No. _____

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, Case Nos. SCN429787, SCN429787
Honorable Daniel J. Link, Judge Presiding

PETITION FOR REVIEW
IMMEDIATE STAY REQUESTED

PERKINS COIE LLP
Julie E. Schwartz, SBN 260624
jschwartz@perkinscoie.com
1201 Third Ave., Ste. 4900
Seattle, WA 98101
Telephone: (206) 359-3840

GIBSON, DUNN & CRUTCHER LLP
*Joshua S. Lipshutz, SBN 242557
jlipshutz@gibsondunn.com
One Embarcadero Center, # 2600
San Francisco, CA 94111
Telephone: (415) 393-8200

Additional counsel listed on signature block

Attorneys for Petitioner Meta Platforms, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

ISSUES PRESENTED FOR REVIEW

1. Section 2702 of the Stored Communications Act (18 U.S.C. § 2702) ("SCA") is the federal law that protects everyone's private communications on services like Facebook and Snap. Courts have uniformly held for decades that Section 2702 prohibits these service providers from disclosing these communications to anyone, except in narrow circumstances. The Court of Appeal broke from this settled precedent to hold that Section 2702 does not protect *anyone's* online communications on virtually *any* modern communications service. This Court should grant review of the Court of Appeal's published decision to decide: Does Section 2702 of the SCA protect users' electronic communications when a service provider is authorized to access those communications for discrete purposes, such as protecting and improving the service or delivering content?

2. The trial court ordered Meta to produce a crime victim's entire account history over a two-year period, without analyzing the good-cause factors in *City of Alhambra v. Superior Court* (1988) 205 Cal. App. 3d 1118. The Court of Appeal found good cause satisfied. This Court should grant review to decide: Are trial courts required to analyze the good-cause factors in the first instance?

INTRODUCTION

This petition raises a question of critical importance to anyone who uses the internet: Are people's private electronic communications protected by Section 2702 of the Stored Communications Act ("SCA")? In a deeply flawed decision, the Court of Appeal held that the answer is "no", eliminating the most important federal privacy protections for virtually all communications online and placing California at odds with federal law. This Court's review is needed to restore uniformity to the application of this critical federal statute, settle an important question of law, and revive these fundamental privacy protections for everyone's communications.

Section 2702 has been the bedrock federal law protecting online communications for decades. Courts uniformly apply Section 2702 to all manner of online communication services, including Facebook and Snapchat. But in this case, the Court of Appeal held that Section 2702 does not apply to *any* communications made on a service that can access the communications for discrete "business purposes," such as improving user experiences or ensuring the service's safety and integrity. Two prior members of this Court recognized the sweeping consequences of that holding as warranting "additional and focused attention" (*Facebook, Inc. v. Superior Court* (2020) 10 Cal.5th 329, 361 (*Touchstone*) [Cantil-Sakauye, C.J., conc.]), and carrying "profound implications" (*id.* at p. 374 [Cuéllar, J., conc.]). And rightly so; the court's holding guts the SCA's core privacy protections for *almost all* online communications because *almost all* online service providers today have been granted some rights by their users to access user communications for those or similar purposes.

The consequences of that decision will be profound. Billions of people use these services—from dating apps to email to Instagram—to communicate with each other daily. They discuss relationships, intimate

matters, politics, protests, and more. But without the SCA's privacy shield, virtually all of those communications can now be disclosed freely in California without fear of federal penalties. That will eviscerate the privacy rights of billions of people.

Worse, it will often do so in situations where privacy is most needed—such as when crime victims or witnesses fear for their safety. The subpoena at issue in this case, for instance, involves a murder defendant seeking his alleged victim's private communications. The Court of Appeal's decision hands new tools to such criminal defendants, as well as civil litigants, to obtain victims' or witness' private communications from online service providers—potentially even without notice to them. The Court of Appeal's decision thus does precisely what Congress feared: It turns online service providers into centralized buffets for discovery requests, opening decades of every internet user's most intimate communications to discovery and disclosure—none of which is even *possible* for traditional paper or vocal communications.

That result is legally wrong and contrary to Congress's core purpose in enacting the SCA: protecting people's privacy when using new forms of technology. The Court of Appeal eliminated the SCA's protections simply because people grant their service providers access to their communications for purposes that benefit users such as providing personalized experiences and keeping their platforms safe. That reads the statute backwards and is flatly inconsistent with both the SCA's text and purpose. And critically, the Court of Appeal's holding is inconsistent with every other court to have addressed this issue, including the Ninth Circuit. Left in place, this conflict will immediately upend the SCA and place *nearly every* internet user and service provider in the middle of an untenable conflict between California or federal law on this critical issue.

This Court's review is needed to resolve this profoundly important question, restore uniformity in the SCA's application, and protect internet users' critical privacy rights under the SCA.

BACKGROUND

A. The Stored Communications Act

Congress enacted the SCA as part of the 1986 Electronic Communications Privacy Act to protect individuals' privacy rights for their electronic communications. (See Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986).) At the time, Congress "was concerned that the significant privacy protections that apply to homes in the physical world may not apply to virtual homes in cyberspace." (*Facebook, Inc. v. Superior Court* (2018) 4 Cal.5th 1245, 1263 ("*Hunter*") [citation and internal quotations].) Congress "tried to fill this possible gap" (*ibid.*) by providing new "statutory standards to protect the privacy and security of communications transmitted by new" online communications services. (S. Rep. No. 99-541, at 5 (1986).) Congress's goal was to "encourag[e] the use and development of new technologies" by eliminating any "'legal uncertainty'" about privacy rights that could chill their development. (*Hunter*, *supra*, 4 Cal.5th at p. 1263 & fn. 16 [quoting H. Rep. 99-647, 2d Sess., p. 19 (1986)].)

Codified in the federal Criminal Code, the SCA thus restricts any entity that provides an "electronic communication service" (ECS) or a "remote computing service" (RCS) "to the public" from "knowingly divulg[ing] to any person or entity the contents of a [stored] communication." (18 U.S.C. § 2702(a)(1)–(2).)[1]

[1] The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (18 U.S.C. § 2510(15).) It defines an RCS as any any "provision to the public of computer storage or processing services by means of an electronic communications system." (18 U.S.C. § 2711(2).) There is no dispute that

More specifically, any entity providing an ECS "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." (18 U.S.C. § 2702(a)(1).) The statute defines "electronic storage" broadly 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 [ECS] for purposes of backup protection of such communication." (*Id.* § 2510(17) [emphasis added].)

An entity providing an RCS similarly cannot "knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service" if certain conditions are met. (18 U.S.C. § 2702(a)(2) [emphasis added].) First, the communication must be "(A) on behalf of, and received by . . . a subscriber or customer or such service." (*Ibid.*) Second, the communication must be received "(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." (*Ibid.*)

The SCA also contains nine specific exceptions to these disclosure prohibitions, as well a statutory mechanism for U.S. law enforcement to compel the disclosure of stored communications. (18 U.S.C. § 2702(b)(1)–(9); *id.* § 2703.) It does not, however, contain any provision that allows for criminal defendants or civil litigants to obtain covered communications absent a statutory exception.[2] (See *Facebook, Inc. v. Wint* (D.C. 2019) 199

Meta provides both ECS and RCS. (Accord Op. at 39 [discussing "users of ECS providers"]; *id.* at 40 [noting that Snap and Meta "provide RCS"].)

[2] For example, Section 2702(b)(3) allows disclosure with consent from the target of the subpoena (see *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 895–96 [holding that a person's consent to disclosure was sufficient

A.3d 625, 632 ["Congress did not intend to permit disclosure in response to criminal defendants' subpoenas"].) And any person "aggrieved" by a violation of the SCA may recover damages from the person or entity that committed the violation. (18 U.S.C. § 2707(a)–(c).)

B. Factual Background

This petition arises out of two subpoenas Meta and Snap received from Adrian Pina, a criminal defendant charged with murder, seeking the victim's stored electronic communications. Specifically, Pina subpoenaed Meta and Snap for "[a]ll records" associated with the victim's social media accounts for a two-year period. (Op. at 5 & fn. 2.) Pina alleged that the subpoenas could uncover evidence that the victim "could potentially have some violent tendencies"; the prosecutor described the subpoenas as a "fishing expedition." (Op. at 7, 15.)

Meta and Snap moved to quash the subpoenas, arguing, among other things, that the SCA prohibited each from making such disclosures absent a search warrant from the government, and that the subpoenas lacked good cause. (Op. at 6.) The trial court denied the motions, "finding probable cause" for the subpoenas and concluding that "any other governmental or constitutional protections . . . become irrelevant because I've now found probable cause." (1/8/24 Tr. 18:7–17.)[3] The trial court also glancingly discussed two of the factors that this Court adopted from *City of Alhambra v. Superior Court* (1988) 205 Cal.App.3d 1118, in *Touchstone*, *supra*, 10 Cal.5th at p. 345. (See 1/8/24 Tr. 9:15.) The trial court then announced that it had "gone through the *Alhambra* factors," that "there's absolutely probable

---

under the SCA even though the consent was compelled by a court order]), but consent is not at issue here (see Op. at 37).

[3] Because the trial court found probable cause, it also noted that "a prosecution agency" could obtain these materials, such as by using a warrant. (1/8/24 Tr. 11:24–28.)

cause," and that the "material sought" was "relevant" and not "publicly available." (Tr. 9:16; 10:1; 11:24–25.) Meta and Snap both sought writ review.

C. The Court of Appeal's Decision

The Court of Appeal, Fourth District, affirmed in a published opinion. The court began by noting that the appeal raised a "critical issue" that two members of this Court in *Touchstone* had "asked [California's] lower courts to address": whether Meta and Snap's "business models place them outside key provisions of the SCA and render them subject to an enforceable state subpoena." (Op. at 20, 30 [internal brackets omitted].) The Court then *sua sponte* took judicial notice of Meta's terms of use (Op. at 23–25), under which Meta's account-holders authorize Meta to, among other things, "help [them] find and connect with people" they "may want to become friends with," "show [them] personalized ads," and "detect potential misuse" and "harmful conduct." (Facebook, Terms of Service, <https://www.facebook.com/legal/terms> (last revised July 26, 2022).) Snap provided its own terms of use. (Op. 38 fn. 16.) Based on those terms, the court held that neither of the SCA's bars on the disclosure of communications by ECS and RCS providers applied to anyone's communications held by Meta or Snap. (Op. at 38, 40.) The court recognized "the import of [its] decision" and its far-reaching consequences on user privacy, but nonetheless held that Section 2702 did not apply. (Op. at 44.)

Specifically, the court first held that the bar on disclosures by ECS providers does not apply to content held by Meta or Snap because the court believed Meta and Snap do not hold people's content exclusively for "electronic storage." (Op. at 38–39.) The court conceded that Meta and Snap "store the content of their user's communications incidentally to transmission and for purposes of backup" in accordance with the SCA's definition of "electronic storage." (Op. at 38.) But it then stated that Snap and Meta "also

maintain that content for their own business purposes," and concluded—without any analysis of the statutory text—that any "dual purpose brings the content outside the SCA's" privacy rights and disclosure prohibitions in Section 2702(a)(1). (Op. at 39.)

The court then turned to the RCS provision, which bars providers from disclosing content it received from users, including any content received "(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." (18 U.S.C. § 2702(a)(2)(B), bold italics added; see Op. at 40.) The court held that the RCS provision does not apply because Meta and Snap do not maintain people's content "*solely* for the purpose of providing storage or computer processing services." (Op. at 40.) But the court applied that statutory requirement even though it is triggered only *if* the provider is *not* permitted to access communications for other purposes. (See Op. at 41.) The court's only reason for declining to apply the threshold condition in this "if" clause was that doing so was not "logical" or "supported by [the SCA's] legislative history." (Op. at 41.)

The appellate court also found good cause to enforce the subpoenas before it. (Op. at 13.) The court noted that the trial court's repeated reference "to the probable cause standard" was "not . . . correct," but nonetheless stated that the trial court's passing reference to "the *Alhambra* factors" was sufficient to satisfy "*Touchstone*'s requirement that the court 'articulate orally, and have memorialized in the reporter's transcript, its consideration of the relevant factors.'" (Op. at 14 [quoting *Touchstone*, *supra*, 10 Cal.5th at p. 358].) The court then proceeded to analyze each of the seven *Alhambra* factors, going far beyond the trial court's cursory analysis, before finding good cause for the subpoenas. (Op. at 14–19.)

The court rendered its decision as final forthwith, giving Meta no chance to petition for rehearing before seeking this Court's review. The court also provided that a stay of the trial court's decision it had previously issued would expire on August 2, 2024—the same day this petition was due to be filed. And on August 2, 2024, before the stay expired, the trial court ordered Meta "to produce the subpoenaed records . . . by the end of business day August 5th, 2024."

DISCUSSION

I. Whether the SCA Protects Private Electronic Communications Is an Important Legal Question the Court of Appeal Got Wrong.

This petition asks this Court to decide whether people's private electronic communications are protected by Section 2702 of the SCA—the key federal law designed to protect these communications. The Court of Appeal's decision that the SCA does not protect private messages from disclosure threatens the privacy of everyone who uses the internet. This Court's review is therefore required to "settle an important question of law" (Cal. Rules of Court, Rule 8.500(b)(1)) and restore these fundamental federal privacy protections.

A. Whether the SCA Protects Private Electronic Communications Is Critically Important.

The SCA protects internet users' privacy by forbidding online service providers like Meta from "knowingly divulg[ing] [communications content] to any person or entity" unless a limited statutory exception applies. (18 U.S.C. § 2702(a), (b).) The Court of Appeal, however, eviscerated that statutory framework, holding that because Meta can access messages and other content for "business purposes" (like removing spam and fraud and providing a personalized experience), the SCA does not protect people's private online communications. (Op. at 38.) If not corrected, the Court of

Appeal's order will undermine a federal statute's text and purposes by (1) gutting its privacy protections for all internet users, (2) harming crime victims and witnesses by disclosing their private content to criminal defendants, (3) allowing civil litigants and almost anyone to obtain others' private electronic communications from providers directly, rather than from the user whose communications are sought, with potentially no notice to the user, and (4) placing immense burdens on any online service provider by forcing them to choose between complying with California or federal law on this issue. These are issues of significant public interest and call for review by this Court—as two members of this Court have previously recognized. (See *Touchstone*, *supra*, 10 Cal.5th at p. 361 [Cantil-Sakauye, C.J., conc.]; *id.* at p. 374 [Cuéllar, J., conc.].)

First, the Court of Appeal's ruling is contrary to Congress's core purpose in enacting the SCA: protecting privacy. The SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications" made through online service providers. (*Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, 1072.) More specifically, the SCA's disclosure prohibitions were designed to "lessen the disparities between the protections given to established modes of private communication and those accorded new communications media." (*O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1444.) Unlike traditional forms of communication, such as personally-held physical letters and phone calls "as ephemeral as a conversation on a street corner," electronic messages are indefinitely and centrally stored—and thus subject to sweeping and invasive discovery that is unavailable for traditional communications. (*Id.* at 1445.) In enacting the SCA, Congress sought to offset that unique "informational windfall" and ensure that new technology would not result in a dramatic loss of individuals' privacy. (*Id.* at 1447.)

Although Congress enacted the SCA in 1986, before the advent of the modern internet, the importance of the statute's protections has only increased as electronic communications have become intertwined with our everyday lives. More and more, people's lives are centered online and they increasingly rely on the internet and electronic devices to send messages that they intend for a limited audience. (See *Carpenter v. United States* (2018) 585 U.S. 296, 311 [noting the breadth of private information that can now be obtained "[w]ith just the click of a button"]; *Riley v. California* (2014) 573 U.S. 373, 386 [explaining the "vast quantities of personal information" people store digitally].) People likewise increasingly turn to the internet for intimate personal communications, such as meeting potential partners and spouses, communicating with loved ones, and engaging in political speech and protest movements.

But the Court of Appeal's ruling all but eliminates the SCA's protections in California courts for the billions of people who communicate over the internet. If the ruling is allowed to stand, the SCA's key disclosure prohibitions would protect virtually no private electronic communications, because nearly *all* online service providers in the modern internet age—from dating apps to email service providers to Meta—employ terms of use permitting the provider to access people's content to, for example, uphold the safety and integrity of the platform.[4] Indeed, California law requires many providers to "publicly post" a "general description of [their] moderation practices that are employed to prevent users from posting or

[4] Although the Court of Appeal seems to have recognized that certain communications held by Meta or Snap are protected by the SCA—for example, if they are currently in electronic transit—its holding means that the overwhelming majority of people's existing online communications are unprotected.

sharing electronic content pertaining to the illegal distribution of a controlled substance." (Bus. & Prof. Code § 22945(b)(2).)

If Meta's standard terms exempt user communications on Facebook and Instagram from the SCA's disclosure prohibitions, as the Court of Appeal wrongly concluded, then communications sent or received on nearly every online service are also no longer protected. The SCA would no longer bar providers from freely disclosing people's online communications *at all*—whether voluntarily (including for profit), in response to subpoenas from civil or criminal litigants, or perhaps even in response to pressure from state, federal, or foreign governments. And further, removing the SCA's disclosure prohibitions would free online service providers of federal limits on their ability to disclose private communications even without informing people that their content is being disclosed. As a result, billions of people's privacy interests will vanish unless this Court corrects the lower courts' errors.

Second, the implications of the Court of Appeal's decision are particularly harmful to victims and witnesses of crimes. Under the holding below, criminal defendants on trial for all sorts of crimes can seek access from providers to their victim's private content—as well as the accounts and contents of witnesses—eroding people's privacy rights in situations where privacy may be most needed. (See *Hunter*, *supra*, 4 Cal.5th at pp. 1254–55 [defendant seeking murder witness's Facebook communications]; *Touchstone*, *supra*, 10 Cal.5th at p. 336 [defendant seeking attempted murder victim's records].) Criminal defense attorneys have already recognized the sweeping effect of that holding, asserting that the Court of Appeal's decision "opens up a new world of possibilities" for subpoenaing victims' and witnesses' private content. (Cheryl Miller, *California Appellate Court Opens 'New World of Possibilities' With Social Media Subpoena Decision*, (July 26, 2024) <https://tinyurl.com/5t5bycx8> [as of Aug. 2, 2024].) And

no wonder; under the Court of Appeal's decision, criminal defendants will be able to seek the communications of victims and witnesses with few legal hurdles—and potentially without even notifying the victims or witnesses, who may never know or have the chance to object to disclosures of their most sensitive content.

Third, that loss of privacy will be amplified because the Court of Appeal's holding is not limited to criminal defendants. The SCA works by barring providers from voluntarily disclosing account-holders' communications; if Section 2702 does not apply to these communications, providers will be free to disclose user communications without the constraints Congress has imposed whenever the service provider decides to do so.[5] And ordinary civil litigants may be able to obtain the most intimate private communications of anyone they wish with a simple subpoena, employing the same logic as the Court of Appeal. (See *O'Grady*, *supra*, 139 Cal.App.4th at p. 1447 [the SCA treats "an email service provider [a]s a kind of data bailee to whom [data] is entrusted," and who "should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent"].)

Fourth, the Court of Appeal's decision imposes substantial burdens on any online service provider that permits people to send private messages. Along with the goal of protecting people's privacy, the SCA was intended to shield providers from being inundated with disclosure requests and subpoenas in criminal and civil litigation. (*Hunter*, *supra*, 4 Cal.5th at

[5] Indeed, by saying Meta and Snap must show that they "comply" with the "statute's requirements," the Court of Appeal flipped Section 2702 from a law that protects communications by restricting providers to a law that benefits providers. (Op. at 42.) Under the SCA, it's the opposite: Providers "have the burden to establish" when Section 2702 *does not apply* if they want to avoid liability for violating its restrictions. (*In re Google Assistant Privacy Litig.* (N.D. Cal. 2020) 457 F. Supp. 3d 797, 823.)

p. 1290 ["With regard to burdens related to disclosure in particular, Congress significantly limited the potential onus on providers by establishing a scheme under which a provider is effectively prohibited from complying with a subpoena issued by a nongovernmental entity"].) The Court of Appeal's decision, however, threatens service providers with an onslaught of requests and subpoenas from litigants seeking discovery from providers directly, as opposed to from the senders and recipients of the content the litigants seek. And those burdens will be amplified because providers will be caught between one disclosure rule in California and the SCA's rule everywhere else.

Finally, nullifying the SCA's key disclosure prohibitions threatens to harm the implementation and development of new technologies, thwarting another of Congress's goals. As Congress recognized in passing the SCA, if "potential customers have less protection when they use an electronic medium than with paper, there may be a disincentive to use an electronic service." (H.R. Rep. No. 99-647, 2d Sess., p. 26 (1986).) The Court of Appeal's decision does precisely what Congress feared: It creates a centralized buffet for discovery requests—online service providers—that has no analogue in the physical world. Likewise, Congress feared that if electronic communications went unprotected, that privacy gap could "discourage American businesses from developing new innovative forms of telecommunications and computer technology." (S. Rep. No. 99-541, 2d Sess., p. 5.) Again, the Court of Appeal's decision brings to life Congress's concerns. By stripping the SCA's core protections from electronic communications made on modern services, which need to handle modern concerns (like online security and integrity), the Court of Appeal hinders technological innovation. (See *Hunter*, *supra*, 4 Cal.5th at p. 1289.)

Unless this Court grants review and corrects the lower court's erroneous interpretation of the SCA, billions of people's privacy rights will

immediately suffer. Crime victims and witnesses will be exposed to privacy invasions and additional trauma, and every electronic messaging or storage service provider in the State will be inundated with discovery requests seeking its users' private messages. This Court's review is needed to resolve the important question of whether Section 2702 of the SCA protects private electronic communications.

B. The SCA Protects Electronic Communications Regardless of Whether Users Let the Service Provider Access Those Communications for Limited Purposes.

The Court of Appeal's refusal to apply the SCA to these communications is wrong twice over.

First, the Court of Appeal wrongly inserted the term "solely" into the ECS provision. (See *California Cannabis Coalition v. City of Upland* (2017) 3 Cal.5th 924, 939 ["In the construction of a statute or instrument, the office of the Judge is simply to ascertain and declare what is in terms or in substance contained therein, not to insert what has been omitted."], quoting Code Civ. Proc. § 1858.) That provision protects any communications held in "electronic storage," and the Court of Appeal acknowledged that the communications held by Meta meet that test: Meta retains people's communications "incidentally to transmission and for purposes of backup" (Op. at 38)—the statutory definition of "electronic storage" (18 U.S.C. § 2510(17) ["[A]ny temporary, intermediate storage . . . incidental to the electronic transmission [and] any storage . . . for purposes of backup protection."]). But the Court of Appeal then stated that if Meta also retains communications for any *additional* purpose, the ECS provision does not protect those communications. (Op. at 38–39.) Nothing in the statute supports that conclusion. The SCA's text never requires that storage be *only* or *solely* for the purposes enumerated in its definition of "electronic storage,"

and the Court of Appeal was wrong to strip people's privacy rights by injecting that limit into the SCA's text.

In addition to incorrectly inserting a new term into the ECS provision of the statute, the Court of Appeal improperly disregarded a conditional clause in the RCS provision that Congress clearly intended to be there. That provision applies the SCA's protections to any communication (A) "received by means of electronic transmission from" users; (B) "***if*** the provider is ***not*** authorized to access the . . . communications for purposes of providing any [other] services," the communication must have been received "solely for the purpose of providing storage or computer processing services." (18 U.S.C. § 2702(a)(2).) Yet the Court of Appeal ignored the "if" condition in clause (B) even though, under its view, that condition is not met because Meta ***is*** "authorized to access the content" for "other purposes." (*Ibid.*) This interpretation makes little sense. If that condition is not met—i.e., if Meta is authorized to access content for other purposes—then the requirement that Meta receive communications "solely for the purpose of providing storage or computer processing services" does not apply based on a straightforward reading of the text. (See *ibid.*) And even if that requirement does apply (which it does not), Meta's services—even if also serving Meta's business purposes—*are* "computer processing services" because Meta's users authorize those services to enhance their Meta experience and functionality.

Both of those interpretations violate the statutory text and purpose of the SCA, which was explicitly designed to give people flexibility in creating and using new communications technologies while still retaining their privacy rights. The Court of Appeal's holdings, however, would strip people of their privacy rights whenever they authorize providers to access or store their communications for virtually any function, such as providing personalized content or connecting individuals with each other. That is not what the text provides, and it is not what Congress intended.

II. The Decision Below Conflicts with Many Cases that Have Applied the SCA's Disclosure Prohibitions in Similar Circumstances.

In addition to deciding an important question of law incorrectly, the Court of Appeal's ruling upends years of precedent. No other court has ever held that the SCA's disclosure prohibitions do not apply to providers like Meta. This creates an intolerable split between California and federal courts applying the same federal law. Thus, this Court's review is also required to "secure uniformity of decision" (Cal. Rules of Court, rule 8.500(b)(1)), and bring California's interpretation of federal law back in line with the many federal and other state courts that have considered the issue.

The Ninth Circuit Court of Appeals, for example, has held that ECS providers are subject to the SCA's disclosure prohibitions for any communication held in electronic storage at least *in part* "for purposes of backup protection." (*Theofel*, *supra*, 359 F.3d at p. 1075.) The Ninth Circuit, unlike the Court of Appeal below, did not insert language into the SCA imposing any requirement that an ECS hold a communication *solely* for backup purposes to trigger the SCA's disclosure prohibitions. (*Ibid.* [explaining that ECS disclosure prohibitions apply to a provider because *one* "obvious purpose for storing a message on an ISP's server after delivery is to provide" backup protection].)

The Fourth Circuit has likewise held that private messages preserved by an online provider for future access are protected by the SCA's disclosure prohibitions, regardless of whether backup protection is the *sole* purpose for which the provider stores them. (*Hately v. Watts* (4th Cir. 2019) 917 F.3d 770, 795.) Indeed, the Fourth Circuit held that online service providers' practice of using copies of stored emails "for their own commercial purposes, such as to more effectively target advertisements," did not negate the application of the SCA's disclosure prohibitions. (*Ibid*.)

Finally, other state and federal district courts have followed the Ninth and Fourth Circuits' leads, consistently applying the SCA's ECS and RCS disclosure prohibitions to online service providers who, like Meta, permit account-holders to send private messages. (See *Republic of Gambia v. Facebook, Inc.* (D.D.C. 2021) 575 F.Supp.3d 8, 13 [where Facebook stored communications for, "'among other reasons, in case it was lawfully called upon to produce them,'" its storage is protected by the SCA's ECS disclosure prohibitions]; *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.* (D.N.J. 2013) 961 F.Supp.2d 659, 667 [holding that Facebook is an ECS]; *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."]; *Wint*, *supra*, 199 A.3d at p. 631 ["The plain text of the SCA thus appears to foreclose Facebook from complying with [a defendant's] subpoenas."]; *Viacom Int'l Inc. v. Youtube Inc.* (S.D.N.Y. 2008) 253 F.R.D. 256, 264 [holding that YouTube is an RCS].)

To be sure, some courts have held that enumerated *exceptions* to the SCA's disclosure prohibitions apply in certain circumstances. (See *Hunter*, *supra*, 4 Cal.5th at p. 1250 [holding that Facebook may disclose content configured as public under the SCA's statutory exception for disclosure with the sender's lawful consent]; *Facebook, Inc. v. Pepe* (D.C. 2020) 241 A.3d 248, 255-56 [permitting disclosure under exception for recipient's lawful consent]; *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 904 [same].) But *no court*, until the Court of Appeal's decision below, has held that when an online service provider obtains an account-holder's consent to access content for certain *limited* purposes, that user loses the SCA's protections against disclosure for *all* purposes. This Court should grant review to restore uniformity of decisions and ensure that the SCA continues to protect internet users' privacy in California courts.

III. In the Alternative, This Court Should Grant Review to Reiterate that Trial Courts Must Adhere to the Good Cause Standard.

The Court should also grant review to, in the alternative, clarify its holding in *Touchstone* that "a trial court" ruling on a motion to quash must "at a minimum, articulate orally, and have memorialized in the reporter's transcript, its consideration of the [*Alhambra*] factors." (10 Cal.5th at 358.) The point of that requirement is to "create a record that facilitates meaningful appellate review." (*Ibid.*) But the Court of Appeal failed to apply that requirement and, in doing so, created a split in authority among California's courts.

The Court of Appeal acknowledged that the trial court "referred several times" to an incorrect "probable cause standard" when deciding to enforce the subpoenas. (Op. at 14.) And though the trial court "stat[ed] explicitly it had considered the [*Alhambra*] factors" (Op. at 14), the trial court at most discussed two of the seven factors without any reference to the others. (Compare Tr. at 9–12 [discussing whether the material is available from other sources and whether the material requested is overly broad], with *Touchstone*, *supra*, 10 Cal.5th at p. 346–47 [listing other factors].) But despite that failure to "articulate orally . . . its consideration of the [*Alhambra*] factors" (*id.* at 358), the Court of Appeal did not remand the case and instead arrogated to itself the role of a court of first view, rather than review, analyzing the seven *Alhambra* factors in the first instance. That is error.

The Court of Appeal's failure conflicts with another decision by the Court of Appeal, *Lunsted v. Superior Court* (2024) 100 Cal.App.5th 138, 150. In *Lunsted*, the trial court likewise never "'expressly considered and balanced' the seven required factors" and instead "applied an incorrect standard" at a motion to quash hearing. (*Id.* at 149–50 [quoting *Touchstone*, *supra*, 10 Cal.5th at 356].) The party trying to enforce the subpoena argued,

as the Court of Appeal here held, that the trial court "must have" considered those factors and that the record supported a finding of good cause anyway. (*Ibid.*) But the *Lunsted* court refused to affirm. Instead, it remanded for the trial court "to reconsider the motion to quash under [*Touchstone*]." (*Id.* at 151.) That holding is irreconcilable with the Court of Appeal's holding here. This Court accordingly should also grant review to, in the alternative, resolve that confusion and enforce *Touchstone*'s holding.

IV. This Court Should Stay Enforcement of the Subpoena and Production Pending This Court's Review.

Meta also respectfully asks this Court to issue an immediate stay of the Superior Court's order requiring Petitioner to comply with the defendant's subpoena. The Court of Appeal initially stayed the Superior Court's order when it granted review of Meta's writ petition on January 24, 2024. But the Court of Appeal's decision provides that the stay "is vacated on August 2, 2024." (Op. at 45.) And on August 2, before remittitur issued and before the stay expired, the trial court ordered Meta and Snap "to produce the subpoenaed records . . . by the end of business day August 5th, 2024."

If the stay of the Superior Court's order is not extended, Meta will be forced to choose between not complying with the trial court's order and risking contempt of court, or complying with the order only for this Court or the U.S. Supreme Court to determine that Meta thereby violated the SCA, teeing up potential civil liability. (See 18 U.S.C. § 2707.) If an immediate stay is not granted and Meta does not comply with that order, the trial court may initiate contempt proceedings. Yet if Meta *does* comply, the central relief sought by this Petition—relief from a compulsion to produce private communications in violation of federal law—may become moot.

CONCLUSION

The Court should grant the petition and stay the enforcement of the subpoena and production order pending review.

Dated: August 2, 2024

Respectfully Submitted,

PERKINS COIE LLP
Julie E. Schwartz, SBN 260624
jschwartz@perkinscoie.com
Ryan T. Mrazik, *Pro Hac Vice Forthcoming*
John R. Tyler, *Pro Hac Vice Forthcoming*
1201 Third Ave., Ste. 4900
Seattle, WA 98101
Telephone: (650) 838-4300
Telephone: (206) 359-8098

Natasha Amlani, SBN 322979
namlani@perkinscoie.com
1888 Century Park East
Suite 1700
Los Angeles, CA 90067
Telephone: (310) 788-3347

Joshua S. Lipshutz, SBN 242557
GIBSON, DUNN & CRUTCHER LLP
jlipshutz@gibsondunn.com
One Embarcadero Center, # 2600
San Francisco, CA 94111
Telephone: (415) 393-8200

GIBSON, DUNN & CRUTCHER LLP
Michael J. Holecek, SBN 281034
mholecek@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 229-7018

Natalie J. Hausknecht, *Pro Hac Vice Forthcoming*
1801 California Street
Suite 4200
Denver, CO 80202
Telephone: (303) 298-5783

Attorneys for Petitioner Meta Platforms, Inc.

CERTIFICATE OF COMPLIANCE

Under rule 8.504(d)(1) of the California Rules of Court, I, JOSHUA S. LIPSHUTZ, hereby certify that, based on the software in the Microsoft Word program used to prepare this document, that this petition contains 5,991 words, excluding the cover page, tables of content and authorities, signature block, and this certification.

Dated: August 2, 2024

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

JOSHUA S. LIPSHUTZ

By: 

Joshua S. Lipshutz
Attorney for Petitioner Meta Platforms, Inc.

PROOF OF SERVICE

I, David Lam, declare as follows:

I am employed in the county of Los Angeles, State of California; I am over the age of eighteen years and am not a party to this action; my business address is 333 South Grand Avenue, Los Angeles, California 90071, in said county and state. On August 2, 2024, I served the following document:

PETITION FOR REVIEW
IMMEDIATE STAY REQUESTED

to the persons named below at the address shown, in the manner described below.

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

San Diego County Superior Court,
Respondent
Hon. Daniel F. Link, Judge C/O Judicial Services
325 S. Melrose, Department 21
Vista, CA 92081

Fenwick & West,
Petitioner Snap Inc.
Attn: Tyler G. Newby
555 California Street #12
San Francisco, CA 94101
tnewby@fenwick.com

Paul Rodriguez, Public Defender
Troy A. Britt, Deputy Public Defender
For Real Party in Interest Adrian Pina
450 B Street, Suite 1100
San Diego, CA 92101
troy.britt@sdcounty.ca.gov

Summer Stephen, District Attorney
Linh Lam, Deputy District Attorney
Karl Husoe, Deputy District Attorney
For Real Party in Interest The People
P.O. Box X-1011
San Diego, CA 92112
karl.husoe@sdcda.org

☑ **BY OVERNIGHT DELIVERY**: On the above-mentioned date, I enclosed the documents in an envelope or package provided by an overnight delivery carrier and addressed to the persons at the addresses shown above. I placed the envelope or package for collection and overnight delivery at an office or a regularly utilized drop box of the overnight delivery carrier with delivery fees paid or provided for.

☑ **BY ELECTRONICALLY FILING**: the foregoing with the Clerk of the County using TrueFiling electronic case filing system which will send notification of such electronic filing to counsel on record for all parties by operation of the TrueFiling system.

I certify under penalty of perjury that the foregoing is true and correct, and that the foregoing document was executed by me on August 2, 2024, at Irvine, California.

_____

David Lam

APPENDIX

Filed 7/23/24

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 Act[1]). 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, W*hat 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 withing section 2702(b)(3)'s lawful consent exception, presumptively permitting disclosure by a provider"].)

Separate from the settled issue of public verses 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 appliable 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' "].)

18 U.S.C. § 2702

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

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

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

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

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

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

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

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

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

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

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

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

(7) to a law enforcement agency--

(A) if the contents--

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

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

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

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

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

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

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

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

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

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

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

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

(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

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

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

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

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

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

18 U.S.C. § 2510

As used in this chapter--

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[1]

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

> **(a)** any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
>
> **(b)** a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations

of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic

communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means--

(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) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. § 2711

As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes--

> **(A)** any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--
>
> > **(i)** has jurisdiction over the offense being investigated;
> >
> > **(ii)** is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
> >
> > **(iii)** is acting on a request for foreign assistance pursuant to section 3512 of this title;
>
> **(B)** a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; or
>
> **(C)** a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice) to which a military judge has been detailed; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.