No. S286267

In the Supreme Court of California

Snap, Inc., *Petitioner,*
vs.
Superior Court of San Diego County, *Respondent,*
Adrian Pina et al., *Real Parties in Interest.*

Meta Platforms Inc., *Petitioner,*
vs.
Superior Court 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 1, Case Nos. D083446, D083475
San Diego Superior Court, Case Nos. SCN429787, SCN429787
Hon. Daniel J. Link, Judge Presiding

Application to File Amicus Curiae Brief; Amicus Curiae Brief of Bolo Bhi, Digital Rights Foundation, Open MIC, Software Freedom Law Center, Tech Global Institute, and Wikimedia Foundation in Support of None of the Parties

---

Vanessa Racehorse (SBN 317737)	Vivek Krishnamurthy (pro hac vice pending)
University of Colorado Law School	*Colorado Law Clinical Programs*
Wolf Law Building | 401 UCB	Wolf Law Building | 404 UCB
2450 Kittredge Loop Dr.	2450 Kittredge Loop Dr.
Boulder, CO 80309–0401	Boulder, CO 80309–0404
vanessa.racehorse@colorado.edu	vivek.krishnamurthy@colorado.edu

Counsel for amici curiae

Table of Contents

Table of Authorities

Cases

Statutes

Other Authorities

International Agreements

Application to File Brief of Amici Curiae in Support of None of the Parties

Pursuant to Rule 8.520(f) of the California Rules of Court, the organizations described below request permission to file the attached brief as amici curiae in support of none of the parties. No party or counsel for any party in the pending appeal authored the proposed amicus brief in whole or in part, or made a monetary contribution intended to fund the preparation or submission of the brief. No person or entity made a monetary contribution intended to fund the preparation or submission of the brief other than the amici curiae, their members, or their counsel.

1. Identity of Amici Curiae

Amici are non-profit organizations that are committed to a free, open, global, and secure Internet. They include civil society groups, digital rights advocates, and free-knowledge organizations based in the U.S. and abroad. Amici work to protect Internet users' rights, strengthen privacy and data security, and ensure that the Internet remains a trusted space for knowledge, communication, and expression.

Amicus curiae **Bolo Bhi** is a civil society organization based in Pakistan geared towards advocacy, policy, and research in the areas of digital rights and civic responsibility. This encompasses the right to information, free speech, and privacy online, so that the Internet can be realized as a free and representative space for civic and political engagement for all segments of Pakistani society, including marginalized communities and genders.

Amicus curiae **Digital Rights Foundation** (DRF) is a registered research-based advocacy NGO that focuses on the information and communication technology sector to support human rights, democratic processes, and digital governance. Based in Pakistan, DRF seeks to increase awareness about privacy issues and defend the right to privacy

by research, monitoring and reporting the tactics around surveillance. DRF also aims to strengthen protections for human rights defenders, with a focus on women's rights in digital spaces, through policy advocacy & digital security awareness-raising.

Amicus curiae **Open MIC** (Open Media and Information Companies Initiative) works to foster greater corporate accountability in the deployment and use of digital technologies. Its primary tools are investor engagement and other finance-focused strategies. It provides investors with the education, tools, and networks needed to hold tech companies accountable for the impact of their policies and practices on people's lives and to promote values of openness, equity, privacy, and diversity—values that provide long-term benefits for individuals, companies, the economy, and democratic society.

Amicus curiae **Software Freedom Law Center** (SFLC.in) is a donor-supported legal services organization based in India that has united lawyers, policy analysts, technologists, business professionals, students and citizens to protect freedom in the digital world since 2010. In discussions of technology where industry and governments have representation, SFLC.in endeavors to present the rights of Indian citizens and fights to keep the Internet open, secure and safe for all.

Amicus curiae **Tech Global Institute** (TGI) is a digital rights non-profit headquartered in Canada, dedicated to advancing equity for communities in the Global Majority on the Internet. Through evidence-based research, policy and legal advocacy, and South-South coalition-building, TGI works to strengthen the accountability of technology design and governance, ensuring that the rights of underserved communities are safeguarded throughout the process. Its mission is to amplify marginalized voices and realities in global policy discussions.

Amicus curiae **Wikimedia Foundation** is a non-profit organization based in San Francisco that operates twelve free-knowledge projects on

the Internet. Wikimedia Foundation's projects host factual and educational content that is created, edited, and moderated by over 300,000 volunteer contributors per month worldwide. Wikimedia Foundation provides this content to people free of charge and is not funded by advertising. Wikimedia Foundation therefore relies on donations and philanthropic grants to provide its services. Wikimedia Foundation's most well-known project is Wikipedia—the largest and most-read reference work in history. As of 2022, Wikipedia was ranked as the fifth-most popular website in the world and, since its creation, users have authored over 6.5 million English language articles.

2. Interests of Amici Curiae

Amici submit this brief to inform the Court of the international implications of this case, which have not been discussed in any detail in the briefs of the parties.

As organizations committed to advancing Internet freedom, amici have a strong interest in the appropriate interpretation of the Stored Communications Act ("SCA"), which has long protected user content data from warrantless searches by U.S. and foreign governmental entities. The Court of Appeals' adoption of the "business purpose" theory of the SCA eviscerates these protections, however. Its effect would be to remove the restrictions that prohibit U.S. technology companies from voluntarily disclosing content data to foreign governments—including data pertaining to U.S. persons—whenever such companies use their users' data for their own "business purposes."

By effectively eliminating the requirement that foreign governments seek the help of the U.S. government in obtaining a search warrant to gain access to content data stored in the U.S., the Court of Appeals' decision threatens the privacy and security interests of Internet users at home and abroad. The dangers are grave as governments, especially authoritarian

ones, are increasingly pressuring foreign technology companies to comply with their arbitrary demands by enacting "hostage-taking" laws that threaten in-country employees with imprisonment if their company does not do so. The Court of Appeals' ruling weakens global trust in U.S. legal protections and the ability of U.S.-based Internet companies to safeguard the privacy and data security interests of their users against the threat posed by foreign government actions.

Many Amici advocate for strong privacy safeguards against government overreach. Some operate platforms for public discourse, knowledge-sharing, and open collaboration—platforms that rely on legal guarantees that user content data will not be improperly disclosed. The Court of Appeals' interpretation of the SCA strips away these protections, exposing Internet users, including journalists, activists, and vulnerable communities, to surveillance and persecution.

Amici therefore urge this Court to reject the Court of Appeals' flawed interpretation of the SCA in view of the danger it poses to the privacy and digital security rights of billions of Internet users in the U.S. and abroad. They further urge the Court to resolve the issues presented by this case on grounds other than the "business purpose" theory of the SCA.

3. Conclusion

For the foregoing reasons, the proposed amici curiae request that the Court accept the accompanying brief for filing in this case.

Respectfully submitted,

/s/ *Vanessa Racehorse*

Vanessa Racehorse (SBN 317737)
University of Colorado Law School
Wolf Law Building | 401 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404

Vivek Krishnamurthy (pro hac vice pending)
Colorado Law Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404

Counsel for amici curiae

February 21, 2025

Brief of Amici Curiae

Amici urge this Court to reject the "business purpose" theory of the Stored Communications Act (SCA) adopted by the Court of Appeals. The Court of Appeals' adoption of this theory shatters longstanding understandings of the SCA. If upheld, this interpretation would dramatically weaken the privacy protections that billions of Internet users in the U.S. and worldwide have long relied upon to keep their personal data safe and secure.

The SCA prohibits technology companies from disclosing user content data stored in the U.S. to foreign governments at their request, absent oversight from the U.S. Department of Justice (DOJ) through either the Mutual Legal Assistance Treaty (MLAT) or letters rogatory processes. This framework ensures that any such disclosures are subject to the Fourth Amendment's probable cause standard.

By holding that private content data loses SCA protection whenever a company processes such data for its own business purposes, the Court of Appeals' decision removes this safeguard, effectively permitting U.S.-based Internet platforms to provide user content data to foreign governments without judicial oversight. This poses a risk to the privacy and security interests of U.S. persons who enjoy the protections of the Fourth Amendment, and to Internet users around the world who depend on the SCA to protect their data against their own governments.
The Court of Appeals' interpretation of the SCA would fundamentally reshape the global digital landscape. Foreign Internet users have long relied on the well-established understanding of the SCA as a "blocking statute" in deciding to entrust their sensitive data to U.S.-based Internet services. The Court of Appeals' ruling betrays that expectation, undermining the trust that foreign Internet users have placed in the American legal system to protect their data.

Many foreign governments have already sought to pressure technology companies into doing their bidding, with some regimes leveraging "hostage-taking" laws that threaten local employees with imprisonment if companies refuse to comply with government demands. This poses a particular threat to Amicus Wikimedia Foundation, as such pressure creates additional risks for the volunteers who contribute and edit content for Wikipedia and its other projects.

Without the SCA's blocking function, U.S. technology firms will lack a clear legal justification to resist such arbitrary foreign government demands, fundamentally altering the power dynamics between repressive states and U.S.-based technology companies. The result will be an Internet that is more fragmented and more dangerous for its users.

For all these reasons, this Court should reject the lower court's interpretation of the SCA and decide the important issues presented by this case on other grounds.

1. The SCA Has Long Functioned as a Blocking Statute That Restricts Disclosures of User Data.

The SCA has long been understood as prohibiting service providers from disclosing user data to private and public entities alike, unless one of nine statutory exceptions applies.[1] Courts have held time and again that these protections apply to users' private data held by companies that were using such data for their own business purposes (such as ad targeting) at the time such cases were decided.[2]

---

[1] These circumstances are specified in 18 U.S.C. § 2702 (b).

[2] *See, e.g., Hately v. Watts,* 917 F.3d 770, 786, 796-797 (4th Cir. 2019); In re Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 145 (3d Cir. 2015); *Republic of Gambia v. Facebook, Inc.,* 575 F. Supp. 3d 8, 13-14 (D.D.C. 2021); *In re Yahoo Litig.,* 7 F. Supp. 3d 1016 (N.D. Cal. 2014); *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.,* 961 F. Supp. 2d 659, 667-669 (D.N.J.

The Court of Appeals' decision upends this settled law by holding that otherwise private user data ceases to be protected by the SCA if a technology company uses it for its own business purposes. This radical shift in doctrine has sweeping implications—particularly in the realm of cross-border data access—that harms U.S. and non-U.S. persons alike.[3]

2. The Court of Appeals' Decision Overturns the SCA's Legislative Framework for Foreign Data Requests

Congress has explicitly structured U.S. law to ensure that foreign governments cannot directly compel technology companies to disclose content data[4] stored in the United States. Under the SCA, such disclosures are prohibited unless the requesting government seeks the assistance of the U.S. government in obtaining it.[5] Specifically, foreign governments

---

2013); *Crispin v. Christian Audigier, Inc.,* 717 F. Supp. 2d 965, 982-991 (C.D. Cal. 2010); *Viacom Int'l Inc. v. Youtube Inc.,* 253 F.R.D. 256, 264 (S.D.N.Y. 2008); *Facebook, Inc. v. Superior Ct.,* 4 Cal. 5th 1245 (2018); *Negro v. Superior Ct.,* 230 Cal. App. 4th 879, 889, 901-904 (2014), as modified (Nov. 18, 2014); Facebook v. Wint, 199 A.3d 625, 628-629 (D.C. 2019); *People v. Harris,* 36 Misc. 3d 613, 621-622 (N.Y. Crim. Ct. 2012).

[3] This brief uses "U.S. persons" as defined in 22 U.S.C. § 6010, which defines the term to mean "any United States citizen or alien admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States."

[4] In the argot of the SCA, "content" is the electronic communication that a person intends to share with another person, while "non-content" data is information about the communication that the network uses to deliver and process the content. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1228 (2004).

[5] The SCA includes an emergency exception that allows U.S.-based Internet companies to disclose content and non-content data to U.S. government agencies in certain life-threatening emergencies. *See id.* at

must request the assistance of the U.S. Department of Justice by invoking the provisions of a mutual legal assistance treaty (MLAT)[6U.] or by issuing letters rogatory.[7] Both options are available for criminal proceedings, but letters rogatory (a significantly slower method) are the only available method for civil proceedings.[8] Following a detailed review by DOJ personnel to ensure that the incoming foreign request is not pretextual and that the offense being investigated by the foreign jurisdiction is also a crime in the United States (the "double criminality" requirement),[9] DOJ personnel will apply for a search warrant in a U.S. court of competent jurisdiction to obtain the content data sought by the foreign entity.

This system ensures that foreign government requests for data stored by U.S. companies are subject to the same due process and probable cause

---

1221; *see also* 18 U.S.C. §§ 2702 (b)(8), (c)(4). While the SCA does not explicitly authorize emergency disclosures to foreign governments, companies have interpreted 18 U.S.C. § 2702(c)(6), which permits voluntary disclosures of non-content information to "any person other than a governmental entity," to include foreign governments. Furthermore, some companies have made emergency disclosures of content data to foreign governments based on provisions in their terms of service that permit them to do so. *See* Carrie Cordero & Aaron Altschuler, *Responding to Foreign Requests for Data Through the MLAT Process*, ZwillGen (Oct. 5, 2020), https://www.zwillgen.com/general/responding-foreign-requests-data-mlat/; see also 18 U.S.C. § 2702(c)(6).

[6] T. Marcus Funk, Fed. Jud. Ctr., Mutual Legal Assistance Treaties and Letters Rogatory: Obtaining Evidence and Assistance from Foreign Jurisdictions 1 (2d. ed. 2024), https://www.fjc.gov/sites/default/files/materials/48/MLAT%20final%20042424.pdf. The Office of International Affairs in the U.S. Department of Justice's Criminal Division maintains a list of MLATs ratified by the U.S. at https://www.justice.gov/d9/pages/attachments/2022/05/04/mutual-legal-assistance-treaties-of-the-united-states.pdf.

[7] Funk, *supra* note 6, at 1.

[8] *Id.*

[9] *Id.* at 11.

requirements as digital searches and seizures by U.S. law enforcement authorities. The passage of the CLOUD Act in 2018[10] modified this framework by allowing the U.S. government to enter into agreements with foreign nations for cross-border data sharing, but only under stringent human rights conditions.[11] During discussions leading up to the CLOUD Act's enactment, there was broad consensus that the SCA functioned as a "blocking statute"[12] that prevented U.S. technology companies—including those that used their users' data for ad targeting or other business purposes—from disclosing user communications to foreign governments other than through the MLAT process. For example, former Acting Deputy Assistant Attorney General Richard W. Downing testified before Congress that data relevant to foreign criminal investigations "[o]ften … is stored or accessible only in the United States, where U.S. law, including the SCA, limits the companies' ability to disclose it."[13]

---

[10] Clarifying Lawful Overseas Use of Data ("CLOUD") Act, Pub. L. No. 115-141, 132 Stat. 1213-25 (2018) (codified in scattered sections of 18 U.S.C).

[11] 18 U.S.C. § 2523(b).

[12] See, e.g., Matt Perault & Richard Salgado, Ctr. for Strategic & Int'l Stud., Untapping the Full Potential of CLOUD Act Agreements (2024), https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements; *see also* Peter Swire & Jennifer Daskal, *Frequently Asked Questions About the U.S. CLOUD Act,* Cross-Border Data Fdn. (Apr. 16, 2019), https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/#:~:text=The%20Stored%20Communications%20Act%20(SCA,place%20(as%20discussed%20below).

[13] *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary, 115th Cong.* (2017) (statement of Richard Downing, Acting Deputy Assistant Att'y Gen., Dep't of Justice), available at https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era.

Correspondingly, "[t]he M[utual] L[egal] A[ssistance] process has frequently been the only mechanism that can provide foreign countries with access to this data…."[14]

The CLOUD Act was designed to create an exception to this general prohibition, but only in tightly controlled circumstances where the U.S. government had reviewed a foreign government's human rights record and found that it met the highest standards.[15] As of the writing of this brief, the U.S. has entered into CLOUD Act agreements with the United

[14] *Id.*

[15] The human rights conditions that foreign states must meet are specified in 18 U.S.C. § 2523(b)(1)(B) and include factors such as adherence "to applicable international human rights obligations and commitments" as well as the existence in the foreign state "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data…."

Kingdom[16] and Australia,[17] and it has begun negotiations with Canada[18] and the European Union.[19]

The Court of Appeals' interpretation of the SCA, however, renders these protections meaningless. If a user's private content data loses SCA protections when a company uses that data for its own business purposes, such companies are under no legal obligation to deny foreign governments' direct requests for user data—bypassing the entire framework Congress established to prevent abuses. This undermines the careful balance struck by the CLOUD Act, which sought to maintain the SCA's blocking function while creating a mechanism for lawful data transfers with foreign states that accord the highest respect for human rights. The implications of such a holding would be extraordinary for U.S.-

---

[16] Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (Oct. 3, 2019), *available at* https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern.

[17] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, (Dec. 15, 2021), *available at* https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia.

[18] Press Release, U.S. Dep't of Just., United States and Canada Welcome Negotiations of a CLOUD Act Agreement (Mar. 22, 2022), https://www.justice.gov/archives/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.

[19] Press Release, U.S. Dep't of Just., Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations (Mar. 2, 2023), https://www.justice.gov/archives/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations .

based Internet companies that operate in jurisdictions beyond the U.S., the U.K., and Australia—as detailed in section 4, *infra.*

3. The Business Purpose Theory Misapprehends How the Modern Digital Economy Works.

The Court of Appeals' reasoning is fundamentally flawed in another respect: in today's digital economy, virtually every technology company processes user data for its own business purposes. In the age of artificial intelligence, nearly all digital service providers—whether social media platforms, search engines, or generative AI companies—use personal data to train models, improve user experience, and optimize content delivery.[20] If such usage were to disqualify user data from SCA protection, virtually no digital service would remain covered by the Act.

---

[20] See *Apple Priv. Policy*, Apple (Sep. 18, 2024), https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf (explaining how Apple collects and uses personal data, *inter alia*, to "power [their] services," "improve [their] offerings," and "for internal purposes such as auditing or data analysis"); *Priv. Policy*, OpenAI (Nov. 4, 2024), https://openai.com/policies/row-privacy-policy ("We may use Personal Data for the following purposes: To provide, analyze, and maintain our Services, for example to respond to your questions for ChatGPT; To improve and develop our Services and conduct research, for example to develop new product features…"); *Microsoft Priv. Statement*, Microsoft (Last Updated Jan. 2025), https://www.microsoft.com/en-us/privacy/privacystatement ("As part of our efforts to improve and develop our products, we may use your data to develop and train our AI models."); *Google Priv. & Terms*, Google (Sept. 16, 2024), https://policies.google.com/privacy?hl=en-US#whycollect ("Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's AI models and build products and features like Google Translate, Gemini Apps, and Cloud AI capabilities.").

At the same time, the Court of Appeals' reasoning threatens U.S. competitiveness in the global digital economy. In an era where user engagement depends on data-driven features—such as monetization and targeted advertising—restricting data usage in this manner places American companies at a structural disadvantage. Yet, the fact that digital services rely on user data for commercial viability should not strip that data of statutory privacy protections. The logic of the opinion below risks weakening digital privacy at the very moment when such safeguards are most essential.

Furthermore, the Court of Appeals' reliance on market forces to discipline companies that voluntarily disclose user data is misplaced. Former Chief Justice Cantil-Sakauye's concurring opinion in *Touchstone* suggests that firms whose terms of service fail to adequately protect user privacy might eventually be driven out of the market.[21] But this reasoning overlooks at least **five** critical factors.

First, contracts with most digital services providers—from residential internet service providers to social media platforms—are contracts of adhesion, meaning users have no meaningful ability to negotiate privacy or any other terms.[22]

Second, the reason that contracts of adhesion are so prevalent in the digital economy is that most digital services are offered by one of a small number of oligopolistic providers. Correspondingly, there is little choice

---

[21] *Facebook, Inc. v. Super. Ct. (Touchstone)*, 471 P.3d 383 at 411 (Cantil-Sakauye CJ, concurring) (2020).

[22] *See generally* Margaret Jane Radin, Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (2013) (explaining how the increasing use of contracts of adhesion, particularly in the digital economy, is undermining traditional notions of consent, agreement, and contract—especially with regard to the inclusion of arbitration clauses that prevent judicial review of disputes arising under such contracts).

available to consumers who wish to seek privacy-protective alternatives.[23] For example, consider the global market in smartphones. Practically all of the billions of smartphones in use around the world today run on just one of two operating systems: Apple's iOS and Google's Android.[24] Hence, users of devices that the U.S. Supreme Court described as "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy" have no choice but to accept the contracts of adhesion offered by Apple and Google that govern their smartphones.[25] Smartphones are the essential technology gateways that we rely upon to access the dizzying array of digital services that are available to us today, but a lack of competition is a feature of most other markets for digital services—from cloud-based storage to social media platforms.

Third, not all digital services are created the same, hence they cannot be offered using identical terms of service. The People's Answer in the case at bar points to the terms on which companies offer encrypted messaging services (e.g. Apple's iMessage, Meta's WhatsApp, and Signal) as evidence that modern digital services can be offered without companies

---

[23] *See, e.g.*, Staff of H. Comm on the Judiciary, 117th Cong., Rep. on Investigation of Competition in Digital Markets 5-6 (Comm. Print 2022) (finding that "Over the past decade, the digital economy has become highly concentrated and prone to monopolization. Several markets investigated by the Subcommittee—such as social networking, general online search, and online advertising—are dominated by just one or two firms. The companies investigated by the Subcommittee—Amazon, Apple, Facebook, and Google—have captured control over key channels of distribution and have come to function as gatekeepers. Just a decade into the future, 30 percent of the world's gross economic output may lie with these firms, and just a handful of others.").

[24] *Global Smartphone Share Sales by Operating System*, Counterpoint (Dec. 2, 2024), https://www.counterpointresearch.com/insights/global-smartphone-os-market-share.

[25] *Riley v. California*, 573 U.S. 373, 385 (2014).

leveraging content data for their own business purposes.[26] Yet, to quote the vivid language of Chief Justice Roberts, "this is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[27] The same is true of the dizzying array of digital services where the SCA serves as a crucial guarantee of user privacy: some are capable of being operated without their providers using their users' data for their own business purposes, but many others (especially those incorporating AI) are not.

Fourth, to the extent that premium, privacy-protecting versions of oligopolistic digital services are even available, they are priced beyond the reach of most people—particularly those who are located in the Global South. For example, the ad-free version of Meta's Facebook social media platform, which is only available in Europe, costs $8.36 per month for use on a mobile device.[28] Even if the ad-free version were available in Pakistan (which it is not), subscribing to Facebook would consume more than 7% of

---

[26] Brief for The People, at 36–42., *Snap, Inc. v. Super. Ct. of San Diego Cnty.*, No. S286267 (Cal. Dec. 18, 2024).

[27] *Riley*, *supra* note 25, at 393.

[28] *Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe,* Meta (Nov. 12, 2024), https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ (explaining how subscriptions for ad-free versions of these products are priced at €5.99/month on the web and €7.99/month on iOS and Android. At current exchange rates, this works out to $6.27 and $8.36, respectively.).

the average person's monthly income.[29] As a proportion of income, this is similar to what the average American spends on healthcare.[30]

Fifth, even if consumer backlash were to eventually eliminate firms that fail to adequately protect their users' privacy from the marketplace, that process would take time—time that vulnerable individuals do not have. If the SCA no longer prevents U.S. companies from complying with foreign government data requests, foreign governments can begin coercing user data from Internet companies immediately. Dissidents, journalists, and activists—including many who have fled to the U.S. for their own safety—cannot wait for the market to correct the situation; the threats they face are immediate and severe.

4. The Business Purpose Theory of the SCA is Especially Dangerous in an Era of Rising Digital Authoritarianism.

A decision upholding the lower court's ruling risks accelerating a global trend toward digital authoritarianism,[31] where governments exert control over Internet infrastructure and services to suppress dissent and engage in surveillance. In recent years, numerous countries have enacted so-called "hostage-taking" laws, requiring foreign technology companies to maintain a local presence with designated representatives who can be

---

[29] *GDP per capita (current US$) - Pakistan*, World Bank Open Data, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=PK, (last visited Feb. 19, 2025) (The World Bank reports that GDP per capita in Pakistan is $1,365.30 per year, which works out to $113.78 per month.).

[30] Dorothy Neufeld, *Visualizing How Americans Spend Their Money*, Visual Capitalist (Jan. 26, 2025), https://www.visualcapitalist.com/how-americans-spend-their-money/ (suggesting that the average American spends about 8% of their income on healthcare).

[31] *See generally* Allie Funk et al., *Freedom on the Net 2024: The Struggle for Trust Online*, Freedom House (2024), https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online.

held personally liable for non-compliance with government demands.[32] To quote a recent analysis by amicus curiae Tech Global Institute, such laws "provide broad discretion for governments to demand data, often without judicial oversight, and rely on vague definitions, enabling governments to exploit them for greater digital control."[33]

For example, India's Information Technology Rules of 2021 require social media platforms to appoint local grievance officers who can face criminal penalties for non-compliance with government takedown requests.[34] Turkey[35] and Vietnam[36] have enacted similar laws, forcing tech companies to either cooperate with government surveillance demands or risk losing access to their markets. These laws serve as tools of coercion, pressuring platforms into doing a government's bidding under the threat

---

[32] Andrew Deck, *"Hostage-taking laws" seem to be fueling a Twitter crackdown in India*, Rest of World (Jul. 1, 2022), https://restofworld.org/2022/twitters-censorship-india.

[33] *Statement: Proactive Role of The Stored Communications Act,* Tech. Global Inst., https://techglobalinstitute.com/announcements/statement-protective-role-of-the-stored-communications-act/ (last visited Feb. 20, 2025).

[34] Karishma Mehrotra & Joseph Menn, *How India tamed Twitter and set a global standard for online censorship*, Wash. Post (Nov. 8, 2023), https://www.washingtonpost.com/world/2023/11/08/india-twitter-online-censorship.

[35] Isabelle Canaan, NetzDG and the German Precedent for Authoritarian Creep and Authoritarian Learning, 28 Colum. J. Eur. L. 101, 127–29 (2022); Kim Lyons, Twitter will set up a legal entity in Turkey to comply with controversial social media law, The Verge (Mar. 20, 2021), https://www.theverge.com/2021/3/20/22341798/twitter-legal-entity-turkey-comply-social-media-law-privacy; *Turkey: Freedom on the Net 2024,* Freedom House (2024), https://freedomhouse.org/country/turkey/freedom-net/2024.

[36] Vittoria Elliott, *New laws requiring social media platforms to hire local staff could endanger employees*, Rest of World (May 14, 2021), https://restofworld.org/2021/social-media-laws-twitter-facebook.

of financial penalties, operational bans, or even the arrest of their employees.

Pakistan, where amici curiae Bolo Bhi and Digital Rights Foundation are based, provides an instructive yet chilling example of how authoritarian governments pressure technology companies into serving their interests. While on paper, Pakistan's laws on electronic surveillance and digital search and seizure are subject to judicial oversight, law enforcement agencies routinely coerce technology companies (especially telecommunications network operators) into conducting unlawful mass surveillance or granting them surreptitious access to personal data.[37] Recent amendments to Pakistan's *Prevention of Electronic Crimes Act* make matters worse by requiring social media platforms to "enlist" with the newly created Social Media Protection and Regulatory Authority ("Authority"),[38] which in turn can order them to promptly remove any content that it deems illegal.[39] Those who fail to obey the law face penalties ranging from fines to up to three years' imprisonment,[40] and the new law also strips the jurisdiction of Pakistan's courts to review the Authority's decisions.[41]

---

[37] *See, e.g., Mian Najam-us-Saqib v. Federation of Pakistan et al.*, WP 1805/2023 (Islamabad High Court, Dec. 20, 2023) (ordering Pakistan government officials to explain to the Court how they undertook cellphone audio surveillance of the son of the former Chief Justice of Pakistan, in view of the lack of any statutory basis to do so).

[38] S. 2Q, Prevention of Electronic Crimes (Amendment) Act (II of 2025) (Pak.) (available at https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf).

[39] *Id.*, S. 2B(l).

[40] *Id.*, S. 2X.

[41] Faisal Daudpota, *Pakistan Criminalizes Fake News: Free Speech Rights of Citizens v/s Desire of Government to Control Online Content* at 9 (Feb. 2, 2025), https://ssrn.com/abstract=5121591.

The longstanding understanding of the SCA as a "blocking statute" stands as a bulwark against unlawful and excessive foreign government demands for user content data held by U.S.-based companies. A recent analysis by amicus curiae Tech Global Institute finds that U.S.-based technology companies "strategically leverage SCA protections to resist overreaching demands" from authoritarian governments.[42] This is borne out by transparency reports published by leading technology companies, which show a low level of compliance with foreign government requests for user content data. For example, in the first half of 2024, Google complied with 0% of non-emergency government demands for user content data in countries ranging from Turkey to Thailand.[43] Such resistance would be futile, however, if a U.S.-based company could not point to the "blocking" provisions of the SCA and the threat of legal liability in its home country as rationales for its non-compliance.

If this Court upholds the lower court's adoption of the "business purpose" theory, it is virtually certain that such laws will be used against U.S.-based Internet companies to circumvent the MLAT process entirely. Without the SCA's blocking function, foreign governments could exploit these laws to demand content data directly from tech firms, sidestepping U.S. judicial oversight. This would expose vulnerable individuals in the U.S. and abroad—including journalists, activists, and opposition figures—to serious harm. In an age where foreign governments have few compunctions about plotting to kill dissidents on U.S. soil,[44] the implications of this decision would not be theoretical; they would be

---

[42] Tech Glob. Inst., *supra* note 33.

[43] *Global Requests for User Information*, Google Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en.

[44] *See, e.g., U.S. v. Gupta*, No. 23 CR 289 (S.D.N.Y. Nov. 29, 2023) (Indictment) (indicting an agent of the Government of India in a plot to assassinate a U.S. citizen who leads a Sikh separatist organization on U.S. soil) (available at https://www.justice.gov/usao-sdny/media/1356186/dl).

immediate and severe, emboldening authoritarian regimes and further eroding digital rights worldwide.

5. Alternative Means Exist to Reconcile Defendants' Rights and Online Privacy Protections.

Amici take no position on whether the real party in interest should be able to access the data he seeks. As organizations committed to the protection of human rights, however, amici recognize the importance of ensuring that defendants have access to evidence necessary for a fair trial. While the lower court's ruling seeks to provide such access, it does so at the cost of dismantling long-standing privacy protections for U.S. and non-U.S. persons alike. Yet alternative legal pathways exist that would preserve both privacy rights and the right to a defense.[45]

For example, this Court could follow the logic of the Sixth Circuit's ruling in *Warshak* and hold that in certain circumstances, the application of the SCA to prevent criminal defendants from accessing materials necessary for their defense violates their constitutional rights.[46] This would permit the creation of a narrow exception to the SCA to permit defendants to obtain private user content data from technology companies

---

[45] See, e.g., Rebecca Wexler, *Life, Liberty, and Data Privacy: The Global CLOUD, the Criminally Accused, and Executive Versus Judicial Compulsory Process Power,* 101 Tex. L. Rev. 1400 (examining structural biases in U.S. and global privacy laws that disadvantage criminal defendants, and suggesting various methods of reconciling Fourth Amendment protections for content data with the Fifth and Sixth Amendment rights of criminal defendants.).

[46] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that a provision of the Stored Communications Act that permitted law enforcement to subpoena emails that have been stored on a server for more than 90 days violated the Fourth Amendment in view of changing societal expectations of privacy, and technological changes in the nature of how email communications are processed and stored).

in appropriate circumstances, without otherwise upsetting longstanding understandings of the SCA.

Alternately, extending the principle recognized in *Chambers v. Mississippi*[47]—the right to present crucial evidence—could justify limited access to data held by technology companies for the defense. This approach could help ensure fairness in criminal trials without undermining the SCA's critical role in protecting user privacy worldwide.

Conclusion

This Court should reject the lower court's interpretation of the SCA. Instead, it should reaffirm that the privacy protections that users of U.S.-based Internet services enjoy against foreign governments should not turn on a provider's use of their content data for its own business purposes. This is consistent with decades of judicial precedent, congressional intent, and the settled expectations of Internet users in the U.S. and abroad.

Respectfully submitted,

/s/ *Vanessa Racehorse*

Vanessa Racehorse (SBN 317737)
University of Colorado Law School
Wolf Law Building | 401 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404

[47] *Chambers v. Mississippi*, 410 U.S. 284 (1973).

Vivek Krishnamurthy (pro hac vice pending)
Colorado Law Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404

Counsel for amici curiae

February 21, 2025

Certificate of Compliance

This brief complies with the typeface and volume limitations set forth in California Rules of Court, rule 8.204(c)(1). The brief has been typeset in a proportionally spaced typeface (13-point Linux Libertine), and it contains 5667 words as counted by the application used to prepare the brief (Microsoft Word for Mac version 16.94 (25020927)), excluding those items listed in CRC 8.520(c)(3).

Respectfully submitted,

/s/ *Vanessa Racehorse*

Vanessa Racehorse (SBN 317737)
University of Colorado Law School
Wolf Law Building | 401 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404

February 21, 2025

Certificate of Service

I, Vivek Krishnamurthy, declare that: (1) I am a citizen of the United States, (2) I am over the age of 18 years, (3) I reside in Boulder, Colorado, and (4) I am not a party to the present action. My business address is: Colorado Law Clinical Programs, Wolf Law Building, 2450 Kittredge Loop Dr. | 404 UCB, Boulder, CO 80309-0404.

I certify that on February 21, 2025, I electronically filed the documents listed below with the Clerk of the Court using the TrueFiling system.

Application to File Amicus Curiae Brief;
Amicus Curiae Brief of Bolo Bhi, Digital Rights Foundation, Open MIC, Software Freedom Law Center, Tech Global Institute, and Wikimedia Foundation in Support of None of the Parties

By operation of the Court's electronic filing system, these documents will be served on the parties to this action listed below:

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

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

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

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

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

Natasha Amlani
Perkins Coie LLP
1888 Century Park East
Suite 1700
Los Angeles, CA 90067
Email: namlani@perkinscoie.com
Counsel for Petitioner Meta Platforms, Inc.

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

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

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

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

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

I declare under penalty of perjury that the foregoing is true and correct, and that this declaration was executed on February 21, 2025, in Boulder, Colorado.

/s/ *Vivek Krishnamurthy*

Vivek Krishnamurthy
Colorado Law Clinical Programs
Wolf Law Building | 404 UCB
2450 Kittredge Loop Dr.
Boulder, CO 80309–0404
vivek.krishnamurthy@colorado.edu