No. S286267

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

SNAP INC., ET AL.,

Petitioners,

vs.

SUPERIOR COURT OF SAN DIEGO COUNTY,

Respondent,

ADRIAN PINA, ET AL.,

Real Parties in Interest.

Fourth Appellate District, Div. 1, Case Nos. D083446, D083475
San Diego Superior Court, Dept. 21, Case No. SCN429787
Honorable Daniel F. Link, Judge Presiding

APPLICATION FOR LEAVE TO FILE AMICI CURIAE BRIEF

AND

PROPOSED BRIEF OF AMICI CURIAE ACLU OF NORTHERN CALIFORNIA AND ACLU IN SUPPORT OF PETITIONERS

Jacob Snow (SBN 270988)
jsnow@aclunc.org
Nicole A. Ozer (SBN 228643)
nozer@aclunc.org
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493

Jennifer Granick (SBN 168423)
jgranick@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, Seventh Floor
San Francisco, CA 94110
Telephone: (415) 343-0758

Attorneys for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES 3

APPLICATION FOR LEAVE TO FILE AMICI CURIAE BRIEF 8

INTERESTS OF AMICI CURIAE 8

BRIEF OF AMICI CURIAE 10

INTRODUCTION 10

ARGUMENT 13

I. The appellate court holding is contrary to Congress's intent, precedent, and practice. 13

A. Congress's intent in passing the Stored Communications Act was to ensure the privacy of electronic communications regardless of whether the Fourth Amendment applies. 13

B. The SCA protects communications even if the provider also uses those materials for its own business purposes. 17

II. CalECPA does not adequately protect Californians if the Court of Appeal's decision is allowed to stand. 22

III. To the extent this Court is concerned about social media's business models' negative impact on users' privacy, California law provides meaningful protections to guard against privacy-invasive business practices. 24

A. Californians are guaranteed a robust constitutional right to privacy against private actors under Article I, section 1 of the California Constitution. 25

B. The California Consumer Privacy Act also includes protections against use of information for targeted advertising. 29

CONCLUSION 32

CERTIFICATE OF WORD COUNT 33

PROOF OF SERVICE 34

TABLE OF AUTHORITIES

Cases **Page**

Brooks v. Thomson Reuters Corp.,
(N.D. Cal., Aug. 16, 2021, No. 21-CV-01418-EMC) 2021 WL 3621837 29

Calhoun v. Google, LLC,
(9th Cir. 2024) 113 F.4th 1141 29

Carpenter v. U.S.,
(2018) 585 U.S. 296 ..... 9, 15

*Facebook, Inc. v. Superior Court of San Dieg*o County,
(2020) 10 Cal.5th 329 (“*Touchstone*”) 22, 23

Facebook, Inc. v. Superior Court,
(2018) 4 Cal.5th 1245 (“*Hunter*”) 21

Herring v. U.S.,
(2009) 555 U.S. 135 9

Hill v. Nat. Collegiate Athletic Assn.,
(1994) 7 Cal.4th 1 ..... 9, 26

In re Ricardo P.,
(2019) 7 Cal.5th 1113 9

In re United States for an Ord. Pursuant to 18 U.S.C. § 275(b),
(D.D.C. 2018) 289 F.Supp.3d 201 20

In re United States for Prtt Ord. for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841,
(D.D.C., Mar. 2, 2018, No. 18-PR-00017) 2018 WL 1358812 ... 21

Quon v. Arch Wireless Operating Co., Inc.,
(9th Cir. 2008) 529 F.3d 892 ..... 19, 20

Renderos v. Clearview AI, Inc.,
(A167179, app. pending) 29

Republic of Gambia v. Facebook, Inc.,
(D.D.C. 2021) 575 F.Supp.3d 8 21

Riley v. California,
(2014) 573 U.S. 373 9

Sheehan v. San Francisco 49ers, Ltd.,
(2009) 45 Cal.4th 992 9

Smith v. Maryland,
(1979) 442 U.S. 735 15

Snap, Inc. v. Superior Court of San Diego County,
(2024) 103 Cal.App.5th 1031 ("*Pina*") .....passim

Suzlon Energy Ltd. v. Microsoft Corp.,
(9th Cir. 2011) 671 F.3d 726 ..... 16, 21

Theofel v. Farey-Jones,
(9th Cir. 2004) 359 F.3d 1066 ..... 19, 20, 22

Twitter, Inc. v. Garland,
(9th Cir. 2023) 61 F.4th 686 21

U.S. v. Miller,
(1976) 425 U.S. 435 15

U.S. v. Warshak,
(6th Cir. 2010) 631 F.3d 266 15

White v. Davis,
(1975) 13 Cal.3d 757..... 9, 25, 26

Statutes

18 U.S.C. §§ 2701–2712 14

18 U.S.C. § 2702 ..... 11, 18

18 U.S.C. § 2703 ..... 11, 19

18 U.S.C. § 2510 ..... 18, 19, 22

Cal. Const., art. I, § 1 .....passim

Civ. Code, § 1798.100 30

Civ. Code, § 1798.110 30

Civ. Code, § 1798.120..... 30

Civ. Code, § 1798.185..... 30

Civ. Code, § 1798.199.10..... 30

Civ. Code, § 1798.199.40..... 30

Pen. Code, § 1546.1, subd. (f) 11, 23

Pub.L. No. 99-508, (Oct. 21, 1986) 100 Stat. 1860. 14

Rules

Cal. Rules of Court, rule 8.520(f) 8

Other Authorities

Ballot Pamp., Gen. Elec. (Nov. 3, 2020) text of Prop. 24 30

Cal. Reg. Notice Register 2024, No. 47-Z..... 30, 31

H.R.Rep. No. 99-647, 2d Sess. (1986) 14, 15

Sen.Rep. No. 99-541, 2d Sess. (1986)..... 14, 15, 17

Airbnb, *Privacy Policy* (Feb. 6, 2025) Help Center <https://www.airbnb.com/help/article/3175#1> [as of Feb. 23, 2025]..... 21

Akselrod & Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired* (Aug. 3, 2023) ACLU: News & Commentary <https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired> [as of Feb. 23, 2025]..... 27

Andrews, *How Flawed Data Aggravates Inequality in Credit* (Aug. 6, 2021) Stanford University Human Centered Artificial Intelligence <https://hai.stanford.edu/news/how-flawed-data-aggravates-inequality-credit> [as of Feb. 23, 2025] 27

Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why* (Apr. 6, 2023) N.Y. Times <https://www.nytimes.com/2023/04/06/opinion/online-

advertising-privacy-data-surveillance-consumer-quality.html> [as of Feb. 23, 2025]..... 28

Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic* (Dec. 18, 2020) Time Magazine <https://time.com/5921820/facebook-shopping-scams-holidays-covid-19> [as of Feb. 23, 2025]..... 28

De Chant, *Amazon is using algorithms with little human intervention to fire Flex workers* (June 28, 2021) ArsTechnica <https://arstechnica.com/tech-policy/2021/06/amazon-is-firing-flex-workers-using-algorithms-with-little-human-intervention/> [as of Feb. 23, 2025]..... 27

Evans, *Amazon's Warehouse Quotas Have Been Injuring Workers for Years. Now, Officials Are Taking Action* (May 16, 2022) Reveal News <https://revealnews.org/article/amazons-warehouse-quotas-have-been-injuring-workers-for-years-now-officials-are-taking-action/> [as of Feb. 23, 2025] 27

Fry, *Landlords Are Using AI to Raise Rents—and Cities Are Starting to Push Back* (Dec. 7, 2024) Gizmodo <https://gizmodo.com/landlords-are-using-ai-to-raise-rents-and-cities-are-starting-to-push-back-2000535519> [as of Feb. 23, 2025]..... 27

Germain, *The FBI Says You Need to Use an Ad Blocker* (Dec. 22, 2022) Gizmodo <https://gizmodo.com/google-bing-fbi-ad-blocker-scam-ads-1849923478> [as of Feb. 23, 2025]..... 28

Heaven, *Predictive policing algorithms are racist. They need to be dismantled* (July 17, 2020) MIT Technology Review <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/> [as of Feb. 23, 2025] 27

Koebler, *Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons* (Aug. 23, 2023) 404 Media <https://www.404media.co/instagram-ads-illegal-content-drugs-guns-hackers/> [as of Feb. 23, 2025] 28

Ozer, *Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age* (2024) 39 Berkeley Tech. L.J. 963 <https://btlj.org/wp-content/uploads/2025/01/39-2_Ozer.pdf> [as of Feb. 23, 2025] 25

Schnadower-Mustri, Adjerid, & Acquisti, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation* (Mar. 23, 2023) SSRN <https://ssrn.com/abstract=4398428> [as of Feb. 23, 2025] 28

Silverman & Mac, *Facebook Profits As Users Are Ripped Off By Scam Ads* (Dec. 10, 2020) BuzzFeed News <https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam> [as of Feb. 23, 2025] 28

Wu et al., *The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People* (June 12, 2023) 2023 ACM Conference on Fairness, Accountability, and Transparency <https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594119> [as of Feb. 23, 2025] 28

APPLICATION FOR LEAVE TO FILE AMICI CURIAE BRIEF

Pursuant to rule 8.520(f) of the California Rules of Court, proposed amici curiae respectfully request leave to file the accompanying Proposed Brief of Amici Curiae in Support of Petitioners.

INTERESTS OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the United States and California Constitutions and our nation's civil rights laws. Amici are the ACLU of Northern California and the ACLU. The ACLU affiliates in California have a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil rights and liberties. Amici supported the passage of the California Electronic Communications Privacy Act and served as key advisors to the law's authors, Senators Mark Leno and Joel Anderson, throughout the legislative process. Amici have frequently appeared as counsel to parties and amici before this Court and the United States Supreme Court in cases implicating the right

---

[1] Pursuant to rule 8.520(f)(4), amici state that no counsel for a party authored this brief in whole or in part, and no other person or entity, other than amici curiae, its members, or its counsel, made any monetary contribution to the preparation or submission of this brief.

to privacy, free speech, and freedom of association, including those rights online. (See, e.g., *In re Ricardo P.* (2019) 7 Cal.5th 1113; *Sheehan v. San Francisco 49ers, Ltd.* (2009) 45 Cal.4th 992; *Hill v. Nat. Collegiate Athletic Assn.* (1994) 7 Cal.4th 1; *White v. Davis* (1975) 13 Cal.3d 757; *Carpenter v. U.S.* (2018) 585 U.S. 296; *Riley v. California* (2014) 573 U.S. 373; *Herring v. U.S.* (2009) 555 U.S. 135.)

Dated: February 24, 2025

Respectfully submitted,

Jacob Snow (SBN 270988)
ACLU FOUNDATION OF
NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
jsnow@aclunc.org

Attorney for Amici Curiae

BRIEF OF AMICI CURIAE

INTRODUCTION

Today, people rely on social media platforms, email providers, and online messaging services to connect, communicate, and engage in essential daily activities. The Stored Communications Act (SCA) is a critical part of protecting privacy in the digital age. It generally precludes companies from divulging the content of people's communications to law enforcement unless compelled to do so by a valid search warrant, court order, or other formal legal process.

If upheld, the Court of Appeal's reasoning would upend the SCA's longstanding protections, which are necessary to safeguard people's privacy rights. The statute's protection for the contents of user communications is what prevents the warrantless sharing of people's sensitive, personal correspondence. To continue to protect people's privacy, the decision below should be reversed.

The appellate court erroneously held that user communications stored with Snap and Meta are not protected by the SCA because the platforms are neither electronic communications service (ECS) providers nor remote computing service (RCS) providers. The court held that the platforms are not ECS providers because they do not hold users' communications "in electronic storage." And it held that the platforms are not RCS providers because they do not hold the content for the "sole purpose" of providing storage or processing services. Rather, it held that these companies also use the content to serve targeted advertisements and make money—a surveillance-based business

model that many technology companies providing communications services to the public currently use.

Under the court's ruling, neither the SCA's prohibition on voluntary disclosure (in 18 U.S.C. § 2702) nor the SCA's requirement that law enforcement obtain a warrant to compel disclosure of content (in 18 U.S.C. § 2703) would continue to apply to these social media or Internet communications companies. But today, companies with surveillance-based business models properly demand warrants before granting law enforcement access to customer information based on protections established in the SCA—a practice that the appellate court decision would undermine. And it would upend the intention of Congress in passing the SCA to protect people's privacy in the digital age. It was incorrect for the Court of Appeal to conclude that Congress, despite explicitly intending to protect these communications, wrote a statute that protected almost none of them, and failed to regulate the companies entrusted with our most private communications.

California has some of the strongest privacy laws in the country. But California's supplement to the SCA, the California Electronic Communications Privacy Act (CalECPA), which went into effect in 2016, includes provisions that build on the existing foundation of the SCA. For example, CalECPA allows voluntary disclosure when that disclosure is not otherwise prohibited by state or federal law. (Pen. Code, § 1546.1, subd. (f).) CalECPA cannot, therefore, in this case, protect Californians from the harm of the decision below.

At the same time, this Court need not endorse Petitioners' privacy-invasive business practices to reject the Court of Appeal's theory that the SCA does not apply to companies whose business model is to profit from targeted advertising. Privacy in communications is one aspect of a body of legal protections in California that allow people to live safe and fulfilling lives in a functioning democracy. Petitioners, by compiling detailed profiles of many millions of people and using those profiles to target advertisements, should be scrutinized carefully to ensure that they comply with California's rigorous privacy laws, including Article I, section 1 of the California Constitution and the California Consumer Privacy Act. The necessity of ensuring that Petitioners' intrusive business models comply with the law does not, however, justify the Court of Appeal's flawed interpretation of the SCA.

Finally, we recognize that the SCA, as properly interpreted, can interfere with essential constitutional and due process rights that should provide criminal defendants, such as Mr. Pina, with a means to access information that could aid in their defense. This deprivation urgently needs to be addressed. But it must be addressed without removing protections for hundreds of millions of users of online communications services, such as through legislation or judicial accommodation (e.g. courts requiring prosecutors to obtain warrants for such information). We know that judicial efforts to accommodate defense interests do not always ameliorate the problem, including in Mr. Pina's case. But the reasoning below is not an answer. It would leave vast swaths

of the public's communications exposed to commercial sale, wanton sharing, extensive discovery during civil litigation, and warrantless, suspicionless, unregulated government searches and seizures.

ARGUMENT

I. The appellate court holding is contrary to Congress's intent, precedent, and practice.

A. Congress's intent in passing the Stored Communications Act was to ensure the privacy of electronic communications regardless of whether the Fourth Amendment applies.

Congress passed the SCA to protect people's significant privacy interests in electronic communications. The purpose of the SCA is to provide clear statutory privacy protections to the contents of communications stored with third parties as well as associated communications data, and to buttress constitutional privacy protection under the Fourth Amendment.

The Court of Appeal's decision would thwart the SCA's clear intent by concluding that the statute only protects communications if users have a Fourth Amendment-protected reasonable expectation of privacy in them. (*Snap, Inc. v. Superior Court of San Diego County* (2024) 103 Cal.App.5th 1031, 1049, 1064 ("*Pina*"), review granted Sept. 18, 2024, S286267.) That conclusion is very wrong. Congress's purpose in passing the SCA was to provide clear rules to protect electronic communications from unjustified disclosure independent of and beyond the protection that might be available under the developing interpretation of the federal Constitution.

Prior to the law's enactment, the judiciary committees of both the House of Representatives and the Senate prepared detailed reports concerning the legislation.[2] Both reports explained that the main goal of its passage was to update then-existing law in light of dramatic technological changes and 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 (1986) (hereafter Senate Report) [speaking of protecting both "privacy interests in personal proprietary information" and "the Government's legitimate law enforcement needs"].)

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

---

[2] Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986. (ECPA; Pub.L. No. 99-508 (Oct. 21, 1986) 100 Stat. 1860.) Title II of the law, the SCA, addresses unauthorized access to, and voluntary and compelled disclosure of, people's communications and related information. (18 U.S.C. §§ 2701–2712.)

constitutional privacy protection" absent new legislation. (Senate Report at p. 3; accord, House Report at pp. 16–19, referencing *U.S. v. Miller* (1976) 425 U.S. 435.[3])

These congressional concerns were animated by the holding in *Miller* (referenced in the Senate Report) and the judicial enunciation of the "third-party doctrine," which courts subsequently applied to conclude that individuals do not retain an expectation of privacy in their information held by a third party. The government has used third-party doctrine reasoning to contend that law enforcement does not need to obtain a search warrant under the Fourth Amendment for emails, other electronic content, or associated non-content data.[4]

---

[3] In *Miller*, the U.S. Supreme Court held that people do not have a constitutional expectation of privacy in the records their banks keep about their accounts. This case, in addition to *Smith v. Maryland* (1979) 442 U.S. 735, where the Court found no expectation of privacy in phone company toll records, contributed to the idea of a "third-party doctrine".

[4] Though there is surprisingly little precedent, courts today generally conclude that at least the content of communications, as well as location-revealing data, are protected by the Fourth Amendment despite the third-party doctrine. (*U.S. v. Warshak* (6th Cir. 2010) 631 F.3d 266, 286 [contents of communications); *Carpenter, supra,* 585 U.S. at pp. 319-320 (majority op., Roberts, C. J., joined by Ginsberg, Breyer, Sotomayor, and Kagan, JJ.) [noting that contents of communications are protected, and declining to extend third-party doctrine to cell phone location history]; *id*. at p. 332 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.) [agreeing that contents of communications are protected]; *id*. at pp. 387, 400 (Gorsuch, J., dissenting) [agreeing that contents of communications are protected, and criticizing third-party doctrine].)

Congress passed the SCA to step in and ensure privacy protections by imposing a statutory warrant requirement. In doing so, Congress made clear that people's privacy in the digital age would be protected despite any uncertainty as to whether there is a "reasonable expectation of privacy" protected by the Fourth Amendment.

The Court of Appeal wrongly believed that SCA protection depends on whether users have an expectation of privacy in the stored data. (*Pina, supra,* 103 Cal.App.5th at p. 1064.) The court noted that "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." (See also *Pina* at p. 1049 ["[T]he SCA does not apply to this case because the information sought is not the type of private information to which that law applies."].)

To the contrary, the SCA's purpose is to provide clear privacy protections despite uncertainty about the "expectation of privacy" (and thus constitutional protection). The statute doesn't ask whether the materials are "private." Rather, Congress defined an all-encompassing category of materials (electronic communications), imposed prohibitions on disclosure, and defined exceptions. The constitutional "expectation of privacy" test that the decision below appears to have applied is not relevant. Indeed, the very purpose of the statute is to absolve courts from having to decide difficult constitutional questions in the context of new technology, especially if the analysis leans against the application of Fourth Amendment protection. (*Suzlon Energy Ltd. v. Microsoft Corp.* (9th Cir. 2011) 671 F.3d 726, 730 ["limiting the

ECPA only to those people entitled to Fourth Amendment protection" would "put email service providers in an untenable position."].)

In sum, the Court of Appeal's erroneous decision effectively nullifies the SCA's core privacy protections, which safeguard people's information from voluntary disclosure by companies, and ensure that law enforcement cannot gain access to protected communications by mere warrantless request.

Were the Court of Appeal's ruling to stand, it would allow law enforcement to obtain private communications upon request. Providers, and the people who rely on these services, would have little recourse against persuasion, pressure, or threats from government agents without legal authorization. Further, upending the SCA also undermines the "clear standards" by which law enforcement knows that they can obtain the contents of communications and ensure admissibility. (Senate Report at p. 5.) The SCA's protections and guidance are also important to law enforcement and would be undermined by the decision below.

B. The SCA protects communications even if the provider also uses those materials for its own business purposes.

The statute, relevant precedent, and past practice of treating Internet platforms as covered by the SCA lead to the conclusion that communications stored with Snap and Meta are in "electronic storage" even if the provider also uses those materials for its own business purposes. The Court of Appeal's novel interpretation (*Pina, supra,* 103 Cal.App.5th at p. 1062)

conflicts with the text of the statute and with longstanding precedent.

To protect users' privacy, the SCA prohibits disclosure of the contents of communications and other related information by certain covered service providers. Both Meta and Snap fit under the definition of an ECS provider.[5] 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).) Wire communications include "any aural transfer made in whole or in part through the use of facilities for the transmission of communications . . . . ." (18 U.S.C. § 2510(1).) "Electronic communications" encompasses a comprehensive category of online activity. It includes "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 any wire or oral communication, or a few other types of information not relevant here). (18 U.S.C. § 2510(12).)

Generally, the SCA prohibits ECSs that offer their services to the public from voluntarily divulging the contents of the communications that they hold in "electronic storage" to any person or entity. (18 U.S.C. § 2702.) The statute also provides some exceptions to that general rule, as well as a mechanism for

---

[5] Amici also agree that Petitioners fit the definition of RCS but do not present that analysis here as it is not necessary to resolve this appeal.

law enforcement to obtain those contents. (18 U.S.C. § 2703.) "Electronic storage" is a term of art under the statute and is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and any storage "for purposes of backup protection of such communication." (18 U.S.C. §§ 2510(17)(A)–(B).) Snap and Meta users' messages are in "electronic storage" because those copies were generated and are kept as backups for the user. All federal courts to weigh in on this question have concluded that the SCA's protections apply. In *Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, the subpoenaing party, supported by the Department of Justice, argued that messages it obtained from an Internet service provider's server following their delivery to the intended recipient were not in electronic storage and thus not protected by the SCA. (*Id.* at p. 1075.) The Ninth Circuit rejected this narrow reading, interpreting the plain language of the statute to hold that "backup protection" may refer to material stored on a server even after delivery "to provide a second copy of the message in the event that the user needs to download it again." (*Ibid.*) It follows that, if messages serve a backup function, the statute requires no further inquiry into what other purpose retaining those copies may serve to the provider.

The Ninth Circuit reaffirmed this reasoning in *Quon v. Arch Wireless Operating Co., Inc.* (9th Cir. 2008) 529 F.3d 892, 900–901, *revd. on other grounds* (2010) 560 U.S. 746. In *Quon*, the court assessed whether the text messaging service provided

by Arch Wireless was an ECS or an RCS.[6] The Ninth Circuit held that under the plain language of the statute, the text messaging service was an ECS. The court compared the text messaging service to the email service in *Theofel*, noting that both archived messages for "backup protection." (*Ibid.*) Critically, the court noted that the messages were in electronic storage regardless of whether the archives were for the benefit of the company rather than that of the user. (*Id.* at p. 902 ["Although it is not clear for whom Arch Wireless 'archived' the text messages—presumably for the user *or Arch Wireless itself*—it is clear that the messages were archived for 'backup protection,' just as they were in *Theofel*."] [emphasis added].)

Other courts outside of the Ninth Circuit have similarly held that copies of communications held by service providers are "in electronic storage" even if the providers retain stored content for targeted advertising or reasons other than just access by the account holder. (*In re United States for an Ord. Pursuant to 18 U.S.C. § 2705(b)* (D.D.C. 2018) 289 F.Supp.3d 201, 209–210 ["Airbnb is an ECS provider despite its provision of other services that are not ECS or RCS and regardless of whether its primary business function is the provision of ECS . . . . The provision of such services does not need to be Airbnb's primary business function in order for the ECS portion of its business to be covered

---

[6] The distinction was relevant because the plaintiff was claiming that the contents of his text messages were unlawfully disclosed and the SCA has different rules, not relevant here, as to whom an ECS or RCS may divulge content.

by the SCA."][7]; *Twitter, Inc. v. Garland* (9th Cir. 2023) 61 F.4th 686, 690 [Twitter is an ECS][8]; *Republic of Gambia v. Facebook, Inc.* (D.D.C. 2021) 575 F.Supp.3d 8, 13 [deleted Facebook posts are held for backup purposes and in electronic storage because "Facebook stored a duplicate of these communications, *among other reasons*, in case it was lawfully called upon to produce them by an international body like the United Nations after their removal."].)

Indeed, courts regularly find that Internet platforms are ECS's in possession of communications protected by the SCA without inquiring into their business models. (*In re United States for Prtt Ord. for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841* (D.D.C., Mar. 2, 2018, No. 18-PR-00017) 2018 WL 1358812, at *5; *Suzlon, supra*, 671 F.3d at p. 730 [Hotmail]; *Facebook, Inc. v. Superior Court* (2018) 4 Cal.5th 1245 ("*Hunter*"), 1268 ["Prior decisions have found that Facebook and Twitter qualify as either an ECS or RCS provider and hence are governed by section 2702 of the SCA" (citing cases).].) The analysis in these cases make clear that the appellate court was wrong to conclude that, in order to be in "electronic storage" and

---

[7] Airbnb shares personal information with third parties to do targeted advertising or data analytics. (Airbnb, *Privacy Policy* (Feb. 6, 2025) Help Center <https://www.airbnb.com/help/article/3175#1> [as of Feb. 23, 2025].)

[8] Twitter uses "the contents of the messages" and your related information to provide our advertising and sponsored content services to "help[s] make ads ... more relevant to you" (e.g. targeted advertising).

protected under the SCA, user contents must be stored "***merely*** for backup purposes." (*Pina, supra,* 103 Cal.App.5th at p. 1061 [emphasis added]). There is no textual basis in the statute for that conclusion. Although user communications may be used for other purposes, including advertising, they are still stored as backup on the platforms' servers, regardless of what other purposes storage may serve, and are therefore covered as ECS content by the SCA. (18 U.S.C. § 2510(17); *Theofel*, *supra,* 359 F.3d at p. 1075.)

For the reasons above and in the petitioners' briefing, the SCA cannot be interpreted to exclude Snap and Meta from its protections based solely on their advertising business models. Simply put, there is no "targeted advertising business model" exception in the SCA's text. And petitioners are correct that finding such an exception would "leave unprotected huge swaths of modern electronic communications." (Meta Reply at p. 17.) If the Fourth District's opinion were correct, it would enable Internet service providers to subvert their responsibilities to user privacy under the SCA simply by drafting their terms of service to include a provider right of access for economic exploitation of user communications. Such an outcome defies existing precedent, common sense, and the SCA's purpose.

The Court of Appeal's decision therefore must be reversed.

II. CalECPA does not adequately protect Californians if the Court of Appeal's decision is allowed to stand.

Both the Court of Appeal's opinion and Chief Justice Cantil-Sakauye's concurrence in *Touchstone* recognized that the

California Electronic Communications Privacy Act (CalECPA) provides protection when electronic information is sought by law enforcement. (*Facebook, Inc. v. Superior Court of San Diego County* (2020) 10 Cal.5th 329 ("*Touchstone*"), 355, fn. 13 [noting that CalECPA generally requires a warrant or comparable instrument to acquire such communications and precludes use of a subpoena for the purpose of investigating or prosecuting a criminal offense] (citations omitted); *Pina, supra,* 103 Cal.App.5th at p. 1066.) These protections are vital, especially when federal privacy protections, whether constitutional or statutory, are imperiled or uncertain.

However, CalECPA will not be able to continue to provide all of the privacy protections that the legislature intended if the Court of Appeal's decision is allowed to stand. Some of CalECPA's provisions are crafted as a supplement to the existing foundation of the federal SCA. For example, CalECPA allows voluntary disclosure "when that disclosure is not otherwise prohibited by state or federal law." (Pen. Code, § 1546.1, subd. (f).) This means that, if the federal SCA no longer prohibits a service provider from voluntarily disclosing user communications, then CalECPA also does not offer that protection.

So while it is true that CalECPA offers strong protections against compelled access to people's communications by government entities, it cannot stop the privacy harms that will result from the Court of Appeal's decision. This is another reason why that reasoning should be rejected.

III. To the extent this Court is concerned about social media's business models' negative impact on users' privacy, California law provides meaningful protections to guard against privacy-invasive business practices.

Snap and Meta's surveillance business practices exact significant privacy costs on Californians. Both companies collect vast amounts of information about people who use their services and use that personal information for profit—to sell advertising space in front of those users, claiming (to advertisers) that the advertisements will be more effective as a result. These practices have been the subject of—to put it mildly—significant public concern (some of which amici discuss below).

Holding that the SCA's protections apply here does not mean that these companies' business practices would escape all legal scrutiny. In fact, California law has long provided the public with legal means to ensure that they exercise control over their personal information—most notably, through the landmark constitutional right to privacy enacted in 1972. And, as technology companies pursue ever more sophisticated means of surveillance, California law offers other mechanisms—including the passage in 2018 of California Consumer Privacy Act (CCPA). To the extent that this Court is concerned that reversal in this case will be perceived as blessing the petitioners' problematic business models, it can take the opportunity in its decision to highlight the importance of California privacy protections and the legal means that must be available to Californians to safeguard their fundamental right to privacy.

A. Californians are guaranteed a robust constitutional right to privacy against private actors under Article I, section 1 of the California Constitution.

Californians are guaranteed an inalienable constitutional right to privacy and this robust right should protect people from harms of surveillance-based business models that are powered by information collection, use, and disclosure. The California constitutional right to privacy was passed by the legislature and the voters in 1972. Society was on the cusp of computerization and many Californians who were engaged in important social movements had developed a very personal understanding about how the government and private actors could take advantage of new technology to weaponize information about their lives to harm them.[9]

The California constitutional right to privacy is a modern right to privacy, with its "moving force" a focused privacy concern "relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society." (*White, supra,* 13 Cal.3d at p. 774.) Its purpose was to address the lack of "effective restraints on the information activities of government and business" and create "a legal and enforceable right of privacy for every

---

[9] (See generally Ozer, *Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age* (2024) 39 Berkeley Tech. L.J. 963 <https://btlj.org/wp-content/uploads/2025/01/39-2_Ozer.pdf> [as of Feb. 23, 2025].)

Californian." (*Ibid.* [citing ballot language] (Italics omitted).) The constitutional privacy right protects against intrusion by both government and private actors. (See *Hill*, *supra*, 7 Cal.4th at p. 20 ["In summary, the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities."].)

A foundational aspect of the right to privacy is the right to control what personal information is collected and how it is used. In fact, the voter guide for the constitutional amendment explained that the right to privacy was targeted at addressing four "principal mischiefs," including "the overbroad collection and retention of unnecessary personal information by government and business interests," and "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party." (*White*, *supra,* 13 Cal.3d at p. 775 [citing ballot argument].) Controlling the use of personal information, as well as its collection or disclosure, is a cornerstone of privacy protections that has been present in California law for over half a century.

This protection is only more vital today, as the ways in which private parties use people's personal information have expanded, from ubiquitous behavioral advertising to other algorithmic systems, including artificial intelligence. For example, the collection, sharing, and use of personal information

can cause people to be incarcerated,[10] to suffer bodily injury,[11] to lose their homes[12] or their jobs,[13] and to be blocked from accessing new opportunities[14] and credit.[15] The use of people's personal information for behavioral advertising specifically can

---

[10] (Heaven, *Predictive policing algorithms are racist. They need to be dismantled* (July 17, 2020) MIT Technology Review <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/> [as of Feb. 23, 2025].)

[11] (Evans, *Amazon's Warehouse Quotas Have Been Injuring Workers for Years. Now, Officials Are Taking Action* (May 16, 2022) Reveal News <https://revealnews.org/article/amazons-warehouse-quotas-have-been-injuring-workers-for-years-now-officials-are-taking-action/> [as of Feb. 23, 2025].)

[12] (Fry, *Landlords Are Using AI to Raise Rents—and Cities Are Starting to Push Back* (Dec. 7, 2024) Gizmodo <https://gizmodo.com/landlords-are-using-ai-to-raise-rents-and-cities-are-starting-to-push-back-2000535519> [as of Feb. 23, 2025].)

[13] (De Chant, *Amazon is using algorithms with little human intervention to fire Flex workers* (June 28, 2021) ArsTechnica <https://arstechnica.com/tech-policy/2021/06/amazon-is-firing-flex-workers-using-algorithms-with-little-human-intervention/> [as of Feb. 23, 2025].)

[14] (Akselrod & Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired* (Aug. 3, 2023) ACLU: News & Commentary <https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired> [as of Feb. 23, 2025].)

[15] (Andrews, *How Flawed Data Aggravates Inequality in Credit* (Aug. 6, 2021) Stanford University Human Centered Artificial Intelligence <https://hai.stanford.edu/news/how-flawed-data-aggravates-inequality-credit> [as of Feb. 23, 2025].)

expose people to hacking,[16] scams,[17] and higher prices and lower quality goods.[18] People report that behavioral advertisements feel creepy and invasive, and research indicates that advertisements can cause a variety of other harms.[19]

Cases assessing the legality of surveillance business models and privacy-invasive practices are making their way through the

---

[16] (Germain, *The FBI Says You Need to Use an Ad Blocker* (Dec. 22, 2022) Gizmodo <https://gizmodo.com/google-bing-fbi-ad-blocker-scam-ads-1849923478> [as of Feb. 23, 2025].)

[17] (Silverman & Mac, *Facebook Profits As Users Are Ripped Off By Scam Ads* (Dec. 10, 2020) BuzzFeed News <https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam> [as of Feb. 23, 2025]; Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic* (Dec. 18, 2020) Time Magazine <https://time.com/5921820/facebook-shopping-scams-holidays-covid-19> [as of Feb. 23, 2025]; Koebler, *Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons* (Aug. 23, 2023) 404 Media <https://www.404media.co/instagram-ads-illegal-content-drugs-guns-hackers/> [as of Feb. 23, 2025].)

[18] (Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why* (Apr. 6, 2023) N.Y. Times <https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html> [as of Feb. 23, 2025] (summarizing Schnadower-Mustri, Adjerid, & Acquisti, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation* (Mar. 23, 2023) SSRN <https://ssrn.com/abstract=4398428> [as of Feb. 23, 2025]).)

[19] (Wu et al., *The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People* (June 12, 2023) 2023 ACM Conference on Fairness, Accountability, and Transparency <https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594119> [as of Feb. 23, 2025].)

courts.[20] In an appropriate case, this Court should take up the question of when collecting reams of personal information and using it to serve targeted advertisements could violate California law, including Article I, section 1 of the California Constitution. But the Court should not undermine important electronic surveillance privacy protections under federal law out of concern that appellants' business models are inadequately protective of their users' privacy.

B. The California Consumer Privacy Act also includes protections against use of information for targeted advertising.

California statutory law also limits how people's personal information can be used for targeted advertising. This California statutory law holds some promise of reining in the worst abuses of people's privacy by business. The California Consumer Privacy Act (CCPA), for example, was passed through the legislature and signed by Governor Jerry Brown in 2018, and then revised through a ballot initiative in November 2020. The law adds explicit transparency and control rights to California privacy law,

---

[20] (See, e.g., *Renderos v. Clearview AI, Inc.* (A167179, app. pending) [case challenging facial recognition company Clearview AI's surveillance activities in California]; *Calhoun v. Google, LLC* (9th Cir. 2024) 113 F.4th 1141 [case challenging a web browser's surreptitious collection of user's personal information under, among other claims, Cal. Const., art. I, § 1]; *Brooks v. Thomson Reuters Corp.* (N.D. Cal., Aug. 16, 2021, No. 21-CV-01418-EMC) 2021 WL 3621837, at *8–9 [denying motion to dismiss Cal. Const., art. I, § 1 claim challenging compilation and sale of "cradle-to-grave dossiers"].)

building on the constitutional foundation of Article I, section 1. (See Ballot Pamp., Gen. Elec. (Nov. 3, 2020) text of Prop. 24, p. 42 et seq., at <https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf> [as of Feb. 23, 2025] [referencing Cal. Const., art. I, § 1 and other then-existing California privacy protections].)

Under the CCPA, businesses must give people notice when their personal information is collected and provide a copy of any personal information held about them upon request. (Civ. Code, §§ 1798.100, subd. (a) [notice when personal information is collected]; 1798.110, subd. (a) [right to access information held by a business].) People have the right to opt out of the sale of personal information, which allows them to refuse to allow businesses to use certain personal information to target advertisements. (Civ. Code, § 1798.120, subd. (a).)

The CCPA also created a new agency, the California Privacy Protection Agency (CPPA), responsible for enforcing the CCPA and adopting regulations on specified topics. (Civ. Code, §§ 1798.199.10, subd. (a) [establishing the agency], 1798.199.40, subd. (a) [enforcement authority], 1798.199.40, subd. (b) [regulatory authority].) Among the topics that the agency is empowered to regulate include the use by businesses of "automated decision-making technology," which includes (among other technologies) "profiling." (Civ. Code, § 1798.185, subd. (a)(15).) Regulations currently proposed[21] by the CPPA include

---

[21] (Cal. Reg. Notice Register 2024, No. 47-Z, p. 1494 et seq., at <https://oal.ca.gov/wp-content/uploads/sites/166/2024/11/2024-

behavioral advertising as one of many examples of automated decision-making technologies and provide consumers with particularly strong rights given the multitude of risks associated with surveillance-based advertising.[22]

Like the California constitutional right to privacy, the CCPA and its enabling regulations reflect that the democratic process in California—through the legislature, regulatory agencies, and cases that could make their way to this Court—offers some promise that the privacy-invasive surveillance business models of today can be addressed.

For these reasons, overturning the Court of Appeal's reasoning and continuing to safeguard privacy rights pursuant to the SCA is important for people's rights and safety. And it is consistent with California's longstanding commitment to robustly protect privacy via both Constitution and statute.

Notice-Register-No.-47-Z-November-22-2024.pdf> [as of Feb. 23, 2025].)

[22] (See Cal. Privacy Protection Agency, Proposed Text of Regulations for Cal. Reg. Notice Register 2024, No. 47-Z, (Oct. 2024) at Section 7221(b)(6) [providing an opt-out right for behavioral advertising in "all circumstances"]), at <https://cppa.ca.gov/meetings/materials/20241004_item3_draft_text.pdf> [as of Feb. 23, 2025]; and Initial Statement of Reasons (Nov. 22, 2024) at p. 62 [stating, while offering additional examples, that "[t]here also is a significant risk of discrimination when using ADMT for profiling for behavioral advertising."], at <https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_add_ins_isor.pdf> [as of Feb. 23, 2025].

CONCLUSION

For the foregoing reasons, amici respectfully urge this Court to reverse the decision below. At another point, this Court may wish to decide whether due process and other constitutional rights afford criminal defendants, such as Mr. Pina, with a means to access information that could aid in their defense.

Dated: February 24, 2025

Respectfully submitted,

Jacob Snow (SBN 270988)
jsnow@aclunc.org
Nicole A. Ozer (SBN 228643)
nozer@aclunc.org
ACLU FOUNDATION OF
NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493

Jennifer Granick (SBN 168423)
jgranick@aclu.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
425 California Street,
Seventh Floor
San Francisco, CA 94110
Telephone: (415) 343-0758

Attorneys for Amici Curiae

CERTIFICATE OF WORD COUNT

Pursuant to California Rules of Court, rule 8.520(c)(1), and in reliance on the word count of the computer program used to prepare this Proposed Brief of *Amici Curiae*, counsel certifies that the text of this brief (including footnotes) was produced using 13-point type and contains 4,646 words. This includes footnotes but excludes the tables required under rule 8.204(a)(1), the cover information required under rule 8.204(b)(10), the Certificate of Interested Entities or Persons required under rule 8.208, the Application to File *Amici Curiae* Brief required under rule 8.520(f), this certificate, and the signature blocks. See rule 8.204(c)(3).

Dated: February 24, 2025

Respectfully submitted,

Jacob Snow (SBN 270988)
ACLU FOUNDATION OF
NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
jsnow@aclunc.org

Attorney for Amici Curiae

PROOF OF SERVICE

I, Samantha May, declare that I am over the age of eighteen and not a party to the above action. My business address is 39 Drumm Street, San Francisco, CA 94111. My electronic service address is smay@aclunc.org. On February 24, 2025, I served the attached,

APPLICATION FOR LEAVE TO FILE AMICI CURIAE BRIEF
AND
PROPOSED BRIEF OF AMICI CURIAE ACLU OF NORTHERN CALIFORNIA AND ACLU IN SUPPORT OF PETITIONERS

BY E-MAIL OR ELECTRONIC TRANSMISSION: I caused to be transmitted to the following case participants a true electronic copy of the document via this Court's TrueFiling system:

San Diego District Attorney's Office, Hall of Justice
Summer Stephan
Karl Husoe
Linh Lam
330 W. Broadway, Ste 860
San Diego, CA 92101
Summer.Stephan@sdcda.org
Karl.Husoe@sdcda.org
Linh.Lam@sdcda.org

San Diego District Attorney's Office, North County Division
David Jarman
325 S. Melrose Drive, Ste 5000
Vista, CA 92081
David.Jarman@sdcda.org

Counsel for Real Party in Interest, The People

(continued on next page)

Munger, Tolles & Olson LLP
L. Ashley Aull
350 S. Grand Avenue, 50th Floor
Los Angeles, CA 90071-3426
Ashley.Aull@mto.com

J. Max Rosen
552 14th Street
San Francisco, CA 94103
Max.Rosen@mto.com

Fenwick & West LLP
David W. Feder
902 Broadway, 18th Floor
New York, NY 10010
DFeder@fenwick.com

Tyler Griffin Newby
Ryan Kwock
555 California Street, 12th Floor
San Francisco, CA 94104
TNewby@fenwick.com
RKwock@fenwick.com

San Diego Office of the Primary Public Defender
Nadine Valdecini
Troy A. Britt
451 A Street, Ste 900
San Diego, CA 92101
Nadine.Valdecini@sdcounty.ca.gov
Troy.Britt@sdcounty.ca.gov

Counsel for Real Party in Interest, Adrian Pina

Perkins Coie LLP
Julie Schwartz
Ryan Mrazik
John R. Tyler
1201 Third Avenue, Ste 4900
Seattle, WA 98101
JSchwartz@perkinscoie.com
RMrazik@perkinscoie.com
RTyler@perkinscoie.com

Natasha Amlani
1888 Century Park E., Ste 1700
Los Angeles, CA 90067
NAmlani@perkinscoie.com

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

Michael J. Holecek
333 S. Grand Avenue
Los Angeles, CA 90071
MHolecek@gibsondunn.com

(continued on next page)

Janie Yoo Miller
Esther D. Galan
730 Arizona Avenue, #1
Santa Monica, CA 90401
JMiller@fenwick.com
EGalan@fenwick.com

Complex Appellate Litigation Group LLP
Brian Adair Sutherland
Gregory Edwin Wolff
96 Jessie Street
San Francsico, CA 94105
Brian.Sutherland@calg.com
Gregg.Wolff@calg.com

Law Office of Orin S. Kerr
Orin S. Kerr
Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305
Orin@orinkerr.com

Counsel for Petitioner, Snap, Inc.

Natalie J. Hausknecht
1801 California Street, Ste 4200
Denver, CO 80202
NHausknecht@gibsondunn.com

Counsel for Petitioner,
Meta Platforms, Inc.

BY MAIL: I mailed a copy of the document identified above by depositing the sealed envelope with the U.S. Postal Service, with the postage fully prepaid.

Clerk of the Superior Court
For: Hon. Daniel F. Link
San Diego County Superior Court
North County Division
325 South Melrose Drive
Department 21
Vista, CA 92081

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

Executed on February 24, 2025 in San Francisco, CA.

Samantha May, Declarant