No. 23-2969

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC,

Plaintiff-Appellee,

v.

ROB BONTA, in his official capacity as
ATTORNEY GENERAL OF THE STATE OF CALIFORNIA,

Defendant-Appellant.

On Appeal from the United States District Court
For the Northern District of California
No. 5:22-cv-08861-BLF

Hon. Beth Labson Freeman, District Judge

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA IN SUPPORT OF PLAINTIFF-APPELLEE

Jacob A. Snow
Nicolas A. Hidalgo
Chessie Thacher
Nicole A. Ozer
Matthew T. Cagle
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org

Vera Eidelman
Elizabeth Gyori
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad St., 18 Fl.
New York, NY 10004
veidelman@aclu.org

Counsel for Amici Curiae

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

Statutes

Other Authorities

Constitutional Provisions

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization. The ACLU of Northern California is an affiliate of the ACLU. Both organizations are dedicated to defending the principles embodied in the Constitution and our nation's civil rights laws. Both have opposed unfounded First Amendment challenges to consumer privacy laws. *See, e.g.*, *ACA Connects v. Frey*, 471 F. Supp. 3d 318 (D. Me. 2020) (amicus); *ACLU v. Clearview AI*, No. 2020-CH-04353 (Ill. Cir. Ct. Aug. 27, 2021) (counsel); *Stark v. Patreon*, No. 22-cv-03131 (N.D. Cal. Dec. 20, 2023), Dkt. No. 95-1 (amicus). Both have also defended the rights to speak and publish online. *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844 (1997) (counsel); *Doe v. Harris*, 772 F.3d 563 (9th Cir. 2014) (counsel); *NetChoice, LLC v. Paxton*, No. 22-555 (petition for cert. filed Dec. 15, 2022) (amicus). As fervent defenders of speech and privacy, both organizations have a strong interest in the proper resolution of this case.

[1] Amici sought consent from counsel for all parties and none oppose the filing of this brief. *See* Fed. R. App. P. 29(a)(2). Amici declare that no party or party's counsel authored the brief in whole or in part or contributed money intended to fund the preparation or submission of the brief, and that no one other than Amici, their members, or their counsel contributed money intended to fund preparation or submission of the brief.

INTRODUCTION & SUMMARY OF ARGUMENT

The California legislature largely framed the California Age-Appropriate Design Code Act ("CAADCA"), Cal. Civ. Code § 1798.99.28 et seq., as a consumer privacy law that would offer stronger privacy protections by default—a critical goal that legislatures can and should accomplish without violating the First Amendment. Yet the actual text of the law reveals a different regulation: one that expressly and impermissibly engages in content-based discrimination in the name of protecting consumer privacy and children. This law should be struck down. But amici respectfully urge the Court to decide the case narrowly, based on the text of the CAADCA, and ensure that the door remains open to sustaining other consumer privacy laws containing similar concepts in the future—including in California, where privacy is a fundamental, inalienable constitutional right. Cal. Const. art. I, § 1.

To that end, this brief begins by highlighting the necessity of privacy protections. It then identifies First Amendment doctrines relevant to the analysis of other laws containing similar concepts—including data minimization and requiring the highest privacy settings by default. Finally, this brief explains why the CAADCA itself is subject to, and fails, strict scrutiny.

Strong privacy laws are vitally important. Websites, platforms, and online services—many of which are necessary to participate in the modern world—collect,

use, share, and sell troves of personal information. Yet the businesses that operate these systems often do so without people's consent and in ways that people do not understand, expect, or want. They track us and profile us, including as we read and speak online; subject us to discrimination in healthcare, housing, and hiring; and make us vulnerable to scammers. Without stronger privacy laws, people of all ages will continue to be tracked, with wide-ranging impacts on individuals and society.

Privacy laws addressing these harms can satisfy First Amendment scrutiny. For example, where such laws regulate the collection or use of information by an entity that obtained the information in exchange for provision of a good or service, they can be subject to and survive intermediate scrutiny. This includes limits on the collection, use, and sharing of information from users accumulated—often surreptitiously—by online platforms. A law can also require the disclosure of factual, noncontroversial information—such as the fact that a user's geolocation is being monitored—so long as the requirement is reasonably related to preventing deceptive commercial transactions or otherwise enabling people to make informed consumer choices.

At the same time, laws are not subject to lower First Amendment scrutiny merely because they purport to protect consumer privacy or children. To the contrary, content-based bans or burdens on speech—like the CAADCA's prohibition on "[u]sing [any child's] personal information" in a way that "is materially detrimental"

to them, Cal. Civ. Code § 1798.99.31(b)(1), and its requirement that businesses assess any risk of exposing kids to "harmful, or potentially harmful, content," "contacts," "conduct" or "algorithms" "before" they are "accessed by children," *id.* § 31(a)(1)(B)(i)–(v), 31(a)(2)—must satisfy strict scrutiny to survive.

In passing the CAADCA, the California Legislature was understandably concerned with the privacy, wellbeing, and safety of children. But the Supreme Court has made clear time and again that, even where children are concerned, the government cannot regulate speech "solely to protect the[m] . . . from ideas or images that a legislative body thinks unsuitable for them." *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214–15 (1975). Nor can it limit adults' access to speech in the name of protecting children. The CAADCA fails on both counts.

This Court should affirm the district court's preliminary injunction while making clear that consumer privacy laws are often constitutional. The continued availability—and proper application—of First Amendment doctrines that do not require strict scrutiny are critical to ensuring that we can have privacy and free speech too.

ARGUMENT

I. Privacy protections are essential.

A. The collection, use, and sharing of personal information can be harmful.

Electronic devices and services have become essential to connect and communicate with others, and to access everything from healthcare and education to transportation. For most people, they are "indispensable to participation in modern society." *See Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018).

Yet the businesses behind these technologies often collect, share, and use personal information to track people's movements, habits, interests, associations, and much more.[2] In the wider digital economy, information associated with people's online and offline activities is increasingly collected,[3] bought,[4] sold,[5] stolen,[6] and

---

[2] *See* Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES (Feb. 24, 2022), https://perma.cc/6HEG-VPWM.

[3] *See, e.g.*, Press Release, Federal Trade Commission, FTC Will Require Microsoft to Pay $20 Million over Charges it Illegally Collected Personal Information from Children Without Their Parents' Consent (Jun. 5, 2023), https://perma.cc/U57Z-PEVP.

[4] *See, e.g.*, Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, MOTHERBOARD (Nov. 16, 2020), https://perma.cc/SC5F-TZWE.

[5] *See, e.g.*, Press Release, Federal Trade Commission, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://perma.cc/EN24-4WJE.

[6] *See, e.g.*, Chris Mills, *Equifax Is Already Facing the Largest Class-Action Lawsuit in U.S. History*, BGR (Sept. 8, 2017), perma.cc/5MSV-ATLC.

used for purposes that most people do not know about and may find difficult to fathom.[7] "The capacity of technology to find and publish personal information . . . presents serious . . . issues with respect to personal privacy and the dignity it seeks to secure." *Sorrell v. IMS Health Inc*., 564 U.S. 552, 579 (2011).

Children are no exception. They too use technology to learn, explore, and communicate.[8] And they too are tracked and experience privacy harms.[9]

In the digital age, privacy violations certainly include the improper disclosure of information that people would prefer to keep to themselves. But privacy harms equally arise from unwanted collection, aggregation, and use of personal information. Those activities can result in discrimination, financial harms, and burdens on free expression.

Consider the discriminatory harms when health insurance companies use algorithms trained on "hundreds of millions of Americans[']" personal details,

---

[7] 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), perma.cc/PCP5-LDXR.

[8] *See, e.g*., *Done Right, Internet Use Among Children Can Increase Learning Opportunities and Build Digital Skills*, UNICEF (Nov. 27, 2019), https://perma.cc/QRC6-WXJ4.

[9] Some privacy laws—like the federal Children's Online Privacy Protection Act ("COPPA")—properly aim to stop harmful consequences that can be unique to children, who, for example "may not appreciate the dangers in disclosing sensitive personal information to commercial entities." Gabe Rottman, *FTC Proposes Changes to Privacy Law That Collide with Free Speech*, ACLU (Sept. 26, 2012), https://perma.cc/B4EK-BZLP.

including "race, education level, TV habits, marital status, net worth . . . post[s] on social media," timing of bill payments, online orders, and more to categorize people as "higher risk."[10] This collection and use of personal information can lead to discriminatory harms like higher premiums for individuals just because they might become pregnant, are deemed at risk for depression, or are members of a minority community that may be statistically more likely to live in poorer neighborhoods.[11] Assumptions arising from big data can similarly result in denial of housing[12] or employment.[13]

The "surveillance capitalism"[14] business model of many companies, including the use of detailed profiles of people's online and offline behavior to target advertisements, can also facilitate discrimination and affect financial stability and economic opportunity. Companies sometimes target advertisements in a

---

[10] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—and it Could Raise Your Rates*, PROPUBLICA (Jul. 17, 2018), https://perma.cc/DQ23-LN4M.

[11] *Id*.

[12] Charge of Discrimination, *Facebook, Inc.*, FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://perma.cc/Q2AF-B7G5 (HUD complaint charging Meta with perpetuating housing discrimination in its advertisements).

[13] Clare Duffy & Carlotta Dotto, *People Are Missing Out on Job Opportunities on Facebook Because of Gender, Research Suggests*, CNN BUS. (June 12, 2023), https://perma.cc/KYY2-VW8M.

[14] 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).

discriminatory manner based on age, sex, race, or ethnicity, resulting in certain groups receiving information about opportunities that others do not.[15] Targeted advertisements can also push products that are worse and more expensive[16] and be used by outright scammers[17] seeking out financially vulnerable consumers[18] (often based on race[19]) and seniors.[20] In addition, it is invasive and unnerving to be

---

[15] For example, in 2019 the Department of Housing and Urban Development charged Meta with housing discrimination based on its targeted advertising. *See* Charge of Discrimination, *supra* note 12.

[16] Julia Angwin, Opinion, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, N.Y. TIMES (Apr. 6, 2023), https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html (summarizing Eduardo Schnadower Mustri, Idris Adjerid, & Alessandro Acquisti, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation* (Mar. 23, 2023), https://perma.cc/VJ3A-DKYP).

[17] Craig Silverman & Ryan Mac, *Facebook Gets Paid*, BUZZFEED NEWS (Dec. 10, 2020), https://perma.cc/WJN7-S2XQ; Andrew Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic*, TIME (Dec. 18, 2020), https://perma.cc/UX28-AUUT.

[18] John Paul Strong, *Target Subprime Credit Using Facebook and Paid Search,* STRONG AUTOMOTIVE MERCHANDISING (Apr. 14, 2019), https://perma.cc/XE96-ETXR.

[19] Jacob Rugh & Douglas Masset, *Racial Segregation and the American Foreclosure Crisis*, 75(5) AM. SOCIO. REV. 629, 630 (Oct. 2010), https://perma.cc/EAU6-C8VU; *see also* Editorial, *Fair Lending and Accountability*, N.Y. 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.").

[20] Jeremy B. Merrill & Kozlowska Hanna, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives*, QUARTZ (Nov. 19, 2019), perma.cc/GB7F-XM3H.

bombarded with advertisements based on records of your activities.[21] The Federal Trade Commission ("FTC") has recommended that people opt out of targeted advertising to protect themselves.[22] But the current pervasiveness of online tracking makes it functionally impossible to opt out entirely.

Finally, the collection of information can also discourage people from freely expressing themselves, accessing resources, and making connections online. Without privacy protections, people may be unwilling to discuss "sensitive, personal, controversial, or stigmatized content." *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007), *aff'd sub nom. ACLU v. Mukasey*, 534 F.3d 181 (3d. Cir. 2008).

B. Privacy regulations can prevent these significant harms and enable people to benefit from the full promise of technologies.

Consumer privacy laws can protect a variety of rights, including "the right to have sufficient moral freedom to exercise full individual autonomy, the right of an individual to define who he or she is by controlling access to information about him

[21] Brian X. Chen, *Are Targeted Ads Stalking You? Here's How to Make them Stop*, N.Y. 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.").

[22] Emma Fletcher, *Social Media a Gold Mine for Scammers in 2021*, FED. TRADE COMM'N (Jan. 25, 2022), perma.cc/GHU2-2DRG ("Here are some ways to help you and your family stay safe on social media: . . . Check if you can opt out of targeted advertising.").

or herself, and the right of an individual to solitude, secrecy, and anonymity." *U.S. W., Inc. v. FCC*, 182 F.3d 1224, 1234 (10th Cir. 1999).

Privacy laws do more than prevent harm. They also help to create spaces where people have the confidence to candidly communicate with friends, seek out advice and community, and engage with experts. This privacy can encourage advocates, activists, whistleblowers, dissidents,[23] and authors and other artists to speak out.[24]

Robust privacy protections can be particularly important for young people. They can make young people feel more comfortable navigating everything from body image concerns to depression. Laws that protect anonymity can enable "open discussion" that lowers "numbers of teenage pregnancy or sexually transmitted diseases." *Cyberspace, Commc'ns, Inc. v. Engler*, 55 F. Supp. 2d. 737, 749 (E.D. Mich. 1999). And giving young people the ability to "control the expression of their sexual and gender identities [can also help] prevent or reduce exposure to stigma and discrimination."[25]

---

[23] *See, e.g.*, Wynne Davis, *It's Not Just the Park Service: 'Rogue' Federal Twitter Accounts Multiply*, NPR (Jan. 27, 2017), perma.cc/E5TJ-S3M6.

[24] *See, e.g.*, Banksy (@Banksy), INSTAGRAM, https://www.instagram.com/banksy/ (last visited Feb. 13, 2024).

[25] Matthew N. Berger et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, 21 J. MED. INTERNET RSCH. e38449 (2022), https://perma.cc/FFM2-BUJ4.

Data minimization is one privacy concept that can lead to the benefits and prevent the harms detailed above. It refers to policies that ensure that personal information is collected, used, or shared only for the purposes that an individual intended. This concept has for decades been a foundational pillar of privacy law and scholarship,[26] and for good reason. Because of the lack of robust data minimization required by law, a phone flashlight app tracked people's movements and sold that information—revealing political affiliations, religious practices, and health-care choices—to advertisers and law enforcement without the users' knowledge or consent.[27] A family photo album service pivoted its business model and extracted biometric information from many millions of personal photographs to build a facial-recognition product marketed to the military.[28] These harms are preventable.

---

[26] *See, e.g.*, Alan F. Westin, PRIVACY AND FREEDOM (1967) (referring to "the individual's interest in ensuring that personal information which he gave for one purpose is not used for another without his consent."); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); *Fair Information Practice Principles*, INTERNATIONAL ASS'N OF PRIVACY PROS., https://perma.cc/3F82-B8GY(last visited Dec. 18, 2023). And it is also a key part of the CCPA. *See* Cal. Civ. Code § 1798.100(c).

[27] Press Release, Federal Trade Commission, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), https://perma.cc/6PJT-LYMZ; 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://perma.cc/3BXH-224A.

[28] Olivia Solon & Cyrus Farivar, *supra* note 7.

Requiring that privacy settings be strict by default is also an important policy. People cannot be expected to spend many hours analyzing vaguely worded and complex privacy policies before using a website or electronic device—let alone understand the complex data ecosystems those policies describe.[29] Nor can they effectively navigate through labyrinthine settings, nested menus,[30] and barely visible hyperlinks that many companies erect to make it harder for people to actually utilize privacy rights.[31] Requiring robust privacy defaults is important for ensuring that privacy rights are not just on paper.

The public understands that the stakes are high. Poll after poll shows that Americans overwhelmingly favor stronger government regulation of how companies use personal information, and they want more control over what marketers can learn about them online.[32] Courts have similarly recognized the

---

[29] *See* Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (Jun. 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[30] Thomas Germain, *How to Use Facebook Privacy Settings*, CONSUMER REPORTS (July 31, 2022), https://perma.cc/F9DL-BM2P.

[31] *See* Kaveh Waddell, *California's New Privacy Rights Are Tough to Use, Consumer Reports Study Finds*, CONSUMER REPORTS (Mar. 16, 2021), https://perma.cc/XQE2-AE2B.

[32] Brooke Auxier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RSCH. CTR. (Nov. 15, 2019), https://perma.cc/LM2F-AKM7 (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. PA.

importance of consumer privacy. *See, e.g.*, *Trans Union Corp. v. FTC*, 245 F.3d 809, 818 (D.C. Cir. 2001) (*Trans Union I*) (expressing "no doubt that th[e government's] interest [in] protecting the privacy of consumer credit information [ ] is substantial").

Legislators have responded, including in California. The state has long been concerned with protecting privacy against both government and business interests. In 1972, voters established the constitutional right to privacy, in large part "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*, 533 P.2d 222, 225 (Cal. 1975). As technology companies have accelerated that collection and retention, California continues to lead the charge in protecting privacy.[33]

ANNENBERG SCH. FOR COMMC'NS 13 (2023), https://perma.cc/J3ZR-RBG6 (91% want to have control over what marketers can learn about them).

[33] In 2003, California became the first state to require businesses and state agencies to alert Californians affected by a data breach. Cal. Civ. Code §§ 1798.29, 1798.82, 1798.84. In 2004, it became the first state to require websites to have a privacy policy. Cal. Bus. & Prof. Code §§ 22575–22579. And in 2018, California passed the California Consumer Privacy Act ("CCPA"), which enabled Californians to access and delete information companies hold about them, and opt out of the sale of their personal information (which includes behavioral advertising). Cal. Civ. Code §§ 1798.110, 1798.105, 1798.120; *id.* § 1798.140(ah)(1).

II. Consumer privacy laws can comply with the First Amendment.

A. Laws regulating the collection and use of information can be subject to, and survive, intermediate scrutiny.

Privacy protections akin to those in some provisions of the CAADCA—like data minimization and strong privacy defaults—will often be subject to, and satisfy, intermediate scrutiny, such as when they regulate entities that obtain the relevant information in exchange for provision of a good or service and offer people the ability to opt into more information-sharing or disclosure.[34]

This is in part because the First Amendment does not guarantee access to non-public information. Though it generally protects the right to access, record, analyze and report on public or legally obtained information, *see, e.g.*, *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494–96 (1975) (right to report on information in public court documents), it does not necessarily protect accessing, collecting, or analyzing nonpublic information, *see, e.g.*, *L.A. Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32, 40 (1999) (no right to access nonpublic government information). Our Constitution does not protect, for example, the acts of trespassing or breaking and entering, even if undertaken to gather data. *See, e.g.*, *Lloyd Corp., Ltd. v. Tanner*, 407 U.S. 551, 568 (1972). It does not protect "stealing documents or private wiretapping" that "could provide newsworthy information," even though these acts

[34] This is not the only theory pursuant to which a privacy law might be subject to intermediate scrutiny.

deal entirely in information. *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972); *see also Bartnicki v. Vopper*, 532 U.S. 514, 523, 526–27, 529–30 (2001). Similarly, though the First Amendment can protect "lying . . . to cross the threshold of another's property," this Court has ruled that it generally does not reach "lying to obtain . . . a material benefit," which can include access to records. *Animal Legal Def. Fund v. Wasden*, 878 F.3d 1184, 1195 (9th Cir. 2018).

Accordingly, the *collection* of information can sometimes be regulated differently—and more rigorously—than the publication or use of information that is already collected and in one's lawful possession. For example, in *Bartnicki*, the Supreme Court recognized that wiretapping a conversation without the participants' knowledge—that is, collecting information without consent—was unlawful. 532 U.S. at 529–30. But it also held that the First Amendment protects the publication of such a recording, when it touches on a matter of public concern, by a third party who did not participate in its unlawful collection. *Id.*

Similarly, this Court has recognized that the First Amendment tolerates many statutes "regulat[ing] the misuse of information by entities that obtain that information from individuals through some exchange." *IMDb.com Inc. v. Becerra*, 962 F.3d 1111, 1124 (9th Cir. 2020). Such restrictions do not pose the same constitutional issues as a law that "prohibits the publication of information without regard to how it was obtained." *Id.* To illustrate the point, this Court cited to laws

that limit companies' ability to collect, use, or share information they obtained from their customers as part of an exchange absent the customers' opt-in consent. *Id.* (discussing 18 U.S.C. § 2710(b) (regulating "information obtained in the course of video tape rental") and 47 U.S.C. §§ 551(a)–(c) (same for cable subscribers)).

Other courts, too, have held that regulations limiting the non-consensual sharing of personal information obtained through a commercial exchange do not violate the First Amendment. For example, applying intermediate scrutiny, the D.C. Circuit upheld a requirement that telecommunications carriers obtain opt-in consent from subscribers before disclosing details about their use of the service. *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 997, 1000–02 (D.C. Cir. 2009). A district court similarly upheld a law limiting "the sellers of certain products from disclosing the identity of individuals who purchase those products" under intermediate scrutiny. *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 445–46 (S.D.N.Y. 2016); *Boelter v. Advance Mag. Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016).

These courts have applied the Supreme Court's test from *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980), pursuant to which regulations of protected commercial speech must further a "substantial" government interest, "directly advance" that interest, and be no "more extensive than is necessary to serve that interest." *Id.* at 566. This approach rests in part on the recognition that the government's "interest in regulating the underlying

transaction may give it a concomitant interest" in regulating speech "'linked inextricably' with the commercial arrangement that it proposes." *Edenfield v. Fane*, 507 U.S. 761, 767 (1993) (citation omitted).

Applying that test, courts have recognized that the state's interest in protecting individuals' use and control of their personal information in such contexts is substantial. *See, e.g.*, *U.S. W., Inc.*, 182 F.3d at 1234–35; *Nat'l Cable*, 555 F.3d at 1001. And courts have held that laws requiring opt-in consent for data-sharing or the highest privacy settings by default directly advance this interest while being no more extensive than necessary because they allow collection, use, and disclosure of information when the user affirmatively consents to it. *See Nat'l Cable*, 555 F.3d at 1002; *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142–43 (D.C. Cir. 2001) (*Trans Union II*).[35]

B. Laws requiring entities to disclose factual, noncontroversial information about data collection are subject to lower scrutiny.

Likewise, laws that require a platform to disclose when users are being tracked or monitored would likely pass muster. Unlike laws that compel speech in order to "prescribe what shall be orthodox in . . . matters of opinion [and] force citizens to confess . . . their faith therein"—and so are highly suspect—laws that compel

[35] Some of the CAADCA provisions appear to track this caselaw, *see, e.g.*, Cal. Civ. Code § 1798.99.31(a)(6), while others are blanket prohibitions on collection and use, *see, e.g.*, *id.* § 31(b)(3)–(4).

"purely factual and uncontroversial information about the terms under which [a] service[] will be available" satisfy the First Amendment so long as they "are reasonably related to the State's interest in preventing deception of consumers." *Zauderer v. Off. of Disciplinary Counsel*, 471 U.S. 626, 651 (1985); *see also CTIA v. City of Berkeley*, 928 F.3d 832, 844 (9th Cir. 2019) (recognizing other substantial government interests that may justify uncontroversial, factual disclosures).

That is the case for mandatory disclosures about when a user is being tracked by a platform: such disclosures seek to give consumers more information about the product they are using, prevent confusion or deception, and empower consumers to choose whether to continue using the service. The requirement is reasonably related to these objectives because users may not otherwise know or be aware that they are being tracked online.

III. Content-based burdens on publishing, hosting, and distributing protected speech, like the CAADCA, trigger strict scrutiny.

Notwithstanding its framing as a consumer privacy law, the CAADCA is not subject to the analysis described above. As explained below, it is a content-based regulation of protected speech and so should be assessed under strict scrutiny and struck down in its entirety.[36]

[36] Amici agree with NetChoice that the law's constitutionally infirm provisions are not severable from those provisions that might be subject to different constitutional analysis.

The CAADCA regulates core First Amendment activities: the "publication and dissemination of . . . the printed word." *Smith v. California*, 361 U.S. 147, 150 (1959). The law also impermissibly burdens and regulates protected editorial discretion. Choosing *how* one speaks is a key part of the right to speak at all, from a newspaper's decisions about what to print, *see Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974), to a parade organizer's choice of participants, *Hurley v. Irish-Am. Gay, Lesbian, & Bisexual Grp. of Bos.*, 515 U.S. 557, 570 (1995), to a utility company's preferences about what to put on its billing envelopes, *Pac. Gas & Elec. Co. v. Pub. Utils. Comm'n of Cal.*, 475 U.S. 1, 17–18 (1986).

The CAADCA strikes at the heart of these rights. In doing so, it impacts not only publishers, including websites and platforms, but "the whole public"—those who create materials and those who receive them. *Smith*, 361 U.S. at 154. Because it regulates online speech, the impact is perhaps even more significant, for "the 'vast democratic forums of the Internet' in general . . . and social media in particular" have become the "most important places . . . for the exchange of views." *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017) (quoting *Reno v. ACLU*, 521 U.S. 844, 868 (1997)).

One provision of the CAADCA expressly prohibits the "[u]se of personal information of a child in a way" that is "materially detrimental to the physical health, mental health, or well-being of a child." Cal. Civ. Code § 1798.99.31(b)(1). This

prohibition would include writing about a child in a way that causes them material detriment—potentially covering everything from articles criticizing high school students for posting racist videos on social media, to articles by survivors of school shootings recounting their experience, to news stories about specific minors' inability to access gender-affirming care. The prohibition could also stop a service from using any information about children—their names, social media handles, user preferences, and more—to deliver resources to them on difficult but critical issues, from parental abuse to eating disorders to depression and anxiety, out of fear that the resources could be deemed "materially detrimental."

Other provisions of the CAADCA single out specific content for greater burdens based on its harm or "potential harm[ ]" to children. Businesses must assess eight different factors related to "harm" prior to offering a new service or feature. *See* Cal. Civ. Code §§ 1798.99.31(a)(1)(B)(i)–(viii). Not only must they review these reports biennially, *id*. § 31(a)(1)(A), and make them available upon request to the Attorney General, *id*. §§ 31(a)(3), (4)(A), but they must "create a timed plan to mitigate or eliminate the risk [of material detriment to children] before the online service, product, or feature is accessed by children," *id*. § 31(a)(2). Thus, every time a website or platform wants to roll out new moderation policies, it must conduct detailed assessments of whether those protected choices will lead to the publication

of "harmful" or "potentially harmful" materials. The same goes for offering a new service for users to post content or meet new people.[37]

These requirements will impair publishers' ability to implement new moderation policies, and delay users' ability to express themselves using new platforms and features. The multitude of requirements could also lead platforms to make their content moderation policies more speech restrictive or not to publish certain content at all.

The law's prohibition on "materially detrimental" speech and its targeting of "harmful" or "potentially harmful" content—left undefined, *see id.* § 31(a)—constitutes content discrimination, triggering strict scrutiny. By the words' plain meanings, websites and platforms must assess the potential for material to instigate grief, sorrow, pain, hurt, distress, or affliction in a minor.[38] This includes online mental health resources and communities that many children turn to for support. It

[37] While these assessments are required "[b]efore any new online services, products, or features are offered to the public," *id.* § 31(a)(1)(A)—including online services that do not specialize in publishing or hosting speech, such as shopping services—the requirement uniquely burdens online speakers, publishers, and distributors. Because the concept of "harm" is far more nebulous and problematic when it comes to speech, *see* Section III *infra*, this provision imposes a different and greater burden on businesses that specialize in online speech. And the more speech a platform hosts, the greater the burden it will face in assessing the potential "harm" from that content.

[38] *See Harm*, OXFORD ENGLISH DICTIONARY (Online ed.) ("OED"), https://perma.cc/W55K-L9JJ; *Harmful*, OED, perma.cc/62TK-3M6N; *Detrimental*, OED, perma.cc/3JJK-7QW3.

touches reporting about school shootings, war, climate change, and teen suicide. And it reaches minors' own political or religious speech, as well as their personal updates about deaths in the family, rejection from a college, or a breakup.[39]

The Supreme Court has made clear that even speech that causes deep anguish or severe emotional distress cannot be banned or burdened based on "the content and viewpoint of the message conveyed." *Snyder v. Phelps*, 562 U.S. 443, 457 (2011). *See also United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 812 (2000) ("The Government's . . . burdens [on speech] must satisfy the same rigorous scrutiny as its . . . bans."). This prohibition on regulating speech *because* of its offensive, hurtful, and even materially harmful message derives, in part, from the recognition that such speech often deals with matters of public concern and so "occupies the highest rung of the hierarchy of First Amendment values." *Snyder*, 562 U.S. at 452 (quoting *Connick v. Myers*, 461 U.S. 138, 145 (1983)). Speech at the zenith of protection "is often provocative and challenging" and "may strike at prejudices and preconceptions and have profound unsettling effects as it presses for acceptance of an idea." *Terminiello v. City of Chicago*, 337 U.S. 1, 4 (1949).

Being a young person can be very difficult. Speech confronting, discussing,

[39] The law is also unconstitutionally vague. Key terms are undefined and turn in part on the subjective reactions of recipients. This defect is especially intolerable "where [the] statute 'abut(s) upon sensitive areas of basic First Amendment freedoms.'" *Grayned v. City of Rockford*, 408 U.S. 104, 109 (1972) (citations omitted).

and working through daily realities may be hard for children and the adults in their lives, but it is often valuable and it is constitutionally protected. Moreover, even where the regulated speech lacks obvious value, "[o]ur Constitution forecloses any attempt to [regulate it] simply on the basis that some speech is not worth it." *United States v. Stevens*, 559 U.S. 460, 470 (2010).

This is no less true where the government's stated interest is to protect children. "No doubt a State possesses legitimate power to protect children from harm . . . but that does not include a free-floating power to restrict the ideas to which children may be exposed." *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 799 (2011). (citation omitted). To the contrary, "minors are entitled to a significant measure of First Amendment protection . . . and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them." *Erznoznik*, 422 U.S. at 212–13 (citation omitted). Notwithstanding societal fears about new technologies and mediums—including the ideas they might expose children to—nearly every time they are introduced, the Supreme Court has struck down legislation seeking to protect kids from new purported dangers, whether violent video games, *see Brown*, 564 U.S. at 789, indecent communications online, *Reno*, 521 U.S. at 874, or drive-in movies, *Erznoznik*, 422 U.S. at 212–13.[40]

[40] The Supreme Court has recognized that there is a discrete and exceedingly narrow category of "harmful to minors" speech that can be prohibited when communicated

Content-based laws, even if meant to protect children, are subject to strict scrutiny. *See Ashcroft v. ACLU*, 542 U.S. 656, 670 (2004) (holding that a law designed to protect minors from viewing harmful materials online was a content-based restriction that did not survive strict scrutiny). Where the details of the regulated speech or medium "arouse the reader's ire, and the reader's desire to put an end to th[e] horrible message," the danger of content-based regulation is revealed: "that the *ideas* expressed by speech—whether it be violence, or gore, or racism—and not its objective effects, may be the real reason for governmental proscription." *Brown*, 564 U.S. at 799; *see also Reno*, 521 U.S. at 868 (noting that a statute regulating minors' access to "indecent" and "patently offensive" material on the Internet was "a content-based blanket restriction on speech").

The CAADCA is such a content-based law, and it cannot survive strict scrutiny. To the extent that the law seeks to silence or discourage speech that the

---

solely to children: materials that "predominantly appeal[] to the prurient, shameful, or morbid interests of minors," are "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors," *Ginsberg v. New York*, 390 U.S. 629, 646 (1968), when "taken as a whole, lack[ ] serious literary, artistic, political, or scientific value," *Miller v. California*, 413 U.S. 15, 24–25 (1973), are "specifically defined by the applicable state law,' and are "limited to 'sexual conduct,'" *Reno*, 521 U.S. at 873. "[I]f any reasonable minor, including a seventeen-year-old, would find serious value, the material is not 'harmful to minors.'" *Am. Booksellers v. Webb*, 919 F.2d 1493, 1505 (11th Cir. 1990) (citing *Pope v. Illinois*, 481 U.S. 497 (1987)). There is no plausible argument that the CAADCA is limited to such speech or harms.

legislature deems inappropriate for children, it is impermissible. To the extent that its concerns about online content are legitimate, there are far less restrictive means available to address them, including encouraging the voluntary installation of filters or application blockers, *see, e.g.*, *Reno*, 521 U.S. at 877–79; encouraging libraries, schools, and other community organizations to provide educational resources; and relying on existing criminal laws that prohibit relevant unlawful conduct, such as sexual exploitation or harassment.

Moreover, regardless of the strength of the government's interest in protecting children, it "may not 'reduc[e] the adult population . . . to . . . only what is fit for children.'" *Reno*, 521 U.S. at 875 (citation omitted). "A statute that effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another . . . is unacceptable if less restrictive alternatives would be at least as effective[.]" *Ashcroft*, 542 U.S. at 665. That, too, is fatal for the CAADCA, which imposes burdens and prohibitions on any new service, product, or feature "likely to be accessed by children," but is in no way limited to those that will be accessed *only* by children. To the contrary, the definition is so expansive that it may well reach all online content.

The law's provision encouraging age estimation does not save it from this constitutional deficiency. *See* Cal. Civ. Code § 1798.99.31(a)(5). For those businesses that choose to use age estimation, rather than "apply the privacy and data

protections afforded to children to all consumers" (an option that undercuts the child-protection rationale), *id.*, the estimation itself will impermissibly burden users, including adult users, who must undergo it to be identified.

Ironically, the CAADCA will also exacerbate privacy and security concerns because age estimation requires the collection and analysis of user data. *See, e.g.*, *Mukasey*, 534 F.3d at 197 (noting age-verification requirement can "create a potentially permanent electronic record" of the sites users choose to visit.). Any adult improperly estimated to be a child will have their access to material unduly restricted. And, not surprisingly, even for those who technically still have access, age estimation will also rob users of anonymity, which is critical to "promot[ing] the robust exchange of ideas and allow[ing] individuals to express themselves freely." *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011) (citation omitted).

CONCLUSION

For the foregoing reasons, the Court should affirm the district court's issuance of a preliminary injunction against the CAADCA, while ensuring that doctrinal avenues to uphold other consumer privacy protections remain available.

Dated: February 14, 2024

Respectfully submitted,

/s/ Vera Eidelman
Vera Eidelman
Elizabeth Gyori
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18 Fl.
New York, NY 11218
veidelman@aclu.org

Jacob A. Snow
Nicolas A. Hidalgo
Chessie Thacher
Nicole A. Ozer
Matthew T. Cagle
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
jsnow@aclunc.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE FOR ELECTRONIC FILING

I hereby certify that on February 14, 2024, 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 ACMS system, which effects service upon all counsel of record.

Dated: February 14, 2024

Respectfully submitted,

/s/ Vera Eidelman
Vera Eidelman

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief contains 6,283 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: February 14, 2024

Respectfully submitted,

/s/ Vera Eidelman
Vera Eidelman

Counsel for Amici Curiae