Case No. S286267

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

SNAP INC.

Petitioner,

v.

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

Respondent,

ADRIAN PINA, et al.,
Real Parties in Interest

META PLATFORMS, INC.

Petitioner,

v.

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

Respondent,

ADRIAN PINA, et al.,
Real Parties in Interest

After a Decision by the Court of Appeal,
Fourth Appellate District, Division One, Case Nos. D083446 and D083475
San Diego Superior Court, Case Nos. SCN429787
(Honorable Daniel F. Link)

AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND MOZILLA CORPORATION IN SUPPORT OF SNAP AND META

F. MARIO TRUJILLO (SBN 352020)
mario@eff.org
ANDREW CROCKER (SBN 291596)
andrew@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Document received by the CA Supreme Court.

TABLE OF CONTENTS

IDENTITY AND INTEREST OF AMICI 6

INTRODUCTION 7

ARGUMENT 8

I. The Plain Text of the SCA Prohibits Meta and Snap from Disclosing the Contents of Communications Sought in this Case. 8

II. The Purpose and History of the SCA Confirm Meta and Snap Are Prohibited from Disclosing the Contents of Communications Sought in this Case. 9

A. The Lower Court's Ruling Thwarts the Broad Privacy Protections of the SCA. 9

B. The Lower Court's Ruling Undermines Congressional Intent Through the Court's Reliance on Corporate Policies. 12

C. The Lower Court's Ruling Conflicts with 40 Years of Interpretation by Courts, Congress, and Federal Prosecutors. 13

D. The Lower Court's Ruling Will Not Curb Online Behavioral Advertising. 16

CONCLUSION 17

CERTIFICATE OF WORD COUNT 18

CERTIFICATE OF SERVICE 19

SERVICE LIST 20

Document received by the CA Supreme Court.

TABLE OF AUTHORITIES

Cases

Byrd v. United States,
584 U.S. 395 (2018) 13

Calhoun v. Google, LLC,
113 F.4th 1141 (9th Cir. 2024) 13

Hately v. Watts,
917 F.3d 770 (4th Cir. 2019) 8, 14

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

Smith v. Maryland,
442 U.S. 735 (1979) 13

Snap, Inc. v. Superior Ct. of San Diego Cty.,
103 Cal. App. 5th 1031 (2024) 10, 12, 13

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004) 8

United States v. Microsoft Corp.,
584 U.S. 236 (2018) 14

United States v. Smith,
110 F.4th 817 (5th Cir. 2024) 13

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 12, 13

Van Buren v. United States,
593 U.S. 374 (2021) 13

Statutes

18 U.S.C. § 2258 8

18 U.S.C. § 2510 8

18 U.S.C. § 2511 ..... 8, 9

18 U.S.C. § 2701 ..... *passim*

18 U.S.C. § 2702 8

18 U.S.C. § 2703 9

Document received by the CA Supreme Court.

Legislative History

S. REP. 99-541, 1986 ..... 9, 10

SCA. Pub. L. 115–141 14

Other Authorities

Aaron S Edlin et al., *The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google*, 15 Yale J. L. & Tech. 169 (2013). 11

CDT, *Future of Online Advertising Project* 17

Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, The New York Times (June 23, 2017) 15

Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. Law Review 593 (2024) 13

Data Broker Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, 2018-2028 (Nov. 2023) 11

DOJ Crim. Div., *Remarks of Deputy Assistant Attorney General Richard W. Downing At the International Symposium on Cybercrime Response*, U.S. Dep't Justice, (Sep. 13, 2023) 15

EFF, Privacy Badger 17

EFF, *Privacy First: A Better Way to Address Online Harms* 17

Federal Government Information Technology, Electronic Surveillance and Civil Liberties, U.S. Congress, Office of Technology Assessment (Oct. 1985) 14

FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019) 11

Jenn Taylor Hodges, *Work Gets Underway on a New Federal Privacy Proposal*, Mozilla (Apr. 26, 2024) 17

Kerr, Orin S., *Terms of Service and Fourth Amendment Rights* U. Penn. L. Rev. 287 (2024) 12

Mario Trujillo, *House Unanimously Passes Email Privacy Bill*, The Hill (Apr. 27, 2016) 15

Matthew Guariglia, *Fourth Amendment is Not For Sale Act Passed the House, Now it Should Pass the Senate*, EFF (April 18, 2024) 12

Document received by the CA Supreme Court.

Microsoft Privacy Statement (Last Updated Feb. 2018) 14

Pew Research Center, *Americans' attitudes and experiences with privacy policies and laws* (Nov. 15, 2019) 11

Report of the Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) 9

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual, DOJ, Computer Crime and Intellectual Property Section (2009) 15

Speech, DOJ, *Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the 5th German-American Data Protection Day on "What the U.S. Cloud Act Does and Does Not Do"* (May 16, 2019) 15

Document received by the CA Supreme Court.

IDENTITY AND INTEREST OF AMICI

The Electronic Frontier Foundation (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 35,000 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.*, 3 Cal.5th 1032 (2017) (counsel); *In re Ricardo P.*, 7 Cal.5th 1113 (2019), as modified (Aug. 28, 2019) (amicus); *People v. Buza*, 4 Cal.5th 658 (2018) (amicus). And it has submitted amicus briefs regarding the proper interpretation of the Stored Communications Act. *See, e.g., Hately v Watts*, 2018 WL 2725646, Brief of Amicus Curiae (4th Cir. May 29, 2018).

The Center for Democracy & Technology (CDT) is a public interest organization that for over thirty 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 digital 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 Stored Communications Act.

Mozilla Corporation is a global, mission-driven organization that creates open source products like its web browser Firefox. It is guided by the Mozilla Manifesto, a set of principles that recognizes that individuals' security and privacy on the Internet are fundamental. Mozilla promotes user privacy through user education, legislative advocacy, and software tools.

Document received by the CA Supreme Court.

INTRODUCTION

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 threatens the 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. Online behavioral advertising creates a range of privacy and other harms that EFF and CDT have sought to change with user tools, advocacy, and legislation. 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 contradicts the plain text of the SCA, 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.

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.

Document received by the CA Supreme Court.

ARGUMENT

I. The Plain Text of the SCA Prohibits Meta and Snap from Disclosing the Contents of Communications Sought in this Case.

Section 2702(a) of the SCA protects the contents of communications held by electronic communication service (ECS) providers like Meta and Snap. Specifically, it prohibits ECS providers from disclosing "the contents of a communication while in electronic storage." 18 U.S.C. § 2702(a)(1). Electronic storage includes "any storage ... for purposes of backup protection." 18 U.S.C. § 2510(17)(B). Meta and Snap are ECS providers 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 v. Watts*, 917 F.3d 770, 795 (4th Cir. 2019) (defining backup protection); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (same); *Republic of Gambia v. Facebook, Inc.*, 575 F. Supp. 3d 8, 13 (D.D.C. 2021) (same).

The plain text of the SCA does not remove this protection even when ECS providers' terms of service reserve the right to use data stored for backup protection for other purposes as well. *Hately*, 917 F.3d at 795 (finding that communications are still in "electronic storage" for purposes of "backup protection" under the SCA even if providers also store communications "for their own commercial purposes, such as to more effectively target advertisements").

In addition, the SCA contains other sections that particularly authorize provider access to (rather than disclosure of) content for a number of purposes aside from backup protection. *See, e.g.*, 18 U.S.C. § 2701(c)(1) (access for conduct authorized by the service); 18 U.S.C. § 2511(2)(a) (access for "protection of the rights or property of the provider of that service"); 18 U.S.C. § 2258A(f) (access for "affirmatively search[ing], screen[ing], or scan[ing] for facts or circumstances" related to CSAM); 18

Document received by the CA Supreme Court.

U.S.C. § 2511(2)(a)(ii) (access for providing technical assistance for foreign surveillance); 18 U.S.C. § 2703 (access for complying with required disclosure to law enforcement). Under the lower court's flawed reading, any statutorily authorized access apart from backup protection would strip the SCA's privacy protections away from users of any ECS.

Thus, the ECS provision should decide this case, and because Meta and Snap store the contents of communication sought in this case for the purpose of backup protection, the ECS provision prohibits disclosure.

II. The Purpose and History of the SCA Confirm Meta and Snap Are Prohibited from Disclosing the Contents of Communications Sought in this Case.

The lower court's ruling vitiates the purpose and history of the SCA. The express purpose of the statute is to protect users' privacy rights by restricting the disclosure of the content of their communications, despite providers' own access to that same content. This principle has guided nearly four decades of practice. Through its ruling, the lower court has erroneously overturned one of the pillars of federal communication privacy protection.

A. The Lower Court's Ruling Thwarts the Broad Privacy Protections of the SCA.

The SCA 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).

The lower court's ruling renders the SCA's disclosure protections

Document received by the CA Supreme Court.

essentially meaningless, because almost no provider—existing in the modern world or in 1986—would meet the requirements imposed under the ruling. Nearly every provider accesses the content of users' communications for their own business purposes—whether it be to combat spam, remove illegal or prohibited content, or serve online behavioral advertising. End-to-end encrypted messaging apps like Signal would be some of the few providers that remain subject to 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 such technical barriers. S. REP. 99-541, 5, 1986 ("Privacy cannot be left to depend solely on physical protection[.]").

If the lower court's ruling is affirmed, Meta, Snap, and other providers would be permitted to voluntarily disclose the content of their users' communications to any other corporation, the government, or any individual for any reason. This would mark a fundamental sea change in communications privacy. Disclosures of the content of a person's communications—which may include intimate conversations with friends and family about private subjects such as a person's health or finances—could be made to a person's enemy, an adverse party in civil litigation, a data broker compiling a personal profile, or the government without a warrant.

The lower court incorrectly waived away this danger as one that "the market" will fix. *Snap, Inc. v. Superior Ct. of San Diego Cty.*, 103 Cal. App. 5th 1031, 1066 (2024).

But the market demonstrates just the opposite: the global data broker market, which traffics in individuals' data, was valued at an estimated $254

Document received by the CA Supreme Court.

billion in 2022.[1] Given the insights that advertisers and others could gain from private communications revealing people's interests and preferences, that already lucrative market could feature huge financial incentives for providers to sell user communications content for a fee, with such fees escalating with the sensitivity of the communication to be disclosed. The possibility of such sales would likely be obfuscated in impenetrable prose in company privacy policies. Unfortunately, even today, average customers are largely unaware of companies' privacy practices. Only nine percent of people say they always read privacy policies.[2] And even if they do, most just glance over them. Moreover, consolidation and network effects of social media make it hard for individual customers to choose to leave popular platforms over their privacy concerns.[3] Privacy laws exist so that users do not have to put their trust in companies to do the right thing, especially when companies have not earned that trust.[4]

---

[1] *Data Broker Market - Global Industry Size, Share, Trends, Opportunity, and Forecast*, 2018-2028 (Nov. 2023), https://www.researchandmarkets.com/reports/5909254/data-broker-market-global-industry-size#tag-pos-4.

[2] Pew Research Center, *Americans' attitudes and experiences with privacy policies and laws* (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

[3] Aaron S Edlin et al., The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google, 15 Yale J. L. & Tech. 169, 178 (2013).Aaron S Edlin et al., *The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google*, 15 Yale J. L. & Tech. 169, 178 (2013).

[4] FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

Document received by the CA Supreme Court.

The lower court's ruling does not disturb the Fourth Amendment requirement that law enforcement would still need a warrant to compel providers to disclose their users' communications. *See United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). But if those communications were available from a data broker for purchase, law enforcement could attempt to bypass the warrant requirement entirely.[5] Moreover, the court's flawed reasoning could have the effect of weakening the foundation of the warrant protection even as to communications service providers. Prosecutors for years have incorrectly tried to side-step Fourth Amendment protections by arguing a company's terms of service remove a user's reasonable expectation of privacy. *See* Kerr, Orin S., *Terms of Service and Fourth Amendment Rights* U. Penn. L. Rev. 287 (2024). The lower court adopted a version of that flawed argument and applied it to a statute instead of the Fourth Amendment.

B. The Lower Court's Ruling Undermines Congressional Intent Through the Court's Reliance on Corporate Policies.

The lower court's ruling 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 the 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*, 103 Cal. App. 5th at 1064. The court also incorrectly asserted the SCA's privacy purpose is absent because "users have given the

[5] *See* Matthew Guariglia, *Fourth Amendment is Not For Sale Act Passed the House, Now it Should Pass the Senate*, EFF (April 18, 2024), https://www.eff.org/deeplinks/2024/04/fourth-amendment-not-sale-act-passed-house-now-it-should-pass-senate.

Document received by the CA Supreme Court.

providers authorization to access and use their content for their own business purposes." *Id.* at 1062.

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*, 631 F.3d at 287. Privacy protections are not set by the "crazy quilt" of corporate policies and billing practices, *Smith v. Maryland*, 442 U.S. 735, 745 (1979), nor by terms that allocate risk "between private parties." *Byrd v. United States*, 584 U.S. 395, 408 (2018). *See also Van Buren v. United States*, 593 U.S. 374, 396 (2021) (cautioning courts not to stake so much of a law's interpretation on the "drafting practices of private parties").

As a factual matter, users do not in any meaningful way give providers authorization to access and use the content of their communications. Users cannot read all the terms that govern the online tools needed to function in modern society.[6] Even if users tried, it would require them to "ferret through a labyrinth of legal jargon." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1151 (9th Cir. 2024). "As anyone with a smartphone can attest, electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary." *United States v. Smith*, 110 F.4th 817, 835 (5th Cir. 2024).

C. The Lower Court's Ruling Conflicts with 40 Years of Interpretation by Courts, Congress, and Federal Prosecutors.

No court since the SCA passed in 1986 has ever ruled that a

[6] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. Law Review 593 (2024), https://ssrn.com/abstract=4333743.

Document received by the CA Supreme Court.

provider's business model of accessing user communications for its own purposes removes SCA protection for users. That is despite courts, Congress, and prosecutors being fully aware of service providers' own access to the content of communications.

Congress's own study in 1985 found that providers regularly retain copies of user messages for their own "administrative purposes"—a reason to protect those copies through statute.[7] And more recently, the Fourth Circuit dismissed the idea that a company's targeted advertising business model would affect the SCA disclosure analysis. *Hately*, 917 F.3d at 795 (taking as given that Google accesses copies of emails "for their own commercial purposes").

Congress has recently agreed that the SCA's disclosure provisions govern modern-day companies. Fully aware of the business model of modern service providers, Congress amended the SCA in 2018 to ensure Microsoft 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.*, 584 U.S. 236 (2018) (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."[8] Similarly, Congress in 2016 engaged extensively with Google and other modern providers before nearly passing a separate

[7] *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.

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

Document received by the CA Supreme Court.

overhaul of the SCA.[9] That debate happened during a time when Google engaged in the maligned practice of scanning the contents of users' emails to serve targeted ads. [10]

Taking a lead from Congress and the courts, federal prosecutors have also consistently held the position that the SCA applies to modern communications providers. The Department of Justice's computer search manual advises prosecutors that the SCA is the primary barrier to companies like Google or Yahoo! voluntarily disclosing information.[11] And the Department of Justice has repeatedly publicly asserted that the SCA— as amended by the CLOUD Act— applies to "social media communications"[12] and companies like "Facebook, Amazon, or Google."[13]

If members of Congress or administration officials concluded that

---

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

[10] 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.

[11] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual*, DOJ, Computer Crime and Intellectual Property Section, 25 (2009).

[12] Speech, DOJ, *Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the 5th German-American Data Protection Day on "What the U.S. Cloud Act Does and Does Not Do"*, (May 16, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american.

[13] DOJ Crim. Div., *Remarks of Deputy Assistant Attorney General Richard W. Downing At the International Symposium on Cybercrime Response*, U.S. Dep't Justice, (Sep. 13, 2023), https://www.justice.gov/criminal/media/1315386/dl?inline.

Document received by the CA Supreme Court.

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.

D. The Lower Court's Ruling Will Not Curb Online Behavioral Advertising

The "business model argument" is animated by a legitimate discomfort with online behavioral advertising and the constant tracking in which online services engage. But rather than solve the very real problem of corporate surveillance, the lower court's ruling will perversely strip away some of the few statutory privacy protections that U.S. users have on the internet.

The "business model argument" is incorrectly based on the idea that the SCA is a "shield that protects" companies. *See, e.g., Facebook, Inc. v. Superior Ct. of San Diego Cty*., 10 Cal. 5th 329, 373 (2020) (J. Cantil-Sakauye, Concurring). Under this theory, companies can earn this protection by limiting their access to and disclosure of users' communications or lose it by doing the opposite.

But this turns the SCA on its head. The SCA is a protection *for users* that runs *against companies* who might wish to share users' information more readily. It is also a modest protection for users against the government, which can, with proper legal process, compel companies to disclose information about their users and their users' communications. Companies should not be able to escape compliance with the SCA by engaging in online behavioral advertising. If the lower court's decision is allowed to stand, that would be the result. It would create a perverse incentive structure in which a company can reason: If we compromise our users' privacy interests enough by using their behaviors to target our

Document received by the CA Supreme Court.

advertising, we do not have to comply with the privacy law at all.

Amici have sought to correct the advertising ecosystem with user tools, advocacy, and legislation.[14] We have asked Congress to strengthen the SCA and pass a strong comprehensive data privacy law. But in the meantime, the SCA's modest protections should be enforced as they have for the past 40 years.

CONCLUSION

Because the services offered by Meta and Snap in this case are subject to the Stored Communications Act, this Court should reverse the lower courts' decision.

Dated: February 24, 2025

Respectfully submitted,

By: */s/ F. Mario Trujillo*

F. MARIO TRUJILLO (SBN 352020)
mario@eff.org
ANDREW CROCKER (SBN 291596)
andrew@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Counsel for Amici Curiae

[14] 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/; Jenn Taylor Hodges, *Work Gets Underway on a New Federal Privacy Proposal*, Mozilla (Apr. 26, 2024), https://blog.mozilla.org/netpolicy/2024/04/26/work-gets-underway-on-a-new-federal-privacy-proposal; Mozilla, *Facebook Container*, https://www.mozilla.org/en-US/firefox/facebookcontainer.

Document received by the CA Supreme Court.

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this **AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND MOZILLA CORPORATION IN SUPPORT OF SNAP AND META** is proportionally spaced, has a typeface of 13 points or more, contains 3,102 words, excluding the cover, the tables, the signature block, verification, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: February 24, 2025

/s/ F. Mario Trujillo
F. Mario Trujillo
Counsel for Amicus Curiae

Document received by the CA Supreme Court.

CERTIFICATE OF SERVICE

STATE OF CALIFORNIA, COUNTY OF SAN FRANCISCO

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

On February 24, 2025, I served the foregoing document entitled:

AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND MOZILLA CORPORATION IN SUPPORT OF SNAP AND META
on the attached Service List

[X] BY ELECTRONIC TRANMISTION VIA TRUEFILING: I caused a copy of the foregoing documents to be sent via TrueFiling to the persons at the e-mail addresses listed in the Service List. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful.

[X] BY FIRST CLASS MAIL: I caused to be placed the envelope for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid.

Executed on February 24, 2025 at San Francisco, California.

/s/ James A. Littau
JAMES A. LITTAU

Document received by the CA Supreme Court.

SERVICE LIST

PERKINS COIE LLP Julie E. Schwartz Ryan T. Mrazik, Pro Hac Vice John R. Tyler, Pro Hac Vice jschwartz@perkinscoie.com 1201 Third Ave., Suite 4900 Seattle, WA 98101	Via E-File Service
Natasha Amlani 1888 Century Park East Suite 1700 Los Angeles, CA 90067	Via E-File Service
GIBSON, DUNN & CRUTCHER LLP Joshua S. Lipshutz, jlipshutz@gibsondunn.com One Embarcadero Center, # 2600 San Francisco, CA 94111	Via E-File Service
Michael J. Holecek Alexander N. Harris 333 South Grand Avenue Los Angeles, CA 90071	Via E-File Service
Natalie J. Hausknecht, Pro Hac Vice 1801 California Street, Suite 4200 Denver, CO 80202	Via E-File Service
FENWICK & WEST, Petitioner Snap Inc. Attn: Tyler G. Newby 555 California Street #12 San Francisco, CA 94101 tnewbygfenwick.com	Via E-File Service
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	Via E-File Service
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	Via E-File Service

Document received by the CA Supreme Court.

San Diego County Superior Court, Respondent Hon. Daniel F. Link, Judge C/O Judicial Services 325 S. Melrose, Department 21 Vista, CA 92081	Via First Class Mail
Court of Appeal, Fourth Appellate District, Division One 750 B Street, Suite 300 San, Diego, CA 92101	Via First Class Mail

Document received by the CA Supreme Court.