NOS. 22-16888, 22-16889, 22-16914, 22-16916, 22-16921, 22-16923

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE: FACEBOOK SIMULATED CASINO-STYLE GAMES LITIGATION

KATHLEEN WILKINSON, et al.,

PLAINTIFFS–APPELLEES,

V.

FACEBOOK, INC.

DEFENDANT–APPELLANT.

IN RE: APPLE INC. APP STORE SIMULATED CASINO-STYLE GAMES LITIGATION

FRANK CUSTODERO, et al.,

PLAINTIFFS–APPELLEES,

V.

APPLE, INC.

DEFENDANT–APPELLANT.

IN RE: GOOGLE PLAY STORE SIMULATED CASINO-STYLE GAMES LITIGATION,

JENNIFER ANDREWS, et al.,

PLAINTIFFS–APPELLEES,

V.

GOOGLE, LLC, et al.,

DEFENDANTS–APPELLANTS.

On Appeal from the United States District Court
for the Northern District of California
District Court Case Nos. 5:21-cv-2777, 5:21-md-2985, and 5:21-md-3001

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA AND AMERICAN CIVIL LIBERTIES UNION, IN SUPPORT OF PLAINTIFFS-APPELLEES

Jacob A. Snow
Nicolas A. Hidalgo
Nicole A. Ozer
Shilpi Agarwal
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org
nhidalgo@aclunc.org
nozer@aclunc.org
sagarwal@aclunc.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
jgranick@aclu.org

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, Amici Curiae state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

FEDERAL STATUTES

STATE STATUTES & CONSTITUTIONS

OTHER AUTHORITIES

Brooke Auxier et al., *Americans' attitudes and experiences with privacy policies and laws*, PEW RESEARCH CENTER (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ 23

Business Guidance: Privacy and Security, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/privacy-security 24

California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App, FEDERAL TRADE COMMISSION (Jan. 11, 2012) https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo 18

Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in data breach*, THE GUARDIAN (Mar. 17, 2018) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election 20

Charge of Discrimination, Department of Housing and Urban Development (Mar. 28, 2019) https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.....21

Craig Silverman & Ryan Mac, *Facebook Gets Paid*, BUZZFEED NEWS (Dec. 10, 2020) https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam 22

Editorial, *Fair Lending and Accountability*, NEW YORK TIMES (Sep. 7, 2011) https://www.nytimes.com/2011/09/08/opinion/fair-lending-and-accountability.html 22

Emma Fletcher, *Social media a gold mine for scammers in 2021*, FEDERAL TRADE COMMISSION (Jan. 25, 2022) https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021 23

FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads, FEDERAL TRADE COMMISSION (May 25, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.....24

John Paul Strong, *Target Subprime Credit Using Facebook and Paid Search,* STRONG AUTOMOTIVE MERCHANDISING (Apr. 14, 2019) https://strongautomotive.com/target-subprime-credit-facebook-paid-search/.....22

Joseph Cox*, How the U.S. Military Buys Location Data from Ordinary Apps*, MOTHERBOARD TECH BY VICE (Nov. 16, 2020) https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x 18

Joseph Turow et al., *Americans Can't Consent to Companies' Use of Their Data*, U. PENN. ANNENBERG SCHOOL FOR COMMS. (2023) https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf 23

Julia Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, NEW YORK TIMES (Apr. 6, 2023) https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html.....21

Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (Jul. 17, 2018) https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates 19

Nicole Ozer & Chris Conley, *After the Facebook Privacy Debacle, It's Time for Clear Steps to Protect Users*, ACLU (Mar. 23, 2018) https://www.aclu.org/news/privacy-technology/after-facebook-privacy-debacle-its-time-clear-steps-protect 20

Nik Froehlich, *The Truth In User Privacy And Targeted Ads*, FORBES (Feb. 24, 2022) https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=14a71796355e.....17

Olivia Solon & Cyrus Farivar, *Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools*, NBC NEWS (May 9, 2019) https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.....18

Ruslana Lishchuk, *Digital Footprint Facts: How Companies Collect Your Data*, MACKEEPER (Aug. 19, 2019) https://mackeeper.com/blog/data-collection-targeted-ads/. 17

STATEMENT OF INTEREST

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Northern California (together with ACLU "Amici") is the Northern California affiliate of the ACLU. The ACLU and its affiliates share a longstanding commitment to freedom of speech and digital rights. In California, our Technology and Civil Liberties Program works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil liberties and civil rights. Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court, this Court, and other federal courts in cases related to free speech and freedom of association, including exercise of those rights online. *See, e.g., Reno v. ACLU*, 521 U.S. 844 (1997) (counsel); *Fair Hous. Council of San Fernando Valley v. Roommates.com*, *LLC*, 521 F.3d 1157 (9th Cir. 2008) (amici); *Gonzalez v. Google LLC*, 598 U.S. 617 (2023) (amici); *Twitter, Inc., v. Taamneh*, *et al*., 598 U.S. 471 (2023) (amici).

SOURCE OF AUTHORITY TO FILE

Amici sought consent from counsel for all parties and none oppose the filing of this brief. *See* Fed. R. App. P. 29(a)(2).

FED. R. APP. P. 29(a)(4)(E) STATEMENT

Amici declare that:

1. no party's counsel authored the brief in whole or in part;
2. no party or party's counsel contributed money intended to fund preparing or submitting the brief; and
3. no person, other than Amici, their members, or their counsel, contributed money intended to fund preparing or submitting the brief.

INTRODUCTION & SUMMARY OF ARGUMENT

The lower court erred when it interpreted Section 230 of the Communications Act ("Section 230") too expansively by finding that Section 230 immunized platforms for sharing user data. The lower court's improper ruling threatens to undermine consumer protection and privacy regulations and puts the public at greater risk of abusive and overreaching data collection and sharing practices.

The immense expressive potential of the Internet has—at least in part—been realized. Today, electronic devices and Internet services mediate nearly every aspect of life. This world presents opportunities, but also presents new risks, as technology companies build businesses based on comprehensive consumer profiles that can expose people to harm. Section 230 provides vital protections for platforms publishing third-party content—including controversial or offensive content. But the statute "was not meant to create a lawless no-man's-land on the Internet." *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1165 (9th Cir. 2008).

Here, Plaintiffs bring a variety of claims related to simulated casino machine games that are offered on Defendants' respective app stores. The district court categorized these claims into three separate "theories." In this brief, Amici address

the district court's analysis of only one of those theories.[1] Plaintiffs allege that the platforms give app developers access to "big data" and data analytics tools that identify, target, and exploit consumers prone to addictive behaviors, and enable developers to update their apps with targeted content designed to keep addicted players spending money. *In re Apple Inc. App Store Simulated Casino-Style Games Litig*., 625 F.Supp.3d 971, 974–76 (N.D. Cal. 2022) (the opinion below) ("*In re Casino Games*"). This practice, they allege, violates state unfair competition law. *Id*. at 976–96.

With respect to this theory relating to data sharing, the district court erred in holding that the "sharing of [big] data" with app developers is properly treated as a "classic editorial role"—and thus immunized by Section 230—when users did not share that data voluntarily, much less for the purpose of publication. *In re Casino Games*, 625 F.Supp.3d. at 995. Some uses of data by platforms are closely entwined with the acts of publishing, editorializing, or distributing content. But not all. As they browse the web, use various apps, and go about their lives making use of technology, people are constantly monitored. The data generated by this monitoring—which Amici call "surveillance data"—is collected nearly invisibly,

[1] Plaintiffs' Principal Brief focuses on a third theory of liability—that the platforms were not protected by Section 230 when they brokered gambling transactions in violation of state law—and only briefly discusses the two theories Amici address here. Amici submit this brief to elaborate on how the district court's analysis raises important questions about the proper scope of Section 230.

and many people have no idea that their devices are watching them, collecting information about them, and potentially sharing that information with others.

The collection and sharing of surveillance data should fall outside of Section 230's immunity for a simple reason: users do not "provide" it to the platform with the intention of having it posted online, as Section 230 immunity requires. Rather, the platform often invisibly collects and shares it. If users are informed at all, it is frequently in vague, legalistic privacy policies or other material that fail to provide real people with the ability to understand—let alone control—how their information is collected and shared. This vast collection and sharing of surveillance data is detached from the purposes of Section 230, which was intended to support the Internet as a forum for public discourse. Where the relevant user did not share the information with the platform in order to have it published online, it is improper for Section 230 immunity to apply.

The district court's broad immunization of data sharing between platforms and app developers could imperil important privacy laws that offer people necessary protections and control over how their data is collected, shared, and used. Section 230's immunity for publishers of third-party content is not, and must not be allowed to be used as, a shield against all grounds for platform liability.

ARGUMENT

I. The District Court Erred in Holding That Sharing of Surveillance Data Was Automatically Immunized by Section 230.

With respect to the sharing of surveillance data, the district court's expansive interpretation of Section 230's immunity was incorrect. Section 230 immunizes platforms for publishing content provided by third parties. It does not, however, shield them when the content was not provided by a third party with the intention of having it published online. Nor does it shield them from liability for their own content separate and apart from their publishing or speaking functions.

In light of the numerous laws regulating the collection and sharing of personal data, these distinctions are critical. If allowed to stand, the district court's interpretation of Section 230 immunity imperils the enforcement of these important privacy laws.

A. Section 230 Immunity Does Not Extend to Platforms' Own Content or Conduct, Nor When they Publish Data that Was not Provided by a Third Party.

None of Defendants dispute the basic principles of Section 230. That is, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). Accordingly, Section 230 immunity applies to "(1) a provider or user of an interactive computer service (2) whom a plaintiff

seeks to treat . . . as a publisher or speaker (3) of information provided by another information content provider." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009).

Whether Section 230 immunity applies often turns on the second factor: whether the plaintiff seeks to hold the defendant liable as a "publisher." "Publishing encompasses any activity that can be boiled down to deciding whether to exclude materials that third parties seek to post online." *Gonzalez,* 2 F.4th at 892 (cleaned up) (*citing Roommates.com*, 521 F.3d at 1170–71); *see also Barnes*, 570 F.3d at 1102 ("[P]ublication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content"). When the gravamen of a plaintiff's complaint seeks to hold the service provider vicariously liable for the publication of third-party content, Section 230 immunity applies.

Much regular Internet business conduct, however, cannot be considered publishing. Thus, if the platforms' own conduct is allegedly unlawful, Section 230 immunity does not apply. For example, in *Roommates.com,* plaintiffs accused a housing website operator of violating the Fair Housing Act and other state laws. The Court found that Roommates.com's "own acts—posting [a] questionnaire [that induced third parties to express illegal preferences] and requiring answers to it—are entirely its own doing and thus [S]ection 230 of the CDA does not apply to them." 521 F.3d at 1165.

In another case, online rental accommodations platform HomeAway.com argued that an ordinance prohibiting short-term rentals in Santa Monica was preempted by Section 230. *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 679–80 (9th Cir. 2019). The Court concluded that the ordinance in question regulated the platform's own conduct by prohibiting it from processing transactions for unlawful properties, but it did not impose on the platform a duty to "monitor third-party content." *Id*. at 682. Because of this, the Court concluded that Section 230 immunity did not apply. The Court expressly noted that Internet companies must, "like their brick-and-mortar counterparts[,] . . . comply with any number of local regulations concerning, for example, employment, tax, or zoning." *Id*. at 683.

Thus, when the challenged conduct is not publishing or speaking, or where the illegality is based on content created by the platform itself, Section 230 does not apply. *See Doe v. Internet Brands*, *Inc.*, 824 F.3d 846, 850–51 (9th Cir. 2016) (finding that plaintiff's "failure to warn" claim did not inherently require the court to treat the platform as a publisher); *Barnes*, 570 F.3d at 1107 (finding that Section 230 did not immunize Yahoo where plaintiff "does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract"); *Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 137–38 (4th Cir. 2019) (finding that Section 230 did not immunize platform from tort product

liability).

A platform can also be held liable for hosting third-party content where its own behavior materially contributes to the alleged illegality of that content. "In other words, a website helps to develop unlawful content, and thus falls within the exception to [S]ection 230, if it contributes materially to the alleged illegality of the conduct." *Roommates.com*, 521 F.3d at 1168 (finding that the defendant contributed to allegedly illegal discrimination on its platform by requiring the collection of discriminatory information). Similarly, in *Liapes v. Facebook, Inc.*, the California First Circuit Court of Appeals held that immunity did not apply when Facebook required users to disclose their age and gender, then allowed advertisers to exclude certain ages and genders from economic opportunities using Facebook's own targeted advertising tools. 313 Cal.Rptr.3d 330, 346–47 (Cal. Ct. App. First. Dist. Sep. 21, 2023). Facebook's actions, *Liapes* explains, materially contributed to the content's alleged unlawfulness. *Id.* at 346.

B. The Collection and Sharing of Surveillance Data Here Is Not Covered by Section 230 Immunity.

Here, the conduct that Plaintiffs challenge is the platforms' monitoring of game activity and sharing of that information with app developers. The information collected by the platforms and shared with the apps is allegedly obtained by monitoring users as they play the games. Apple Complaint ¶ 91;

Facebook Complaint ¶ 81; Google Complaint ¶ 88. It is not provided by those users to the platforms for the purpose of publishing or sharing it with others. According to the complaints, the data is an important tool used by the app developers to bring in and retain players and to thereby generate revenue. The complaints also allege that this tool targets and exploits vulnerable and gambling-addicted players. Apple Complaint ¶ 166; Facebook Complaint ¶ 153; Google Complaint ¶ 157. According to a Securities and Exchange Commission filing by one of the app developers, the data collected and shared by the platforms also allows it to "estimate the expected value of a player and adjust [its] user acquisition spend to a targeted payback period." Apple Complaint ¶ 75; Facebook Complaint ¶ 71; Google Complaint ¶ 72. "Since all payment processing occurs through third-party platforms, the Illegal Slot companies have limited access to personal user data unless players login through Apple or otherwise sign up for loyalty programs." Apple Complaint ¶ 91; Facebook Complaint ¶ 81; Google Complaint ¶ 88. As another app developer explains, "[s]ubstantially all of our revenue is generated by players using [Apple, Facebook, Google, and Amazon]. Consequently, our expansion and prospects depend on our continued relationships with these providers . . ." Apple Complaint ¶ 75; Facebook Complaint ¶ 71; Google Complaint ¶ 72.

Based on these allegations, the complaints claim that Apple, Facebook, and

Google have engaged in unfair business practices by "working together" with the app developers to target and exploit people and to "operate their online slot machines outside the bounds of licensing, regulation, and tax policy." Apple Complaint ¶ 166; Facebook Complaint ¶ 153; Google Complaint ¶ 157.

The district court summarized these claims as follows: "Plaintiffs hold the Platforms liable for sharing data with the social casino app developers to make their illegal product more appealing and addicting." *In re Casino Games*, 625 F.Supp.3d at 995. With respect to this theory of liability, the district court concluded that "[p]roviding social casino developers with big data is like an editor providing edits or suggestions to a writer" and that "the Platforms sharing of data is fairly seen as a classic editorial role" *Id*. (analogizing to *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), which held that a platform's minor edits to third-party content before publishing it was protected by Section 230 immunity).

This holding was wrong for two reasons. First, the user data obtained by the app developers does not appear to have been "provided" to the platforms as Section 230 uses that term. And second, the platforms appear to have created, or made a material contribution to the creation of, the surveillance data at issue.

1. The User Data Was Not Provided for the Purpose of Having it Posted Online.

For Section 230 immunity to apply, the circumstances must reflect that the

third-party content was "tendered . . . for posting online." *Roommates.com*, 521 F.3d at 1170–71. As *Roommates.com* explained, "if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination." *Id.* at 1171.

This Court offered a detailed rationale for this holding in *Batzel v. Smith*. There, the author (Smith) of the third-party content (an allegedly defamatory email) maintained that he never "imagined [his] message would be posted on an international message board or [he] never would have sent it in the first place." *Batzel*, 333 F.3d at 1032. And Section 230 immunity, the Court explained, does not apply when interactive computer services "knew or had reason to know that the information provided was not intended for publication on the Internet."[2] *Id.* at 1033–34.

In so holding, the Court noted that a different result would have negative impacts on people's ability to use the Internet privately. Smith, the defendant in

[2] *Batzel* added an important proviso regarding the Court's inquiry into the requisite level of intention for Section 230 immunity to apply. The Court highlighted the risk that "posting of information on the Internet and other interactive computer services would be chilled, as the service provider or user could not tell whether posting was contemplated [by the individual user]." *Batzel*, 333 F.3d at 1034. Therefore, "the focus should be not on the information provider's intentions or knowledge when transmitting content but, instead, on the service provider's or user's reasonable perception of those intentions or knowledge." *Id.*

Batzel, was emphatic that he was "simply sending a private email" and that "he would not have sent the message if he had known it would be sent through the listserv." *Id.* at 1034. "Users of the Internet," the Court wrote, "are likely to be discouraged from sending e-mails for fear that their e-mails may be published on the web without their permission." *Id.* Indeed, connecting immunity to people's expectations has another salutary effect: ensuring that communications to which immunity attaches reflect the care a person uses "when [they] know[] those words will be widely read." *Id.*

In contrast, when a user of a social media platform plainly *intends* to make a post, including posts that violate the law, Section 230 immunity does apply to the platform's hosting of that content. A claim against the social media platform for defamation, or even invasion of privacy, that is based on the content of a user's post would therefore trigger immunity. *See, e.g.*, *Caraccioli v. Facebook, Inc.*, 700 Fed.App'x 588, 590 (9th Cir. 2017) (affirming dismissal of various torts when Facebook acted as the "republisher" of material posted by a third party).

Here, the district court overshot the limits of Section 230's immunity. The data allegedly gathered through the platforms' monitoring of users and shared with app developers was not provided by users in circumstances reflecting that the users "[sought] to post [the information] online." *See Gonzalez,* 2 F.4th at 892. Rather, according to the complaint, the platforms and the app developers "monitor

the game activity and use the collected data to increase user spending." Apple Complaint ¶ 91; Facebook Complaint ¶ 81; Google Complaint ¶ 88. Those users never sought to provide or share the details of their interactions within an app online; indeed, they were likely unaware that their clicks, movements, and payments within the app were being tracked at all by the platforms. Many users of social media purposely provide their posts, photos, achievements, successes, and disappointments to platforms for publication, with the intent to share them with their online communities. But that purposeful conduct is absent where platforms gather surveillance data about users through the nearly invisible tracking systems that pervade the online environment.

Batzel's concern—that, under an erroneous interpretation of Section 230, private content could spread across the Internet—takes on special resonance today. If every detail of people's interaction with apps and websites on the Internet is subject to surreptitious monitoring, unfettered data collection, and unrestrained sharing, even when these actions are prohibited by law, privacy on the Internet will be significantly diminished. Section 230 was not intended to lead to this result. Quite the contrary, the longstanding limits on Section 230 immunity—going back to *Batzel*—rely on the notion that respecting people's privacy interests can lead to a richer and healthier community of speakers.

2. The Platforms Likely Made a Material Contribution to the Content of the Surveillance Data.

Even if this Court were to conclude that surveillance data was shared for publication, Section 230 still does not apply to Defendants' sharing of surveillance data because the platforms likely made a material contribution to the content. *See Roommates.com*, 521 F.3d at 1168. Here the platforms are alleged to have provided "marketing and analytics" services to app developers that include infrastructure that collects extensive information about how people use the apps. Facebook Complaint ¶ 78; *see also* Apple Complaint ¶ 87 ("Apple provides marketing guidance" and other tools to "target consumers and maximize revenue"); Google Complaint ¶ 85 (same allegations about Google). Once that information is collected, the platforms offer services to app developers to analyze it, ostensibly to help developers improve their apps, reach new users, and increase engagement from existing users. Apple Complaint ¶¶ 80–102; Facebook Complaint ¶¶ 75–94; Google Complaint ¶¶ 76–97. In other words, the *platforms* make the decision to collect surveillance data in the first place, and then the *platforms* also choose what specific surveillance data to collect and how to share it.

Collecting information can certainly constitute a material contribution to content. In *Roommates.com*, the platform contributed to the content by "developing the discriminatory questions, discriminatory answers, and

discriminatory search mechanism." 521 F.3d at 1172. The Court accordingly found Section 230 did not immunize Roommates.com's conduct because, while the questionnaire data originated with users, Roommates.com materially contributed to its development and illegal use by soliciting the information. *Id*. Similarly, the California Court of Appeals in *Liapes* clarified that Section 230 immunity does not apply where a platform is "responsible, in whole or in part, for the creation or development" of the content at issue, finding that Facebook had contributed to the allegedly illegal conduct where it had required its users to disclose certain information before they could use its services. 313 Cal.Rptr.3d at 345–46.

While the surveillance data itself may represent information associated with user activity, the Section 230 analysis must consider that it is the platform-created version of that data, which may exist only because the platforms decided to collect it. Section 230 foundationally protects the content only of third parties; but when platforms design and develop a surveillance infrastructure, they make a material contribution to the content of the resulting surveillance data. Section 230 immunity, in those instances, does not apply.

C. Construing Section 230's Immunity to Reach All Sharing of Surveillance Data Could Imperil Laws Giving People Control Over How and Whether They Are Tracked Online.

Extending the scope of Section 230's immunity to reach all collection and

sharing of people's personal data could also undermine important state and federal privacy laws under the guise of protecting the Internet as a forum for free speech.

1. *Privacy Laws—Including Those That Limit the Use of Information for Targeted Advertising—Are Vitally Important.*

Electronic devices and services are now necessary to participate in modern life—they have become essential to connect and communicate with others, to seek healthcare and education, and even to use public or private transportation. *See Carpenter v. U.S.*, 138 S.Ct. 2206, 2220 (2018) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."). But these same electronic devices and services also enable businesses to collect, share, and use personal data to track people's movements, habits, interests, associations, and much more.[3] In the wider digital economy, information associated with people's online and offline

[3] *See* Nik Froehlich, *The Truth In User Privacy And Targeted Ads*, FORBES (Feb. 24, 2022) https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=14a71796355e; Ruslana Lishchuk, *Digital Footprint Facts: How Companies Collect Your Data*, MACKEEPER (Aug. 19, 2019) https://mackeeper.com/blog/data-collection-targeted-ads/.

activities is increasingly collected,[4] bought,[5] sold,[6] and stolen,[7] as well as used for purposes of which most people are unaware and may find difficult to fathom.[8] Many privacy laws aim to stop the harmful consequences of these data flows by limiting collection and use of personal information at the source.

Privacy laws protect people from a variety of social harms. Health insurance companies, for example, often use algorithms to predict health-care costs and increase people's premiums for those categorized as "higher risk." Those

---

[4] *See, e.g.*, *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent,* FEDERAL TRADE COMMISSION (Jun. 5, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information.

[5] *See, e.g.*, Joseph Cox*, How the U.S. Military Buys Location Data from Ordinary Apps*, MOTHERBOARD TECH BY VICE (Nov. 16, 2020) https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[6] *See, e.g.*, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, FTC PRESS RELEASE (Aug. 29, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[7] *See, e.g.*, Chris Mills, *Equifax is already facing the largest class-action lawsuit in US history*, BGR (Sep. 8, 2017) https://bgr.com/business/equifax-hack-lawsuit-class-action-how-to-join/.

[8] Olivia Solon & Cyrus Farivar, *Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools*, NBC NEWS (May 9, 2019) https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371; *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App*, FEDERAL TRADE COMMISSION (Jan. 11, 2012) https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo.

algorithms are trained on "hundreds of millions of Americans[']" personal details, including "race, education level, TV habits, marital status, net worth, . . . post[s] on social media," timing of bill payments, online orders, and more.[9] Individuals could be tagged by an algorithm as "higher risk" for medical costs just because they might get pregnant, are deemed to be at risk for depression, or are members of a minority community that may be statistically more likely to live in poorer or more dangerous neighborhoods.[10]

Similarly, data brokers compile large databases of personal data and sell access to third parties who can use those databases to target specific groups of people, including religious minorities. For example, in 2020 the U.S. military purchased "location and movement data" that data brokers compiled from apps targeted at Muslim users.[11] The government's discriminatory focus on Muslim

---

[9] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (Jul. 17, 2018) https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[10] *Id*.

[11] Johana Bhuiyan, *Muslims reel over a prayer app that sold user data: 'A betrayal from within our own community'*, L.A. TIMES (Nov. 23, 2020) https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors.

activity was a "serious threat to privacy and religious freedom" and an example of "unconstitutional surveillance."[12]

Vast repositories of personal data also risk corroding the democratic process. In the 2016 U.S. presidential election, the infamous data analytics firm Cambridge Analytica collected information from tens of millions of Facebook accounts to generate personalized voter profiles and target political messaging.[13] The revelation of Cambridge Analytica and Facebook's actions caused an international controversy and prompted numerous calls for Facebook to reform its privacy practices.[14] This extraction of millions of people's personal data was possible only because of Facebook's permissive information sharing policies[15] and Cambridge Analytica's exploitation of the lack of privacy protections in place.

Privacy laws are also critical to protecting people from the various threats related to the collection and sharing of personal data, including the use of personal

---

[12] Gabrielle Canon, *ACLU files request over data US collected via Muslim app used by millions*, THE GUARDIAN (Dec. 3, 2020) https://www.theguardian.com/us-news/2020/dec/03/aclu-seeks-release-records-data-us-collected-via-muslim-app-used-millions.

[13] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in data breach*, THE GUARDIAN (Mar. 17, 2018) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[14] Nicole Ozer & Chris Conley, *After the Facebook Privacy Debacle, It's Time for Clear Steps to Protect Users*, ACLU (Mar. 23, 2018) https://www.aclu.org/news/privacy-technology/after-facebook-privacy-debacle-its-time-clear-steps-protect.

[15] *Id*.

data in targeted behavioral advertising. While the Cambridge Analytica scandal is the most infamous, advertising platforms that rely on detailed profiles of people's online and offline behavior to target advertisements—sometimes called "surveillance capitalism"[16]—are the sources of significant public concern, and rightly so. It is invasive and unnerving to be bombarded with targeted advertisements based on your online or offline activity.[17] Companies may target their advertisements in a discriminatory way, based on age, sex, race, or ethnicity, resulting in certain groups receiving information about opportunities that others do not.[18] And the products in behaviorally-targeted ads are often lower quality and higher priced.[19] Targeted ads also enable outright scammers to proliferate and

---

[16] While the label "surveillance capitalism" has earlier roots, it came into common parlance through Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

[17] Brian X. Chen, *Are Targeted Ads Stalking You? Here's How to Make them Stop*, NEW YORK TIMES (Aug. 15, 2018) https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html ("Even if you end up ordering the watch, the ads continue trailing you everywhere. They're stalker ads.").

[18] For example, in 2019 the Department of Housing and Urban Development charged Meta with housing discrimination based on its targeted advertising. Charge of Discrimination available at https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

[19] Julia Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, NEW YORK TIMES (Apr. 6, 2023) https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html (summarizing Schnadower Mustri, Eduardo and Adjerid, Idris and Acquisti, Alessandro, Behavioral *Advertising and Consumer Welfare: An Empirical Investigation* (Mar. 23, 2023) available at SSRN: https://ssrn.com/abstract=4398428).

financially harm people.[20] A 2018 investigation described how advertisers could make millions by targeting consumers with deceptive ads.[21] Examples abound of predatory advertisements deliberately targeting vulnerable people, such as subprime lenders targeting financially vulnerable consumers[22] (which often target victims based on their race[23]) or seniors with direct investment scams.[24] The

---

[20] Craig Silverman & Ryan Mac, *Facebook Gets Paid*, BUZZFEED NEWS (Dec. 10, 2020) https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam; Andrew Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic*, TIME (Dec. 18, 2020) https://time.com/5921820/facebook-shopping-scams-holidays-covid-19/; Jason Koebler, *Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons*, 404 MEDIA (Aug. 23, 2023) https://www.404media.co/instagram-ads-illegal-content-drugs-guns-hackers/.

[21] Zeke Faux, *How Facebook Helps Shady Advertisers Pollute the Internet*, BLOOMBERG.COM (Mar. 27, 2018) https://www.bloomberg.com/news/features/2018-03-27/ad-scammers-need-suckers-and-facebook-helps-find-them.

[22] John Paul Strong, *Target Subprime Credit Using Facebook and Paid Search,* STRONG AUTOMOTIVE MERCHANDISING (Apr. 14, 2019) https://strongautomotive.com/target-subprime-credit-facebook-paid-search/.

[23] Jacob Rugh & Douglas Masset, *Racial Segregation and the American Foreclosure Crisis*, 75(5) AMERICAN SOCIOLOGICAL REVIEW 629, 630 (Oct. 2010), available at http://www.asanet.org/wp-content/uploads/savvy/images/journals/docs/pdf/asr/Oct10ASRFeature.pdf; *see also* Editorial, *Fair Lending and Accountability*, NEW YORK TIMES (Sep. 7, 2011) https://www.nytimes.com/2011/09/08/opinion/fair-lending-and-accountability.html ("Studies by consumer advocates found that large numbers of minority borrowers who were eligible for affordable, traditional loans were routinely steered toward ruinously priced subprime loans that they would never be able to repay.")

[24] Jeremy B. Merrill & Kozlowska Hanna, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives*, QUARTZ (Nov. 19, 2019) https://qz.com/1751030/facebook-ads-lured-seniors-into-giving-savings-to-metals-com.

Federal Trade Commission ("FTC") has gone so far as to recommend that people opt out of targeted advertising to protect themselves from scammers.[25] But even though opting out is possible in some cases, the pervasiveness of online tracking makes it functionally impossible for consumers to opt out of all targeted advertisements.

The public understands that the stakes are high. Poll after poll shows that Americans overwhelmingly favor stronger government regulation of how companies use people's information, and they want more control over what marketers can learn about them online.[26]

2. Misreading Section 230 Immunity to Cover Collection and Sharing of Surveillance Data Could Threaten Important Privacy Protections Under State and Federal Law.

Regulators and legislators have taken important steps to enforce existing

---

[25] Emma Fletcher, *Social media a gold mine for scammers in 2021*, FEDERAL TRADE COMMISSION (Jan. 25, 2022) https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021 ("Here are some ways to help you and your family stay safe on social media: . . . Check if you can opt out of targeted advertising.").

[26] Brooke Auxier et al., *Americans' attitudes and experiences with privacy policies and laws*, PEW RESEARCH CENTER (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ (75% of Americans strongly favor more government regulation of consumer data); Joseph Turow et al., *Americans Can't Consent to Companies' Use of Their Data*, U. PENN. ANNENBERG SCHOOL FOR COMMS. (2023) https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf at 13 (91% want to have control over what marketers can learn about them).

laws and to pass new privacy laws. Holding that Section 230 immunity reaches all sharing of surveillance data could threaten these critical privacy protections.

For example, state and federal prohibitions on unfair and deceptive practices require companies to keep the promises they make to consumers, including representations made in connection with what information is collected from consumers and how it will be used.[27] In 2022, Twitter settled an FTC investigation based on allegations that the company had asked users to provide their personal information for security purposes, but used that information to instead sell targeted ads.[28] Other cases settled by federal and state privacy-enforcement authorities likewise demonstrate the importance of unfair and deceptive business practices laws in enforcing privacy rights and limiting the harms of an online environment awash in people's personal information.[29]

---

[27] *Business Guidance: Privacy and Security*¸ FEDERAL TRADE COMMISSION ("If your company makes privacy promises–either expressly or by implication–the FTC Act requires you to live up to those claims."), https://www.ftc.gov/business-guidance/privacy-security.

[28] *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads*, FEDERAL TRADE COMMISSION (May 25, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

[29] *See, e.g., Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*¸ CALIFORNIA OFFICE OF THE ATTORNEY GENERAL (Aug. 24, 2022) https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement (settling claims under the CCPA and California's unfair competition law based on failure to honor settings that allow people to control whether they are

In addition, state constitutional privacy protections—like the California constitutional right to privacy protecting against the collection and sharing of personal information by both government and business interests—impose important limits on invasive business models that rely on the exploitation of personal information. Passed in 1972, a principal aim of the privacy amendment in Article I, Section 1 of the California Constitution is "to limit the infringement upon personal privacy arising from the . . . increasing collection and retention of data relating to all facets of an individual's life." *White v. Davis*, 13 Cal.3d 757, 761 (1975) (en banc); *see also In re Facebook, Inc. Consumer Privacy User Profile Litigation*, 402 F.Supp.3d 767, 777 (N.D. Cal. 2019) (finding that an Article I, Section 1 privacy claim was adequately pled on the basis of "Facebook [giving] app developers and business partners [people's] sensitive information on a widespread basis."); *Brooks v. Thomson Reuters Corp*., No. 21-cv-01418, 2021 WL 3621837, *8 (N.D. Cal. Aug. 16, 2021) (The California Constitution "expressly enshrines the right to privacy" and that "[t]he unauthorized dissemination of virtually every piece of Plaintiffs' personal information . . . may constitute a severe invasion of privacy.").

---

monitored as they shop); *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FEDERAL TRADE COMMISSION (Jul. 24, 2019) https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

Other more recent state laws such as the California Consumer Protection Act ("CCPA") and Colorado Privacy Act ("CPA") give users some control over personal information in the hands of private actors, including how their information is used as part of the behavioral advertising industry. The CCPA, passed in 2018, added statutory rights for Californians to access the information companies hold about them, delete their information, and opt out of the sale of their personal information.[30] The CCPA requires companies to inform consumers that their information is being collected at the time it is collected[31] and gives consumers the right to opt out of the use of their information for behavioral advertising.[32] The law also requires that companies provide on their websites a clear and conspicuous link that enables people to exercise those opt-out rights.[33] The CPA provides similar protections for Colorado consumers.[34]

Privacy laws that protect people's personal information from being collected, used, and shared for targeting advertising without their consent can be

[30] Cal. Civ. Code §§ 1798.110 (right to access), 1798.105 (right to delete), 1798.120 (right to opt out of sale of personal information, including in targeted advertising).
[31] Cal. Civ. Code §§ 1798.100(a).
[32] Cal. Civ. Code § 1798.140(ah)(1).
[33] Cal. Civ. Code § 1798.135(a)(1).
[34] Colorado Revised Statutes § 6-1-1306(1)(a)(I)(opt out rights overall); 6-1-1306(1)(a)(I)(A) (right to opt out of processing of personal data for the purposes of "[t]argeted advertising"); 6-1-1306(1)(a)(III) (clear and conspicuous method to exercise rights).

essential to protect rights, safety, and democracy in the digital age. This Court should preserve Section 230's textual limits and the current law in this Circuit and make it clear that unlawful collection, sharing, and use of data that is not provided by a third party for publication, but rather constructed by the platform itself, is outside Section 230's immunity.

CONCLUSION

The Court should hold that platforms are not immunized by Section 230 for sharing of surveillance data with app developers.

Respectfully submitted,

Dated: November 1, 2023

/s/ *Jacob A. Snow*
Jacob A. Snow
Nicolas A. Hidalgo
Nicole A. Ozer
Shilpi Agarwal
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org
nhidalgo@aclunc.org
nozer@aclunc.org
sagarwal@aclunc.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street,
San Francisco, CA 94111
jgranick@aclu.org

Attorneys for Amici Curiae

CERTIFICATE OF SERVICE FOR ELECTRONIC FILING

I hereby certify that on November 1, 2023, I electronically filed the foregoing Amici Curiae Brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the CM/ECF system, which effects service upon all counsel of record.

Dated: November 1, 2023

/s/ *Jacob A. Snow*

Jacob A. Snow
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org

Attorney for Amici Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief contains 5,848 words, excluding the items exempted by Fed. R. App. P. 32(f), and complies with the length specifications set forth by Fed. R. App. P. 29(a)(5). I further certify that this brief was prepared using 14-point Times New Roman font, in compliance with Fed. R. App. P. 32(a)(5) and (6).

Dated: November 1, 2023

/s/ Jacob A. Snow

Jacob A. Snow
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org

Attorney for Amici Curiae