schedule as it requested. Unlike Snap, Meta did not respond at all to the initial subpoena served by Pina.⁵ In addition, after receiving the second subpoena accompanied by the court’s December 8, 2023 order, Meta failed to act promptly. Meta retained counsel, who contacted Pina’s defense counsel just five days before the January 8, 2024 hearing. It asserts that during that conversation, Pina’s counsel agreed Meta could file its motion to quash on January 8, 2024.

At the hearing, Meta’s attorney, Micheal C. Bleicher, stated that he requested a continuance from Pina’s counsel to see if they could work out an informal resolution. Bleicher stated that Pina’s counsel responded she could not agree to a continuance but they “agreed that Meta could file a response to the subpoena and order by January 8, today.” Bleicher stated his

⁵ Meta’s counsel asserted in her declaration in support of Meta’s motion to quash that “Meta does not have any record of receiving” the initial subpoena issued by Pina.

“understanding was that today’s hearing, as far as Meta [was] concerned, would be an opportunity to explain to the court that Meta was appearing in response to the subpoena and order, to state these objections, and to work out an abbreviated briefing schedule so that Meta could receive the defendant’s opposition to its motion before” its substance was addressed. The court denied this request, repeating its finding that good cause for the subpoena had been shown and denied both motions to quash.

We reject Snap’s assertion that the court’s December 8, 2023 relevance finding was improper because Snap did not appear at the hearing on that date. Rather, we agree with Pina that Snap’s decision to rest on its letter, rather than bring a motion to quash after receiving the initial subpoena, bars this argument. Likewise, Meta’s failure to act in a timely manner bars its argument that it was deprived of due process. Further, Snap filed its motion and received opposition, and, as Pina points out, Snap and Meta were both provided the opportunity to make a record at the hearing without constraint.

B

Good Cause Supports the Trial Court’s Denial of the Motions to Quash

Meta, Snap, and the District Attorney contend the trial court made an inadequate record concerning its good cause finding. We disagree. As Snap asserts, when a defendant seeks information via a subpoena duces tecum from a third party that is challenged by a motion to quash he “must make a showing of good cause—that is, specific facts justifying discovery.”

(*Madrigal, supra*, 93 Cal.App.5th at p. 256.) Further, the trial court must “create a record that facilitates meaningful appellate review. ... [A] trial court should, at a minimum, articulate orally, and have memorialized in the reporter’s transcript, its consideration of the relevant factors.” (*Touchstone*,

supra, 10 Cal.5th at p. 358.) Contrary to Meta’s and Snap’s assertions, this relatively low bar was satisfied by the trial court here.

We do agree with the petitioners that the probable cause standard cited at points by the trial court during the January 8, 2024 hearing was not the correct one. The court, struck by the petitioners’ concession that they would not object to providing the material to law enforcement in response to a valid search warrant, referred several times to the probable cause standard applied in that context.⁶ This was not the correct standard for the defense subpoenas at issue. However, the court itself noted at the outset of the hearing the correct standard and that it was required to assess the *Alhambra* factors. And, once Meta’s counsel pointed out that standard, the court articulated its determination under the *Alhambra* factors, stating explicitly it had considered the factors and found good cause existed for the subpoenaed material. Its explanation satisfied *Touchstone*’s requirement that the court “articulate orally, and have memorialized in the reporter’s transcript, its consideration of the relevant factors.” (*Touchstone*, 10 Cal.5th at p. 358; see also *In re Marriage of Askmo* (2000) 85 Cal.App.4th 1032, 1040 [“Code of Civil Procedure section 632 requires the trial court to issue a statement of decision ‘upon the trial of a question of fact’ when it receives a request therefor by a party appearing at trial. In general, however, section 632 applies when there has been a trial followed by a judgment. [Citation.] It does not apply to an

⁶ Under this test, “[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a ‘substantial basis for ... [concluding]’ that probable cause existed.” (*Illinois v. Gates* (1983) 462 U.S. 213, 238–239.)

order on a motion. ... This is true even if the motion involves an evidentiary hearing and the order is appealable.”].)

Turning to the *Alhambra* factors, we also agree with Pina that the court did not abuse its discretion and reasonably concluded good cause exists for the subpoenaed materials. “We first consider whether defense counsel demonstrated a ‘plausible justification’ for acquiring the documents. This is the ‘most significant’ consideration, and ‘should be given prominence.’” (*Madrigal, supra*, 93 Cal.App.5th at p. 258.) The trial court concluded that a plausible justification existed based on the information obtained from Samuel’s phone and his girlfriend’s testimony at the preliminary hearing. The court stated the information obtained from Samuel’s phone showed “the victim could potentially have some violent tendencies, which may or may not be relevant at trial which ... does satisfy that plausible justification.”

The evidence submitted by Pina in support of his opposition to the motion to quash showed a photograph of Samuel with the gun used in the shooting, suggesting that Samuel’s social media accounts might contain similar material that could support Pina’s defense, either if he acted in self-defense during an altercation with his brother or to show that Samuel had a violent character. Samuel’s girlfriend, in fact, stated that she took a picture of Samuel holding a gun that was posted on Snapchat. These facts supported the court’s finding that the requested material could be relevant to Pina’s defense and could contain admissible evidence about Samuel’s character. (*Touchstone, supra*, 10 Cal.5th at p. 348 [“ ‘ ‘A showing ... that the defendant cannot readily obtain the information through his own efforts will ordinarily entitle him to pretrial knowledge of any unprivileged evidence, or information that might lead to the discovery of evidence, if it appears reasonable that such knowledge will assist him in preparing his defense...’ ”], italics

omitted.) This conclusion was reasonable, and not an abuse of the court's discretion.

Indeed, as Meta points out in its petition, the prosecutor "conceded at the hearing that this material *could* be relevant, exculpatory evidence that the prosecution has an obligation to obtain via search warrant" and that "if the prosecution did so, the material could be discoverable." Further, all parties agreed at the hearing that had the prosecution obtained a search warrant for the same material, there would be probable cause to support the warrant. While the two standards are arguably not identical, they bear strong similarities, and certainly a finding of probable cause (which was conceded by the petitioners) suggests the existence of good cause in the context of a defense subpoena.

Snap argues that plausible justification for material from its platform does not exist, and the defense is on an impermissible "fishing expedition," because the exhibits submitted by the defense in opposition to its motion to quash contained only photographs from Meta's platforms. However, as stated, the preliminary hearing transcript shows that Samuel's girlfriend indicated there were photographs on Snapchat that showed him with a gun. This evidence was sufficient to show a plausible justification to obtain the requested material from Snap.

The next *Alhambra* factor requires the court to assess whether the request is "adequately described and not overly broad." (*Touchstone, supra*, 10 Cal.5th at p. 346.) Snap and Meta contend the material sought by the subpoenas is not sufficiently narrow because it seeks all content from Samuel's accounts over a two-year period. Pina responds that without access to Samuel's accounts it is not possible to draft a more narrow or specific request. Further, Pina points to the trial court's statement that defense

“focused in on specific data, which very well could exist, since we’ve already been through the phone and realized there’s some matter there that could be relevant.”

The requested material is somewhat broad. However, as Pina notes, there is no way to narrow the request because the contents of the accounts are not known.⁷ As Pina concedes, the proper procedure is for the material to be produced to the court for an in camera inspection so that its relevance can be further considered by the trial court before the material is produced to Pina. We agree with Pina that the trial court’s decision that this factor does not prevent disclosure was appropriate in these circumstances.⁸

We also reject Snap’s assertion that the sixth, fourth, and seventh *Alhambra* factors favored granting its motion to quash. Snap argues the request is untimely because Samuel’s girlfriend’s testimony at the preliminary hearing that she posted a photo of Samuel on her Snapchat account took place on December 7, 2022, more than ten months before the

⁷ At oral argument, Snap and Meta took issue with the two-year period set forth in the subpoenas. We cannot say, however, as a matter of law that this timeframe is overbroad.

⁸ The two cases cited by Snap, which involve far broader requests than the ones at issue here, do not persuade us otherwise. (See *People v. Serrata* (1976) 62 Cal.App.3d 9, 15 [holding trial court did not abuse its discretion by quashing a subpoena calling “for the production of ‘literally millions of pieces of paper’ which were located at IBM plants throughout the world and which constituted the work product of numerous teams of experts and scientists who had devoted as much as four or five years to the development of the sixteen complex computer devices which were the subject of the subpoenas”]; and *Lemelle v. Superior Court* (1978) 77 Cal.App.3d 148, 166–167 [order granting motion to quash subpoena seeking 10 years of all crime and arrest reports made by two police officers was overly broad and burdensome, especially in light of order granting other similar discovery to defendant].)

subpoenas were issued. However, the record shows that Pina's public defender was pursuing discovery in this case over the course of 2023, including working to obtain the contents of Samuel's cell phone from the Oceanside Police Department. It wasn't until the fall of 2023 that Pina's counsel received additional evidence from that phone suggesting Samuel's social media content might contain additional relevant information. This record does not show the court's finding that the request was timely is an abuse of discretion.

The fourth *Alhambra* factor, whether the requested material violates individual privacy rights or intrudes on a protected government interest, also does not support reversal of the court's order denying the petitioners' motions to quash. With respect to privacy, Snap points to the SCA. As we shall explain, however, we conclude the SCA does not apply to this case because the information sought is not the type of private information to which that law applies. Given this conclusion, we are left only with the privacy concerns of Samuel and the third parties that he interacted with. Samuel is deceased and we agree with Pina that any privacy interest that remains with respect to Samuel's interest is outweighed by Pina's interest to discover information that is potentially relevant to his defense. Further, as stated, because the statutes governing the production of this information allow for the material to be produced only to the trial court for a determination of its relevance, any privacy concern is significantly mitigated. Accordingly, we agree with Pina that this factor does not show the court's order was an abuse of discretion.

Finally, with respect to the final *Alhambra* factor (whether the request is unreasonably burdensome to the nonparty), the only burden Snap cites in its petition is its potential civil liability under the SCA. The SCA does impose civil liability for violations of the Act. (§ 2707.) However, as Snap

recognizes, the law contains a safe harbor for good faith reliance on a court order requiring disclosure. (§ 2707(e)(1).) There is no question that the safe harbor applies in this case.

Only Meta’s petition specifically addresses the third *Alhambra* factor, whether “the material [is] ‘reasonably available to the ... entity from which it is sought (and *not* readily available to the defendant from other sources).’” (*Touchstone, supra*, 10 Cal.5th at p. 346.) Meta argues the court failed to adequately assess this factor or consider whether Pina could obtain Samuel’s Instagram or Facebook content from another user Samuel interacted with, a “legacy contact” for Facebook,⁹ or another person with access to Samuel’s account. At the January 8, 2024 hearing, however, the court explicitly found that there was no other source for Pina to obtain this information, and no “legacy contact” for Samuel. In response, Meta made no argument to counter this finding and in its petition, despite being the repository for the material at issue, does not indicate whether a legacy contact exists.

Particularly in light of the length of time since Samuel’s death, we agree with Pina that the trial court’s determination that the material at issue is not available from other sources was a reasonable finding, and not an abuse of the court’s discretion. As with the other *Alhambra* factors, this factor also supports the court’s conclusion that Pina provided good cause for the information sought in his subpoenas to Snap and Meta that may contain information relevant to Pina’s defense to the murder of his brother.

⁹ Meta explains that “[a] legacy contact is someone you choose to look after your main profile if it’s memorialized after you’ve passed away. If you add a legacy contact, that person will be able to make decisions about your main profile once it is memorialized.’”

C

Procedure for Disclosure

As discussed, the procedure for Pina to obtain this information does not require Snap and Meta to produce the material directly to Pina. Rather, under “subdivision [(d)] of section 1326, the sought materials must be given to the superior court for its in camera review so that it may ‘determine whether or not the [requesting party] is entitled to receive the documents.’ (Pen. Code, § 1326, subd. [(d)]; see also *People v. Blair* (1979) 25 Cal.3d 640, 651 [such materials cannot legally be given directly to the requesting party].)” (*Touchstone, supra*, 10 Cal.5th at p. 344.) Accordingly, we direct the trial court to issue a modified order requiring the petitioners to provide the requested material to the trial court for its consideration of whether or not the material should be provided to Pina as relevant to his defense.

III

The SCA Does Not Apply to the Subpoenaed Material

A

Touchstone, supra, 10 Cal.5th 329, identified another critical issue now placed squarely before this court: Whether these social media companies’ “business model[s] place[them] outside key provisions of the SCA and render[them] subject to an enforceable state subpoena.” (*Id.* at p. 360.) In *Touchstone*, a defendant charged with attempted murder issued a subpoena to Facebook seeking all of the victim’s “Facebook communications (including restricted posts and private messages), and a related request that Facebook preserve all such communications.” (*Id.* at p. 342.) The defendant, Lance Touchstone, supported the subpoena “by offering a *sealed* declaration describing and quoting certain public Facebook posts made by [the victim] after the shooting that, defendant asserted, revealed [the victim’s] violent

general musings.” (*Id.* at p. 342.) “The trial judge ordered Facebook to comply with the subpoena or appear in court to address any objection to it and to preserve the account and related stored communications.” (*Ibid.*)

Facebook then moved to quash the subpoena. The trial court denied the motion, “finding good cause for the subpoena” based on Touchstone’s sealed declaration and a subsequent, second sealed declaration containing additional public Facebook posts. (*Touchstone, supra*, 10 Cal.5th at p. 355.) However, “[n]either the reporter’s transcript of the hearing, nor the resulting minute order, reflect[ed] that the court expressly considered and balanced the most relevant *Alhambra* factors.” (*Id.* at pp. 355–356.)

Like Meta and Snap in this case, Facebook filed a petition for writ of mandate seeking to overturn the trial court’s order. The Court of Appeal reversed the trial court’s decision, rejecting the defendant’s claims that to “the extent the SCA allows Facebook to block his subpoena, the Act must be found to violate his federal Fifth Amendment due process rights, along with his Sixth Amendment rights of confrontation, cross-examination, and counsel—and hence [that] the SCA is unconstitutional as applied to him.” (*Touchstone, supra*, 10 Cal.5th at p. 338.) In the Supreme Court, the defendant advanced the same constitutional arguments. (*Ibid.*)

The Supreme Court, however, identified significant problems with the underlying record. In particular, the documents that had been filed under seal in the trial court presented an incomplete picture of the factual basis for the material sought by the defendant from Facebook. (*Touchstone, supra*, 10 Cal.5th at pp. 339–341.) Further, because it sealed the subpoena, the trial court had proceeded on an *ex parte* basis, without the full participation of the prosecution or the subpoenaed third party. (*Ibid.*) The Supreme Court concluded this procedure called into question the veracity of the assertions

that had been made by the defendant in the underlying proceedings. (*Id.* at p. 341.) In addition, and critically, the Supreme Court held that the trial court had failed to conduct the proper analysis to determine good cause. It held “the trial court below abused its discretion when ruling on the motion to quash by failing to apply the seven-factor *Alhambra* test,” and remanded the matter “to afford the trial court an opportunity to consider the good cause issue anew, this time with full participation by all three parties.” (*Id.* at p. 359.)

The *Touchstone* court, thus, did not reach the constitutional issues asserted by the defendant concerning the SCA. (*Touchstone, supra*, 10 Cal.5th at p. 359.) The Supreme Court, however, did *address*, but not decide, the issue of “whether [Facebook] is covered and bound by the SCA.” (*Id.* at p. 360.) The defendant and prosecutor there, as here, jointly argued “that Facebook’s business model places it outside key provisions of the SCA and renders it subject to an enforceable state subpoena.” (*Ibid.*) They asserted that Facebook’s Terms of Service and Data Policy constitute a “business model of mining its users’ communications content, analyzing that content, and sharing the resulting information with third parties to facilitate targeted advertising,” which “precludes it from qualifying as an entity subject to the SCA.” (*Ibid.*)

Facebook responded by suggesting the court’s opinion in *Facebook, Inc. v. Superior Court* (2018) 4 Cal.5th 1245 (*Hunter*), and decisions in other prior litigation, had resolved the question and determined that Facebook operates as a provider of either ECS or RCS under the SCA. (*Touchstone, supra*, 10 Cal.5th at p. 360.) The Supreme Court, however, rejected this assertion, stating that in *Hunter*, it “undertook no substantive analysis concerning whether the entities in that case (including Facebook) provide ECS or RCS

with regard to the communications there at issue. Because (1) prior decisions had found or assumed that Facebook and analogous social media entities provide *either* ECS or RCS with regard to the type of sought posts and/or messages at issue in those prior cases and in *Facebook (Hunter)*, and (2) neither party in *Facebook (Hunter)* contested the issue, [the court] stated that [it] saw ‘no reason to question [that] threshold determination.’ (*Hunter, supra*,] 4 Cal.5th at p. 1268.) Accordingly, [the court] assumed, but did not decide, that Facebook provided either ECS or RCS with regard to the communications sought—and hence was covered by the Act’s general ban on disclosure of content by any entity providing those services.” (*Touchstone*, at pp. 360–361.) The Supreme Court stated explicitly, it “did not consider whether, under the business model theory..., Facebook provides either ECS or RCS, or neither, under the Act” and that “potentially dispositive issue remain[ed] unresolved.” (*Id.* at p. 361.)

Of great importance here, in a concurring opinion, then Chief Justice Cantil-Sakauye wrote separately to specifically “explore [the business model] theory in greater depth because, in [her] view, it deserve[d] additional and focused attention, perhaps on remand in [the present] case or at least in other similar future litigation.” (*Touchstone, supra*, 10 Cal.5th at p. 361 (conc. opn. of Cantil-Sakauye, C. J.)) The concurrence outlines the contours of the business model argument advanced by the defense and district attorney, Facebook’s response, and the applicable statutory language of the SCA. (*Id.* at pp. 363–366.)

Meta’s Terms of Service for Facebook, of which we take judicial notice in this case, provide: “Instead of paying to use Facebook and the other products and services we offer, by using the Meta Products covered by these Terms, you agree that we can show you personalized ads and other

commercial and sponsored content that businesses and organizations pay us to promote on and off Meta Company Products. We use your personal data, such as information about your activity and interests, to show you personalized ads and sponsored content that may be more relevant to you.” (Facebook, Terms of Service <www.facebook.com/legal/terms> (revised July 26, 2022) [as of July 23, 2024], archived at <<https://perma.cc/5A49-85MR>>, pt. 2, *How our services are funded*.) Moreover, the terms provide: “We need certain permissions from you to provide our services: [¶] ... [¶] [T]o provide our services we need you to give us some legal permissions (known as a ‘license’) to use this content. ... [¶] Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means, for example, that if you share a photo on Facebook, you give us permission to store, copy, and share it with others (again, consistent with your settings) such as Meta Products or service providers that support those products and services.” (*Id.*, at pt. 3, *Your commitments to Facebook and our community*, pt. 3.3, *The permissions you give us*, pt. 3.3.1, *Permission to use content you create and share*.)

Meta’s Data Policy for Facebook, which we also take judicial notice of, states: “We collect the content, communications and other information you provide when you use our Products, including when you ... message or communicate with others. This can include information in or about the content you provide ... Our systems automatically process content and communications you and others provide to analyze context [¶] ... [¶] We

also receive and analyze content, communications and information that other people provide when they use our Products.’ ([Facebook, Data Policy <www.facebook.com/full_data_use_policy> (revised Apr. 19, 2018) (as of Aug. 10, 2020)], at pt. I, *What kinds of information do we collect?/ Things you and others do and provide/ Information and content you provide/ Things others do and information they provide about you.*)” (*Touchstone*, *supra*, 10 Cal.5th at pp. 362–363, fn. 3. (conc. opn. of Cantil-Sakauye, C. J.).)

“Facebook’s Data Policy further explains it employs users’ mined and analyzed content to facilitate various services, including to ‘[p]rovide, personalize, and improve our Products. [¶] ... and make suggestions for you’ by showing users ‘personalize[d] ads, offers, and other sponsored content.’ ([Facebook, Data Policy <www.facebook.com/full_data_use_policy> (revised Apr. 19, 2018) (as of Aug. 10, 2020)], at pt. II, *How do we use this information?/ Provide, personalize and improve our Products/ Ads and other sponsored content.*) In that regard, Facebook relates, it shares information about its users’ content with ‘third-party partners ... which [in turn] makes it possible to operate our companies and provide free services to people around the world.’ (*Id.*, at pt. III, *How is this information shared?/ Sharing with Third-Party Partners.*) Facebook states that it ‘do[es]n’t sell any of your information to anyone,’ but instead ‘[s]har[es] with,’ ‘work[s] with,’ and ‘provide[s]’ that information to ‘third-party partners.’ (*Ibid.*, italics added.) Specifically, for some partners, it supplies ‘aggregated statistics and insights that help people and businesses understand how people are engaging with their posts ... and other content.’ (*Id.*, at pt. III, *Partners who use our analytics services.*) And for advertisers, Facebook explains: ‘We provide ... reports about the kinds of people seeing their ads and how their ads are performing’ (*Id.*, at pt. III, *Sharing with Third-Party*

Partners/Advertisers.) At the same time, Facebook stresse[d]: ‘[W]e don’t share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser.’” (*Touchstone, supra*, 10 Cal.5th at p. 363, fn. 3. (conc. opn. of Cantil-Sakauye, C. J.)) The concurrence also noted that “Facebook does not contest that it mines, analyzes, and shares with third party advertisers information about content found in, among other things, its users’ communications—including restricted posts and private messages.”¹⁰ (*Id.* at pp. 362–363.)

The concurrence then provides an explanation of the relevant provisions of the SCA, explaining that under the Act, “ECS is defined as ‘any service which provides to users thereof the ability to send or receive wire or electronic communications.’ (§ 2510(15) [incorporated into the SCA by § 2711(1)].) Section 2702(a)(1), directs that an ‘*entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while [the communication is] in electronic storage by that service.*’ (Italics added.) ‘Electronic storage’ is defined in section 2510(17), as ‘(A) *any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and [¶] (B) any storage of such communication by an electronic communication service for purposes of backup protection of such*

¹⁰ Likewise, Meta does not contest this fact in the present case.

communication.' (Italics added.)" (*Touchstone, supra*, 10 Cal.5th at p. 364 (conc. opn. of Cantil-Sakauye, C. J.).)

"RCS, by contrast, is defined as 'the provision to the public of computer storage or processing services by means of an electronic communications system.' (§ 2711(2).) Section 2702(a)(2)'s introductory language directs that an '*entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service*' when certain conditions are met. (Italics added.)" (*Touchstone, supra*, 10 Cal.5th at p. 364 (conc. opn. of Cantil-Sakauye, C. J.).) "The next parts of section 2702(a)(2) describe the conditions that will trigger the duty of an entity providing RCS to 'not knowingly divulge' the contents of any communication carried or maintained by that entity. ... [T]he first condition set out in subsection (a)(2)(A) [states]: the 'carried or maintained' communication must be 'on behalf of, and received by means of electronic transmission from ... a subscriber or customer of such service.'" (*Ibid.*)

The opinion then explains, "[i]t is the second condition set out in section 2702(a)(2)(B) that lies at the center of the business model argument advanced by defendant and the district attorney. Under section 2702(a)(2)(B), the prohibition on disclosure by an entity that provides RCS applies only if the communication is carried or maintained on the service "*solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.*" (Italics added.)" (*Touchstone, supra*, 10 Cal.5th at p. 365 (conc. opn. of Cantil-Sakauye, C. J.).)

The concurring opinion notes, “[t]his crucial passage is hardly a model of clarity. It appears to express two related conditions in order to qualify as a communication held by an entity that provides RCS: (1) the user’s data must be transmitted to the provider ‘solely for the purpose of providing storage or computer processing services’; *and* (2) the entity must ‘not [be] authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.’ (§ 2702(a)(2)(B); see, e.g., Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act* (2010) 98 Geo. L.J. 1195, 1213–1214 ... [so construing the statute].) Based on this language, the author of the cited law journal and other commentators have argued that if the entity *is* ‘authorized to access the contents of any such communication for purposes of providing any services *other than* storage or computer processing’ (§ 2702(a)(2)(B), italics added)—that is, for the purposes of providing any services *in addition* to storage or computer processing—the Act’s bar on disclosure is inapplicable. In other words, these commentators reason, such an entity would not be acting as an RCS that is, in turn, generally barred from disclosing communications content—and hence the entity would be subject to a viable subpoena duces tecum.” (*Touchstone, supra*, 10 Cal.5th at pp. 365–366 (conc. opn. of Cantil-Sakauye, C. J.), fn. omitted.)

The concurring opinion then implores the United States Congress to update the then 34-year old, outdated law, which was adopted prior to the advent of the internet and long before the social media platforms at issue here came into existence. (*Touchstone, supra*, 10 Cal.5th at p. 366 (conc. opn. of Cantil-Sakauye, C. J.)) The opinion quotes from cases and scholarly literature over the past two decades expressing frustration with the SCA’s failure to account for changes in technology and opines that “[b]ecause

Congress has not acted to alter the relevant provisions of the SCA despite the pleas of courts and commentators that it do so, litigants and judges have no option but to apply the Act's outdated definitions to the evolved and still developing technology and entities of today.” (*Id.* at p. 368.)

After outlining the arguments of the parties, which are similar to those made here, and repeating the majority opinion's conclusion that whether Facebook falls within the ambit of the SCA's protections remains an open question, Chief Justice Cantil-Sakauye provided her tentative assessment of policy arguments made by Facebook in support of its position that the SCA barred it from producing any information in response to a criminal defense subpoena. (*Touchstone, supra*, 10 Cal.5th at p. 371.) In particular, Facebook asserted it should be afforded status as an ECS or RCS because “concluding otherwise would (1) unduly disrupt and impair technological innovation, (2) disappoint users' settled privacy expectations, and (3) frustrate its ability to protect against malware.” (*Id.*, at p. 371 (conc. opn. of Cantil-Sakauye, C. J.))

While noting “[t]he first two contentions certainly should give a court pause before holding that Facebook and similar entities fall outside section 2702(a),” the concurrence predicts “for practical marketplace reasons, it may be doubted that such a holding would likely lead to such disruptions or voluntary disclosures by most Internet entities, absent legal compulsion.” (*Touchstone, supra*, 10 Cal.5th at pp. 371–372 (conc. opn. of Cantil-Sakauye, C. J.)) Additionally, the concurrence noted it was not “likely that law enforcement actors would attempt to compel entities to disclose users' communications with, as Facebook asserts in its briefing, ‘a mere subpoena’ ” since “other laws and authority already protect against that.” (*Ibid.*) “Finally,” she stated, “as a matter of policy, a holding finding Facebook to lie

outside the SCA might have the beneficial effect of spurring long-needed congressional adjustment of the outdated Act, as repeatedly advocated by courts and commentators.”¹¹ (*Ibid.*)

B

Because we agree with Pina that the trial court conducted a sufficient good cause analysis, and that good cause supports the subpoenaed material, we are faced with the question *Touchstone*’s concurring opinions asked our state’s lower courts to address. We must decide whether the SCA applies in this circumstance to preclude discovery of the social media material subpoenaed by Pina. In their petitions, Snap and Meta maintain that the SCA allows production of material in a criminal case only when it is requested by a government entity as defined by the Act and that the public defender does not meet this definition.

In response, Pina and the District Attorney both contend that neither Snap nor Meta qualify under the SCA’s definition of ECS or RCS, and thus they cannot prevent disclosure of the subpoenaed material on that basis. In its reply brief, Snap argues that under the statute’s plain language, the SCA is applicable here and also that the real parties’ interpretation of the statute

¹¹ Writing in a separate concurrence, former Justice Cuéllar noted the importance of the issue now before us, i.e. “the crucial matter of how broadly to read the SCA—and, in particular, whether it protects Facebook and similar entities from the duty to honor valid subpoenas issued by our state courts,” and implored lower courts “to take up [this] very question.” (*Touchstone*, *supra*, 10 Cal.5th at p. 373 (conc. opn. of Cuéllar, J.)) In his concurrence, Justice Cuéllar noted that courts “should endeavor to discern whether Congress’s purpose in enacting the SCA encompassed protecting communications held by social media companies such as Facebook” and that “[t]he companies storing ever-expanding troves of data about our lives,” as well as the people of California, “would surely benefit from greater clarity about the full extent of [those companies]’ responsibility to honor a valid subpoena.” (*Id.* at p. 374.)

would lead to absurd results by stripping the users of its platform of the privacy protections the SCA was designed to create. Further, it asserts that the real parties' interpretation would "negatively impact [the] providers[]" ability to protect their users and platforms by identifying wrongdoing, removing illicit content, and when appropriate, reporting responsible individuals to law enforcement..." In its reply, Meta argues the issue was not sufficiently raised in the trial court and thus should not be considered in its writ petition and, alternatively, the SCA applies to preclude disclosure of the material subpoenaed by Pina.

1. *The SCA*

"Congress enacted the Electronic Communications Privacy Act in 1986. (ECPA; Pub.L. No. 99-508 (Oct. 21, 1986), 100 Stat. 1848, 1860.) Title I of that law, amending the prior 'Wiretap Act,' addresses the interception of wire, oral, and electronic communications. (§§ 2510–2521.) Title II of the law, set out in chapter 121, is often referred to as the [SCA]. It addresses unauthorized access to, and voluntary and compelled disclosure of, such communications and related information. (§§ 2701–2712.)" (*Hunter, supra*, 4 Cal.5th at p. 1262.)

"Prior to the ECPA's enactment, the respective judiciary committees of the House of Representatives and the Senate prepared detailed reports concerning the legislation. Each explained that the main goal of the ECPA in general, and of the SCA in particular, was to update then existing law in light of dramatic technological changes so as to create a 'fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.' (H.R.Rep. No. 99-647, 2d Sess., p. 19 (1986) (hereafter House Report); see also Sen. Rep. No. 99-541, 2d Sess., p. 3 (hereafter Senate Report) [speaking of protecting both 'privacy interests in personal proprietary

information’ and ‘the Government’s legitimate law enforcement needs’].) Each report also highlighted a related objective: to avoid discouraging the use and development of new technologies. These three themes—(1) protecting the privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies (with privacy protection being the primary focus)—were also repeatedly emphasized by the bill authors in their debate remarks. As this history reveals, and as a leading commentator on the SCA has explained, Congress was concerned that ‘the significant privacy protections that apply to homes in the physical world may not apply to “virtual homes” in cyberspace,’ and hence ‘tried to fill this possible gap with the SCA.’” (*Hunter, supra*, 4 Cal.5th at pp. 1262–1263, fns. omitted.)

“‘The [SCA] reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, [citation], the [SCA] protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.’” (*Juror Number One v. Superior Court* (2012) 206 Cal.App.4th 854, 860 (*Juror Number One*.)

“‘The SCA addresses two classes of service providers, those providing electronic communication service (ECS) and those providing remote computing service (RCS).” (*Juror Number One, supra*, 206 Cal.App.4th at p. 860.) “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); see 18 U.S.C. § 2711(1).) An RCS provides ‘computer storage or processing

services by means of an electronic communications system.’ (18 U.S.C. § 2711(2).)” (*Id.* at pp. 860–861.)

Subject to certain conditions and exceptions, the SCA prohibits “ECS’s from knowingly divulging to any person or entity the contents of a communication while in ‘electronic storage’ (§ 2702(a)(1)) and prohibits RCS’s from knowingly divulging the contents of any communication ‘which is carried or maintained on that service’ (*id.*, § 2702(a)(2)).” (*Juror Number One, supra*, 206 Cal.App.4th at p. 861.) In addition, “[i]f an entity does not act as a provider of ECS or RCS with regard to a given communication, the entity is not bound by any limitation that the SCA places on the disclosure of that communication—and hence the entity cannot rely upon the SCA as a shield against enforcement of a viable subpoena seeking that communication.” (*Touchstone, supra*, 10 Cal.5th at p. 363 (conc. opn. of Cantil-Sakauye, C. J.))

As stated, the SCA prohibits an ECS “from divulging ‘the contents of a communication while in electronic storage by that service.’^[12] (18 U.S.C. § 2702(a)(1).) However[, as discussed in the *Touchstone* concurrence,] the term ‘electronic storage’ has a limited definition under the SCA. It covers ‘(A) any *temporary, intermediate storage* of a wire or electronic communication *incidental to the electronic transmission* thereof; and (B) any storage of such communication by an electronic communication service *for purposes of backup* protection of such communication.’ (18 U.S.C. § 2510(17), [italics

¹² Section 2702(a)(1) states that, subject to specified exceptions set forth in subdivisions (b) and (c), “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” (§ 2702(a)(1).)

added].)^{13]} Thus, only copies of electronic communications held by the ECS pending initial delivery to the addressee or held thereafter for backup purposes are protected.” (*Juror Number One, supra*, 206 Cal.App.4th at p. 861.)

Similarly, “[a]n RCS is prohibited from divulging the content of any electronic transmission that is carried or maintained on its service ‘solely for the purpose of providing storage or computer processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.’ (18 U.S.C. § 2702(a)(2)(B).)”¹⁴ (*Juror Number One, supra*, 206 Cal.App.4th at pp. 861–862.) “Thus, if the service *is* authorized to access the customer’s information for other purposes, such as to provide targeted advertising, [as Chief Justice Cantil-Sakauye

¹³ Under section 2711(1), the terms defined in the Wiretap Act (§§ 2510–2521) of the ECPA at section 2510 are given the same definitions for purposes of the SCA.

¹⁴ Section 2702(a)(2) states, subject to specified exceptions set forth in subdivisions (b) and (c), that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service— [¶] (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; [¶] (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing ...”

suggests in *Touchstone*,] SCA protection may be lost.”¹⁵ (*Juror Number One, supra*, 206 Cal.App.4th at p. 862.)

The next two subsections of section 2702—(b) and (c)—list the exceptions to the general prohibitions on disclosure by ECS and RCS providers that are contained in subsection (a). “Subsection (b) describes eight circumstances under which a provider ‘may divulge the contents of a communication.’ (§ 2702(b).) As relevant here, subparts (1) through (3) of subsection (b) permit disclosure: (1) ‘to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient’ (§ 2702(b)(1)); (2) pursuant to section 2703, which, as described below, permits a ‘governmental entity’ to compel a covered provider to disclose stored communications by search warrant, subpoena or court order; [or] (3) ‘with the *lawful consent of the originator or an addressee or intended recipient* of such communication, or the subscriber in the case of [a] remote computing service.’” (*Hunter, supra*, 4 Cal.5th at p. 1265.) Subsection (c) of section 2702 “describes [seven] circumstances under which a covered provider may divulge non-content information—that is, any ‘record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications ...).’” (*Ibid.*)

In *Hunter, supra*, 4 Cal.5th 1245, the Supreme Court examined the legislative history of the disclosure exceptions in section 2702. The court found that the 1986 house report on the legislation “indicated its understanding that with regard to electronic communications configured by the user to be accessible to the public, a covered service provider would be

¹⁵ Section 2702(a)(3), again subject to the same exceptions of subdivisions (b) and (c), “bars any service provider from knowingly divulging any non-content ‘record or other information pertaining to a subscriber to or customer’ to any governmental entity.” (*Hunter, supra*, 4 Cal.5th at p. 1265.)

free to divulge those communications under section 2702(b)(3)'s lawful consent exception.” (*Id.* at p. 1268.) In reaching this conclusion, the court looked to the house report’s analysis indicating that consent could be implied both by a “user’s act of posting publicly, and/or by a user’s acceptance of a provider’s terms of service: ‘Consent may ... flow from a *user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use—e.g., continued use of such an electronic communication system.*’ ([H.R.Rep. No. 99-647, 2d Sess., p. 19 (1986) (hereafter House Rep.)], italics added.)” (*Hunter, supra*, 4 Cal.5th at pp. 1267–1268.)

“The report explained that ‘[a]nother type of *implied consent* might be inferred from the very nature of the electronic transaction. For example, a subscriber who places a communication on a computer “electronic bulletin board,” with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication.’ (... , italics [omitted].) Moreover, the report continued, ‘If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.’ ” (*Hunter, supra*, 4 Cal.5th at p. 1268.)

2. *Application of the SCA to the Material Subpoenaed by Pina*

As an initial matter, it is not clear from the record developed on the writ petitions whether Samuel’s Facebook, Instagram, and Snapchat accounts were configured as public or private. To the extent they were configured by him as public, that information is unquestionably subject to the

user consent exception under section 2702(b)(3) of the SCA, as set forth in *Hunter, supra*, 4 Cal.5th at p. 1274, and should be produced to the trial court and identified by Meta and Snap as public. (*Ibid.* [“communications configured by a social media user to be public fall within section 2702(b)(3)’s lawful consent exception, presumptively permitting disclosure by a provider”].)

Separate from the settled issue of public versus private communications, Pina argues that Snap and Meta do not qualify as ECS or RCS providers because they “do not provide temporary or intermediate storage of communications incidental to its transmission, nor do[they] store that communication merely for backup purposes.” Pina asserts that, “as evidenced by their own terms of service and privacy policy, Snap Inc. and Meta Platforms Inc. retain and utilize user communication content for their own business purposes and to enhance services offered on the platforms.” Therefore, Pina contends, the SCA does not apply to the material sought by his subpoenas. The District Attorney also argues that the SCA does not apply, asserting that Snap and Meta failed to present any evidence to support their assertion that the law precludes them from producing the subpoenaed material.

Pina accepts the invitation of the *Touchstone* concurring opinions to argue that the business model of these companies brings them outside the limitations of disclosure created by the SCA. We are persuaded by this argument. The statutes at issue, which notably were “ ‘enacted before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994,’ ” by their terms do not apply when the provider of ECS or RCS is accessing the user’s content for purposes other than facilitating

communications or storing the content as backup for the user. (*Juror Number One, supra*, 206 Cal.App.4th at p. 861.)

First, with respect to ECS, as *Juror Number One* explained, “only copies of electronic communications held by the ECS [provider] pending initial delivery to the addressee or held thereafter for backup purposes are protected.” (*Juror Number One, supra*, 206 Cal.App.4th at p. 861.)

Specifically, section 2702(a)(1) of the SCA prohibits a provider of ECS from divulging the contents of an electronic communication while the provider holds that content in “electronic storage” for its users. (§ 2702(a)(1).)

However, as discussed, the SCA explicitly limits the definition of “electronic storage” for purposes of the protection afforded by section 2702(a)(1) to “*temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof*” or “any storage of such communication by an electronic communication service *for purposes of backup protection of such communication.*” (§ 2510(17), italics added.)

Here, neither Snap nor Meta refute Pina’s assertion that—while their platforms do store the content of their user’s communications incidentally to transmission and for purposes of backup for its users—they also maintain that content for their own business purposes.¹⁶ Snap and Meta contend that because the content is stored for both reasons, the SCA precludes disclosure

¹⁶ Facebook’s terms of service and privacy policy set forth in the concurring opinion in *Touchstone* are the same ones at issue in this case. As Snapchat explains in its reply brief in this court, citing to its terms of service and privacy policy, “Snapchat users grant Snap permission to access their communications” for reasons in addition to providing storage and computer processing services, including agreeing that “Snap may access and review their content ‘at any time and for any reason,’ ” and to “permit Snap to store, use, and analyze content to improve the services provided and to research and develop new ones.”

in this circumstance. However, the underlying policy purpose of the SCA, to give privacy protections to the users of ECS providers who intend for their communication to be private, is belied where, as here, the users have given the providers authorization to access and use their content for their own business purposes. (See *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002) 302 F.3d 868, 875 [concluding, based on the SCA’s legislative history, that “Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards”].) This dual purpose brings the content outside the SCA’s plain definition of ECS provider because the content is held and used by Snap and Meta for their own profit-driven purposes.¹⁷

¹⁷ Meta cites to a series of cases it contends have “held or assumed” that “the SCA covers Facebook or similar services.” As explained in the concurrence in *Touchstone*, however, none of these cases addressed the specific argument advanced here, that the social media companies’ business models—which require their users to authorize the companies to access their communications—bring the services outside the definitions of ECS and RCS providers set forth in the SCA. (See *Hunter, supra*, 4 Cal.5th at p. 1268 [seeing “no reason to question” that the SCA covers Facebook content]; *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 889, 901–904 [applying the SCA to private email (Gmail account administered by Google, Inc.) and rejecting Google’s contention that the SCA barred civil discovery from an ECS provider where consent was provided by users]; *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F.Supp.2d 965, 989–991 [finding social media services like Facebook and MySpace are covered by the SCA, but not considering the argument that access by the providers could eliminate that status]; *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 667 [finding the SCA applies to Facebook posts in context of civil lawsuit asserting violation of the SCA by the plaintiff’s employer; not considering Facebook’s access to users content]; *Viacom Int’l Inc. v. YouTube Inc.* (S.D.N.Y. 2008) 253 F.R.D. 256, 264 [finding the SCA applies to videos on YouTube that are configured to be private]; *State v. Johnson* (Tenn. Crim. App. 2017) 538 S.W.3d 32, 69 [stating in dicta, after finding it lacked

Similarly, and slightly more clearly, section 2702(a)(2) precludes “a person or entity” that provides RCS from disclosing the content of its users’ communications in situations where the content is maintained by the provider on behalf of its users “*solely* for the purpose of providing storage or computer processing services” to the user and “if the provider is not authorized to access the contents ... for purposes of providing any services other than storage or computer processing ...” (§ 2702(a)(2)(A)–(B).) Here, Snap and Meta concede that they do not provide RCS solely for purposes of providing storage or processing services, and they concede that their terms of service authorize them to access the contents for their own business purposes. Thus, under the plain language of section 2702(a)(2), because Snap and Meta are not maintaining communications “solely for the purpose of providing storage or computer processing services” to their users, the SCA does not preclude them from disclosing the material sought by Pina’s subpoenas. (§ 2702(a)(2)(B).)

In its reply brief, Snap presents a different interpretation of this statutory language. Snap argues that under section 2702(a)(2)(B) “the only time that SCA protection for a communication depends on whether it is held ‘solely for the purpose of providing storage or computer processing services,’ is *if* the user has *not* given the provider authorization to access those communications for any other reason.” Thus, it asserts, if the communication is held solely for the purpose of providing storage or processing, it is protected only if the user has given the provider authorization to access it for another reason—here, Snap’s users have agreed to allow Snap to access their communications “‘at any time for any reason’”, including “to identify

jurisdiction in the case before it, that the SCA is applicable to communications shared on social media websites].)

content [that] violates [its] terms or any applicable law’ ” and “to store, use, and analyze content to improve the services provided and to research and develop new ones.”

While the statutory language at issue is certainly not “a model of clarity,” Snap’s interpretation makes little sense. (*Touchstone, supra*, 10 Cal.5th at p. 365 (conc. opn. of Cantil-Sakauye, C. J.)) If Snap’s users allow it to use their content for other purposes, they do not have the expectation of privacy contemplated by the SCA. The interpretation that we adopt and that Pina advances is logical and supported by its legislative history showing a policy to protect *private* communications. Accordingly, the statute limits its privacy protections to situations where the provider is facilitating private communication or storing private information for its users, not when it is accessing and using content for its own purposes. “In other words,” the entity is not acting as an RCS that is “barred from disclosing communications content—and hence the entity [is] subject to a viable subpoena duces tecum.” (*Ibid.*)

Snap also argues that the real parties’ interpretation of the SCA yields absurd results because it “exclude[s] broad swaths of communications from the privacy protections Congress intended to confer” and “significantly undermine[s], if not destroy[s], providers’ ability to protect their users and platforms by identifying and taking action against users who are engaged in harmful and/or illegal conduct.” Snap also asserts that Pina’s interpretation would “strip the privacy protections that Congress designed the statute to create from an astronomical number of stored communications held by numerous providers and upon which both providers and users of those services have come to rely.” Snap, however, does not explain what exactly the disastrous consequences would be, or how the platform would no longer

be able to protect its users or itself from harmful conduct. It is Snap and Meta's decision to access its users' communications that brings it outside the disclosure limitations of SCA, and neither provides a concrete explanation as to why their failure to comply with the statute's requirements should be overlooked.

Similarly, Snap also argues that failing to apply the SCA to these communications is contrary to public policy because it would "negatively impact providers' ability to protect their users and platforms by identifying wrongdoing, removing illicit content, and, when appropriate, reporting responsible individuals to law enforcement, unless providers and users alike are willing to forego SCA protection for their users' communications." However, Snap does not explain why any legal obligations that exist with respect to reporting wrongdoing or removing illicit content would be altered by a conclusion that they are not acting as an ECS or RCS provider under the SCA.

Instead, Snap argues that if it is not an ECS or RCS provider, then it "would no longer be obligated under the SCA to preserve accountholder data pursuant to the requests of law enforcement and could no longer be bound by nondisclosure orders that prohibit them from disclosing the existence of legal process seeking user account data." Even if the SCA does not apply to Snap and Meta, however, they are still required to comply with search warrants, law enforcement subpoenas, and court orders requiring the preservation of documents or other data or directing nondisclosure of a warrant or subpoena. Further, if they are not prohibited from disclosure by the SCA, Snap, Meta,

and other social media companies like them, can voluntarily disclose wrongdoing to authorities.¹⁸

Meta also asserts an additional argument. Turning the concept of forfeiture on its head, Meta argues that whether the SCA applies to it is not properly before this court because neither it nor Pina raised the issue in the trial court. Meta's assertion that Pina was obligated to address the application of the SCA is not well taken; he was under no requirement to address a federal statute he maintains is not applicable to the corporate entities he subpoenaed. Further, Meta's failure to timely respond to the initial subpoena and subsequent court order by filing a motion to quash prior to the January 8, 2024 hearing, if anything, constitutes a forfeiture of Meta's argument that the SCA bars it from complying with the court's order. (See *Hewlett-Packard Co. v. Oracle Corp.* (2021) 65 Cal.App.5th 506, 548 [“ “New theories of defense, just like new theories of liability, may not be asserted for the first time on appeal.” ’ ’].) Finally, as Meta points out in its own reply brief, it *did* address the application of the SCA to Pina's subpoena in the motion to quash it filed on January 8, 2024.

In sum, we agree with Pina that the SCA does not apply in this particular circumstance to bar Snap and Meta's compliance with Pina's subpoenas based on these third parties' ability to access and use their users' content. We emphasize, however, that our conclusion that the SCA does not protect the communications at issue here does not mean the third party is authorized generally to publicize the information provided to them by their

¹⁸ Snap also argues that the trial court's order requiring it to comply with Pina's subpoena violates the supremacy clause. However, because we conclude that the federal statute is not applicable to Snap and Meta in the circumstances presented here, there is no conflict of law to which the supremacy clause applies. Accordingly, we do not reach Snap's argument.

users. Rather, their own contractual agreements with users govern the terms of their use of that information. As the *Touchstone* concurring opinion notes—in response to Facebook’s argument “that if disclosure is not prohibited by the SCA, a ‘provider could choose to disclose a communication to anyone’[—]“an entity that became known for disclosing its users’ communications on its own, without legal compulsion, would not long survive in the market—and hence would refrain from doing so in the first place.” (*Touchstone, supra*, 10 Cal.5th at p. 372, fn. 12 (conc. opn. of Cantil-Sakauye, C. J.))

Further, as that concurrence also points out, it is also not “likely that law enforcement actors would attempt to compel entities to disclose users’ communications with ... ‘a mere subpoena’; other laws and authority already protect against that.” (*Touchstone, supra*, 10 Cal.5th at p. 372.) Specifically, “California’s Electronic Communications Privacy Act (Pen. Code, § 1546 et seq.) generally requires a warrant or comparable instrument to acquire such ... communication [and] *precludes use of a subpoena* ‘for the purpose of investigating or prosecuting a criminal offense.’” (*Touchstone*, at p. 372, fn. 13, citing Pen. Code, § 1546.1, subd. (b)(1)–(5).) And, “federal case law requires a search warrant, instead of a mere subpoena or court order, before a governmental entity may obtain private electronic communications.” (*Touchstone*, at p. 372, fn. 13.)

We recognize the import of this decision and do not take lightly the policy arguments presented by Snap and Meta. However, we conclude that the plain language of the SCA provisions at issue and the legislative history

behind them establish that the disclosure limitations contained in the Act do not apply to the material at issue here.¹⁹

DISPOSTITION

The petitions of Snap, Inc. and Meta, Inc. for writ relief are denied in part and granted in part. Let a peremptory writ issue directing respondent court to set aside its order of January 8, 2024, and issue a modified order directing petitioners to produce the subpoenaed information in camera to the respondent court for it to determine whether the material should be produced to Pina’s defense counsel. The stay issued by this court on January 24, 2024 is vacated on August 2, 2024 and this decision is final forthwith.

McCONNELL, P. J.

WE CONCUR:

HUFFMAN, J.

CASTILLO, J.

¹⁹ Because we decide this case based on the SCA, we decline to reach the constitutional issues raised by Pina in response to the petitions. (See *Hunter*, *supra*, 4 Cal.5th at p. 1275, fn. 31 [“we are guided by the familiar principle that we should address and resolve statutory issues prior to, and if possible, instead of, constitutional questions [citation], and that ‘we do not reach constitutional questions unless absolutely required to do so to dispose of the matter before us’ ”].)

Attachment B

FILED
Clerk of the Superior Court

AUG 02 2024

By: L. Lubsen

**SUPERIOR COURT OF CALIFORNIA
County of San Diego**

DATE: August 2, 2024

DEPT. 21

**HONORABLE DANIEL F. LINK,
JUDGE**

**CLERK:
L. Lubsen**

SCN429787

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff,

vs.

OCT110

PINA, ADRIAN, Defendant

EXPARTE

Court orders NONPARTY SNAP and META to produce the subpoenaed records in camera to Judge Daniel F. Link, Department 21 to determine whether the material should be produced to defense. Please supply the documents by the end of business day August 5th, 2024, directly to Department 21.



DANIEL F. LINK

-ll-

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SAN DIEGO <input type="checkbox"/> CENTRAL DIVISION, CENTRAL COURTHOUSE, 1100 UNION ST., SAN DIEGO, CA 92101 <input type="checkbox"/> CENTRAL DIVISION, HALL OF JUSTICE, 330 W. BROADWAY, SAN DIEGO, CA 92101 <input type="checkbox"/> CENTRAL DIVISION, KEARNY MESA, 8950 CLAIREMONT MESA BLVD., SAN DIEGO, CA 92123 <input type="checkbox"/> CENTRAL DIVISION, JUVENILE COURT, 2851 MEADOW LARK DR., SAN DIEGO, CA 92123 <input type="checkbox"/> EAST COUNTY DIVISION, 250 E. MAIN ST., EL CAJON, CA 92020 <input checked="" type="checkbox"/> NORTH COUNTY DIVISION, 325 S. MELROSE DR., VISTA, CA 92081 <input type="checkbox"/> NORTH COUNTY DIVISION, JUVENILE COURT, 325 S. MELROSE DR., VISTA, CA 92081 <input type="checkbox"/> SOUTH COUNTY DIVISION, 500 3RD AVE., CHULA VISTA, CA 91910		FOR COURT USE ONLY F I L E D <small>Clerk of the Superior Court</small> AUG 02 2024 By: L. Lubsen
PLAINTIFF(S)/PETITIONER(S) PEOPLE	JUDGE: DANIEL F. LINK DEPT: 21	
DEFENDANT(S)/RESPONDENT(S) PINA, ADRIAN	CASE NUMBER SCN429787	
CLERK'S CERTIFICATE OF SERVICE BY MAIL		

I certify that I am not a party to the above-entitled cause, that I placed a copy of the following document(s): **EX PARTE ORDER FOR PRODUCTION OF SUBPOENAED DOCUMENTS**

VIA Email

~~in a sealed envelope addressed to the parties shown with postage prepaid, and deposited it in the United States mail at~~
 Chula Vista El Cajon San Diego Vista, California.

NAME & ADDRESS

NAME & ADDRESS

Tyler G. Newby, Esq.
 Tnewby@fenwick.com

Natasha Amlani, Esq.
 NAmlani@perkinscoie.com

Janie Yoo Miller, Esq.
 jmillier@fenwick.com

Ryan Mrazik, Esq.
 RMrazik@perkinscoie.com

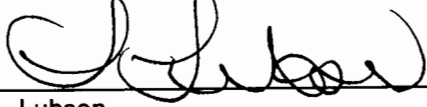
David W. Feder, Esq.
 dfeder@fenwick.com

DDA David Jarman
 DPD Nadine Valdecini

Esther D. Galan, Esq.
 egalan@fenwick.com

Julie E. Schwartz, Esq.
 JSchwartz@perkinscoie.com

Micheal C. Bleicher, Esq.
 MBleicher@perkinscoie.com

Clerk of the Superior Court
 by  Deputy
 L. Lubsen

Date: August 2, 2024