August 22, 2024

Chief Justice Patricia Guerrero and Associate Justices
Supreme Court of California
350 McAllister Street
San Francisco, CA 94102

Re: *Snap, Inc. v. The Superior Court of San Diego County; Adrian Pina et al.*, Case No. S286267, Letter of Amici Curiae Electronic Frontier Foundation and Center for Democracy & Technology in Support of Petition for Review

To the Honorable Chief Justice Patricia Guerrero and Associate Justices of the Court,

Amici Electronic Frontier Foundation (EFF) and Center for Democracy & Technology submit this letter in support of Petitioners in *Snap, Inc. v. The Superior Court of San Diego County* and respectfully urge the Court to grant review in this matter. Amici submit that, for the reasons discussed herein, review is necessary "to settle an important question of law." (Cal. Rules of Court, rule 8.500(b)(1).) Specifically, this Court should grant review in order to reverse the Court of Appeal's opinion in this case, which misinterprets the federal Stored Communications Act and significantly undermines the privacy of internet users.

IDENTITY AND INTEREST OF AMICI

EFF is a member-supported, non-profit civil liberties organization that has worked to protect and promote fundamental liberties in the digital world for more than thirty years. With over 30,000 active donors, including donors in California, EFF encourages and challenges industry, government, and courts to support privacy, civil liberties, free expression, and transparency in the information society. EFF regularly participates as amicus or counsel in cases involving the intersection of privacy and technology. EFF has litigated extensively in this court. (See, e.g., *A.C.L.U. Found. v. Superior Ct.* (2017) 3

Cal.5th 1032 (counsel); *In re Ricardo P.* (2019) 7 Cal.5th 1113, *as modified* (Aug. 28, 2019) (amicus); *People v. Buza* (2018) 4 Cal.5th 658 (amicus).) And it has submitted amicus briefs regarding the proper interpretation of the Stored Communications Act. (See, e.g., *Hately v Watts*, (4th Cir. May 29, 2018), 2018 WL 2725646, Brief of Amicus Curiae.)

The Center for Democracy & Technology is a public interest organization that for over twenty-five years, has represented the public's interest in an open, decentralized Internet and worked to ensure that the constitutional and democratic values of privacy and free expression are protected in the digial age. CDT was the founder of the Digital Due Process Coalition, which brought together over 100 civil society groups, tech and telecom companies and their trade associations, and academics to reform the Electronic Communications Privacy Act.

ARGUMENT

The Stored Communications Act (SCA) protects the privacy rights of hundreds of millions of people who use certain online communications and storage services. (18 U.S.C. 2701 *et seq*.) The lower court's opinion damages the privacy rights of those users.

In a break with nearly 40 years of precedent, the lower court found that the SCA largely does not protect the users of services offered by Meta, Snap, and many similar companies because those companies choose to access the content of user communications for their own business purposes, including for online behavioral advertising. The online behavioral advertising business model poses problems that EFF and CDT have sought to change with user tools, advocacy, and legislation.[1] But rather than solve the very real problem of corporate surveillance, the lower court's opinion will perversely strip away some of the few statutory privacy protections that U.S. users have on the internet.

The decision is wrong because it conflicts with the statute's purpose of protecting the privacy of user communications from disclosure, it incorrectly elevates private contracts of adhesion over statutory text, and it ignores decades of interpretation by courts and Congress.

---

[1] EFF, *Privacy First: A Better Way to Address Online Harms*, https://www.eff.org/wp/privacy-first-better-way-address-online-harms. EFF, *Privacy Badger*, https://privacybadger.org. CDT, *Future of Online Advertising Project*, https://cdt.org/online-advertising/.

The legal question here is simple. Under the SCA, providers like Meta and Snap are electronic communication services, and users' private messages are stored, in part, for the purposes of backup protection. The SCA, therefore, restricts the disclosure of those communications pursuant to the subpoenas at issue in this case.

I. The Lower Court's Decision Would Severely Limit One of the Few Federal Online Privacy Laws

A. The Ruling Thwarts the SCA's Privacy Purpose

The 1986 Stored Communications Act protects the privacy of users' communications, encourages adoption and innovation of communications services, and creates procedures for law enforcement access. (S. REP. 99-541, 5, 1986.) The law is built on the principle that users have a reasonable expectation of privacy that providers will not *disclose* users' communications to third parties, even though providers have *access* to those communications as they are stored on those services. (*Id.* at 3. See also Report of the Privacy Protection Study Commission, *Personal Privacy in an Information Society*, 362-63 (1977).) It protects people who use electronic communication services (ECS) and remote computing services (RCS).

Under the lower court's opinion, however, the SCA's disclosure protections would be rendered essentially meaningless, because almost no provider—existing in the modern world or in 1986—would meet the requirements.[2] If the decision is allowed to stand, Meta, Snap, and other providers would be allowed to voluntarily disclose the content of their users' communications to any other corporations for any reason, to parties in civil litigation, and to the government without a warrant.

Under the Fourth Amendment, law enforcement would still need a warrant to compel providers to disclose their users' communications, (*United States v. Warshak*, (6th Cir. 2010) 631 F.3d 266), but the court's flawed reasoning could have the effect of weakening the foundation of that protection as well.

[2] End-to-end encrypted messaging apps like Signal would be some of the few that remain covered by the SCA because they cannot physically access their users' communications. However, the SCA was meant to set up legal barriers to disclosure, even when services choose not to set up technical barriers. (S. REP. 99-541, 5, 1986 ["Privacy cannot be left to depend solely on physical protection[.]"].)

B. The Ruling Stakes Too Much on Corporate Terms of Service

The lower court's opinion wrongly elevates corporate terms of service into statutory interpretation, a move that is consistently rejected in similar contexts. The opinion boils down to a reading of providers' terms of service and a conclusion that if users allow companies "to use their content for other purposes, they do not have the expectation of privacy contemplated by the SCA." (*Snap, Inc. v. Superior Ct. of San Diego Cnty.*, (Cal. Ct. App. July 23, 2024) No. D083446, 2024 WL 3507024, at *18.)

This line of reasoning has been rejected in constitutional and statutory analysis. In the Fourth Amendment context, a provider's "right of access" reserved through terms of service does not diminish a user's right to protect against disclosure. (*Warshak, supra*, 631 F.3d at 287.) Privacy protections are not set by the "crazy quilt" of corporate policies and billing practices, (*Smith v. Maryland*, (1979) 442 U.S. 735, 745), nor by terms that allocate risk "between private parties." (*Byrd v. United States*, (2018) 584 U.S. 395, 408). Not to mention the fact that users do not—and likely could not—read all the terms the govern the online tools needed to function in modern society.[3]

Similarly, in interpreting the separate Computer Fraud and Abuse Act (CFAA), the Supreme Court has also cautioned that courts cannot stake so much of a law's interpretation on the "drafting practices of private parties." (*Van Buren v. United States*, (2021) 593 U.S. 374, 396.)

C. The Ruling Conflicts with 40 Years of Interpretation By Courts and Congress

No court since the SCA passed in 1986 has ever ruled that a provider's business model of accessing user communications for its own purposes removes Stored Communications Act protection for users. That is despite courts and Congress being fully aware of service providers' own access to the content of communications.

Before the SCA was passed, courts acknowledged that telephone service providers sometimes access user communications for reasons separate from offering the service to users, while still protecting those communications from disclosure. (*Bubis v. United States*, (9th Cir. 1967) 384 F.2d 643, 648). Congress's own study in 1985 found that providers regularly retain copies of user messages for their own "administrative

[3] Solove, Daniel J., *Murky Consent: An Approach to the Fictions of Consent in Privacy Law* (August 20, 2023). 104 Boston University Law Review 593, 614-621 (2024), https://ssrn.com/abstract=4333743.

purposes"—a reason to protect those copies through statute.[4] And more recently, the Fourth Circuit dismissed the idea that a company's targeted advertising business model would affect the SCA disclosure analysis. (*Hately v. Watts*, (4th Cir. 2019) 917 F.3d 770, 795 [taking as given that Google accesses copies of emails "for their own commercial purposes"]).

Congress has recently agreed that the Stored Communications Act's disclosure provisions govern modern-day companies. Fully aware of the business model of modern service providers, Congress in 2018 amended the SCA to ensure Microsoft, in particular, and other providers with control over user data stored outside the U.S. complied with compelled disclosure provisions of the SCA. (Pub. L. 115–141. See also *United States v. Microsoft Corp.*, (2018) 584 U.S. 236 [describing circumstances of CLOUD Act passage].) Like other modern service providers, Microsoft's privacy policy at the time read that it used customer data to "improve our products and personalize your experiences."[5] Similarly, Congress in 2016 engaged extensively with Google and other modern providers before nearly passing a separate overhaul of the SCA.[6] That debate happened during a time when Google engaged in the maligned practice of scanning the contents of users' emails to serve targeted ads.[7]

If members of Congress concluded that Microsoft, Google, and other modern day service providers like Snap and Meta did not fall under disclosure restrictions of the SCA because of their business model of accessing communication content, much of the debate and changes to the SCA during that period would have been meaningless.

---

[4] Federal Government Information Technology, Electronic Surveillance and Civil Liberties, U.S. Congress, Office of Technology Assessment, 46 (Oct. 1985), https://ota.fas.org/reports/8509.pdf.

[5] Microsoft Privacy Statement (Last Updated Feb. 2018), https://web.archive.org/web/20180323081421/https://privacy.microsoft.com/en-US/privacystatement.

[6] Mario Trujillo, *House Unanimously Passes Email Privacy Bill*, The Hill, April 27, 2016), https://thehill.com/policy/technology/277897-house-unanimously-passes-bill-to-protect-email-privacy/.

[7] Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, The New York Times (June 23, 2017), https://www.nytimes.com/2017/06/23/technology/gmail-ads.html.

II. Meta and Snap Are Electronic Communication Services Covered By the SCA's Disclosure Restrictions

There is a straightforward answer to the lower court's error. Meta and Snap are electronic communication services for the purposes of this case, and users' private messages are stored in part for the purposes of backup protection for the user. (18 U.S.C. 2702(a)(1), 18 U.S.C. 2510(17). See *Hately, supra*, 917 F.3d at 795 [defining backup protection]; *Theofel v. Farey-Jones*, (9th Cir. 2004) 359 F.3d 1066, 1075 [same]; *Republic of Gambia v. Facebook, Inc.*, (D.D.C. 2021) 575 F. Supp. 3d 8, 13 [same].)

An electronic communication can be in electronic storage for dual purposes. (Compare 18 U.S.C. 2510(17) ["for purposes of backup protection"] with 18 U.S.C. 2702(a)(2)(B) ["solely for the purpose of providing storage or computer processing services"].) The statutory text does not strip away privacy protections that prevent the disclosure of user communications merely because providers may bury in their terms of service that they can also use backed-up communications for their own internal purposes. (*Hately*, 917 F.3d at 795 [disregarding fact that many providers also store communications "for their own commercial purposes"].)

Respectfully Submitted,

By: */s/ F. Mario Trujillo*
F. Mario Trujillo (SBN: 352020)
Andrew Crocker (SBN: 291596)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
mario@eff.org
andrew@eff.org

/s/ Kevin Stuart Bankston
Kevin Stuart Bankston (SBN: 217026)
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 20005
(202) 637-9800
kbankston@cdt.org

PROOF OF SERVICE

I am over the age of 18 years and not a party to the within action. I am employed in the County of San Francisco, State of California. My business address is 815 Eddy Street, San Francisco, California 94109.

On August 22, 2024, I served the foregoing document:

☒ **BY ELECTRONIC SERVICE VIA TRUEFILING**. I caused the foregoing to be electronically filed with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website:

Tyler Griffin Newby
Fenwick & West LLP
555 California Street, 12th Floor
San Francisco, CA 94104

Janie Yoo Miller
Esther D. Galan
Fenwick & West LLP
730 Arizona Avenue, 1st Floor
Santa Monica, CA 90401

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

Orin S. Kerr
Law Office of Orin S. Kerr
334 Law Building
Berkeley, CA 94720-7200

Attorneys for Petitioner Snap, Inc.

Julie Erin Schwartz
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101

Michael Constantine Bleicher
Perkins Coie LLP
700 13th Street NW
Ste 700
Washington, DC 20005-6619

Natasha S. Amlani
Ryan T. Mrazik
Perkins Coie
1882 Century Park East, Suite 1700
Los Angeles, CA 90067

Joshua Seth Lipshutz
Gibson, Dunn & Cructcher LLP
One Embarcadero Center, #2600
San Francisco, CA 94111

Attorneys for Petitioner Meta Platforms, Inc.

Nadine Jeannette Valdecini-Arnold
San Diego Primary Public Defender
451 A Street, Suite 900
San Diego, CA 92101

Troy Anthony Britt
Office of the Primary Public Defender
450 B Street, Suite 1100
San Diego, CA 92101

Attorneys for Adrian Pina, Real Party in Interest

Karl Kristian Husoe
San Diego District Attorney
330 West Broadway, Suite 860
San Diego, CA 92101-3827

David Lee Jarman
San Diego County District Attorney
330 West Broadway
San Diego, CA 92101

Attorneys for the People, Real Party in Interest

Clerk of the Court
FOURTH DISTRICT COURT OF APPEAL, DIVISION ONE
750 B Street, Suite 300
San Diego, CA 92101

☒ **BY FIRST CLASS MAIL**. I placed the foregoing document in a sealed and postpaid envelope addressed as indicated below for collection and mailing following our ordinary business practices. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service:

Clerk of the Superior Court
San Diego County
For: Hon. Daniel F. Link
North County
325 S. Melrose
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 August 22, 2024 at Los Angeles, California.

Victoria Python