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, San Jose
5:22-cv-08861-BLF
The Honorable Beth L. Freeman, District Court Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF PLAINTIFF-APPELLEE AND AFFIRMANCE

Samir Jain
Eric Null
Kate Ruane
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street, NW
Washington, DC 20005

Aaron Mackey
Counsel of Record
Adam Schwartz
David Greene
F. Mario Trujillo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: February 14, 2024

By: /s/ *Aaron Mackey*
Aaron Mackey

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF AMICI[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 33,000 dues-paying members that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF is dedicated to protecting online users' free expression and privacy rights. We've fought for both in courts and legislatures across the country. We challenge laws that burden all internet users' rights by seeking to age-gate portions of the internet or that otherwise require online services to verify their users' age. *E.g.*, *ACLU v. Reno*, 929 F. Supp. 824, 825 (E.D. Pa. 1996) (serving as a plaintiff challenging the Communications Decency Act); *ACLU v. Reno*, 31 F. Supp. 2d 473, 480 n.3 (E.D. Pa. 1999) (serving as a plaintiff challenging the Child Online Protection Act). We defend the constitutionality of well-crafted consumer data privacy laws. *E.g., In re Clearview AI Ltgn.*, 585 F. Supp. 3d 1111 (N.D. Ill. 2022); *ACA Connects v. Frey*, 471 F. Supp. 3d 318 (D. Me. 2020). We advocate in Congress and state legislatures to pass consumer data privacy laws. *E.g.*, H.R. 3420, My Body My Data Act of 2023; Cal. A.B. 1760, Privacy For All Act of 2019.

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici certify that no person or entity, other than amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

The Center for Democracy & Technology (CDT) is a non-profit public interest organization. For over twenty-five years, CDT has represented the public's interest in an open, decentralized Internet and worked to ensure that the constitutional and democratic values of free expression and privacy are protected in the digital age. CDT regularly advocates before legislatures, regulatory agencies, and courts in support of First Amendment rights on the Internet, including limits on governmental authority to compel or silence speech, and in support of privacy protections for online users.

INTRODUCTION

The California Age-Appropriate Design Code ("AADC") should be struck down in its entirety because its age verification scheme and vague standards violate the First Amendment and are not severable from the statute's other provisions concerning children's data privacy. The Court should hold that (1) the AADC's age-verification provision unlawfully burdens adults' and children's ability to speak and receive information online, Sec. 1798.99.31(a)(5), and (2) key AADC provisions are unconstitutionally vague because they prohibit online services' display of a variety of protected speech, such as the news and other users' speech, that may be ambiguously considered (in the words of the AADC) "harmful" to children. *See, e.g.*, Sec. 1798.99.31(a)(1)(B)(i).

The Court should then hold that the remaining provisions of the AADC, which limit how businesses process the data of children, are inseverable from the unconstitutional parts. With no surviving rule regarding how a business is to know a consumer is a child, there is no way for a business to implement the law's data processing limits.

By affirming the invalidity of the entire AADC in this way, the Court will chart a different, narrower path than the district court, which unnecessarily raised questions about the constitutionality of well-crafted privacy laws. This more focused path will protect all internet users' free speech rights, affirm the constitutionality of existing well-crafted privacy laws, and guide legislators working to pass future data privacy laws.

The Court need not and should not separately address the constitutionality of the AADC's consumer data privacy provisions. *See* Sec. 1798.99.31(a)(6)-(10) & (b)(1)-(8). If the Court does so, however, it should be explicit that those provisions are subject to less-searching First Amendment scrutiny. Data privacy laws are regulations of commercial speech on matters of private concern—people's personal information. Thus, such measures face intermediate First Amendment scrutiny, not strict scrutiny. The Court should be careful to not prejudge the constitutionality of data privacy principles within the AADC that are likely to be essential components of comprehensive consumer data privacy laws.

ARGUMENT

I. THE AADC VIOLATES THE FIRST AMENDMENT.

The AADC places barriers on adults' and children's ability to speak and to access others' speech online, and burdens online services with vague standards concerning the content they host. The statute impermissibly interferes with "one of the most important places to exchange views" today—the "'vast democratic forums of the Internet.'" *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017) (quoting *Reno v. ACLU*, 521 U.S. 844, 868 (1997)).

A. Adults And Children Rely On The Internet To Engage In A Diverse Range Of Free Expression.

Internet users of all ages rely on online services, including social media, "to engage in a wide array of protected First Amendment activity on topics 'as diverse as human thought.'" *Packingham*, 582 U.S. at 105 (quoting *Reno*, 521 U.S. at 870). As of October 2023, there were roughly 5.3 billion people online, with 4.95 billion people using online social media platforms.[2]

Those billions of internet users, including adults and minors, routinely flock

[2] *See Number of internet and social media users worldwide as of October 2023*, Statista (Oct. 25, 2023) https://www.statista.com/statistics/617136/digital-population-worldwide/.

to online forums to express their political views[3] or to get their news.[4] The interactive nature of many online services also enables direct interactions with elected officials. *See Packingham*, 598 U.S. at 104–05.

As the Supreme Court recognized, internet users rely on these same forums for other important reasons, too, including to share photos with their family and friends, to look for work, to advertise that they are hiring, and to improve themselves. *See Packingham*, 582 U.S. at 104.

The internet is also a prime forum for artistic creation. In 2015, YouTube users uploaded roughly 400 hours of videos to the website every minute.[5] By 2020, this had grown to 500 hours of videos each minute.[6]

---

[3] Sam Bestvater, Sono Shah, Gonzalo Rivero, and Aaron Smith, *Politics on Twitter: one-third of tweets from U.S. adults are political*, Pew Research Center (June 2022), https://www.pewresearch.org/politics/2022/06/16/politics-on-twitter-one-third-of-tweets-from-u-s-adults-are-political/; Rainier Harris, *How Young People Use Social Media to Engage Civically*, PBS (Nov. 5, 2020), https://www.pbs.org/newshour/classroom/classroom-voices/student-voices/2020/11/student-voice-how-young-people-use-social-media-to-engage-civically.

[4] Elisa Shearer, *More than eight-in-ten Americans get news from digital devices*, Pew Research Center (Jan. 2021), https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/.

[5] Bree Brouwer, *YouTube Now Gets Over 400 Hours of Content Uploaded Every Minute*, Tubefilter (July 2015), http://www.tubefilter.com/2015/07/26/youtube-400-hours-content-every-minute/.

[6] Jason Wise, *How many videos are uploaded to YouTube a day in 2022?* Earthweb (Nov. 22, 2022), https://earthweb.com/how-many-videos-are-uploaded-to-youtube-a-day/.

Teens use the internet to create art. Twenty-five percent of teens said that social media is very important for their creative expression.[7] Thirteen percent of teens used social media to write, create art, or make music.[8]

B. The AADC Impermissibly Burdens Everyone's Ability To Express Themselves And Receive Information Online.

The AADC requires that online services "likely to be accessed by children," Sec. 1798.99.31(a), shall "[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers." *Id.* at (a)(5). The requirement is essential to the law's regulatory scheme: the law imposes various duties and prohibitions on online services with respect to child users when the services are likely to be accessed by children. *See id. at* (a)(1)-(4), (a)(6)-(10), & (b)(1)-(8).

The AADC defines children as anyone under 18, Sec. 1798.99.30(b)(1), and the term "online service, product, or feature" includes most general-purpose

---

[7] Victoria Rideout et al., *Coping With Covid-19: How Young People Use Digital Media to Manage Their Health*, Common Sense Media (2021), https://www.commonsensemedia.org/sites/default/files/research/report/2021-coping-with-covid19-full-report.pdf.

[8] Victoria Rideout et al., *The Common Sense Census: Media Use by Teens and Tweens, 2021*, Common Sense Media (2022), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.

websites—from search engines to social media. To comply with the AADC, most services will have to verify the ages of *all their users* to determine which are children to whom they must apply special protections. Even services that are unsure whether their sites are likely to be accessed by children will also need to verify users' ages to determine whether they are subject to the AADC.

Although AADC purports to give online services the option to avoid verifying their users' ages if they "apply the privacy and data protections afforded to children to all consumers," *id.* at (a)(5), that is a false choice. Because the vast majority of online services monetize user information, such as by selling it or using the data to target advertisements, the services are highly unlikely to forgo that revenue by treating all their users as children.

The AADC thus effectively requires all internet users to prove their age to access a diverse range of online expression. The only viable way for services to verify their users' ages will be to exclude users until they submit government-issued identification, biometrics, or other proof-of-age.

The AADC's strong incentivization of age-verification violates the First Amendment because it imposes significant burdens on adults' access to constitutional speech, and "discourage[s] users from accessing" the services that require such verification. *Reno*, 521 U.S. at 856. The "right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of

speech, press, and political freedom." *Bd. of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality). By enacting an age-verification scheme to identify minors, the AADC burdens adults' First Amendment right to receive online speech.

The AADC's age-verification requirement also burdens minors' First Amendment rights. "[M]inors 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 v. City of Jacksonville*, 422 U.S. 205, 212–13 (1975). Government may permissibly restrict minors from accessing only one content category: sexual material that would be obscene from the perspective of children. *See Brown v. Entertainment Merchants Ass'n*, 564 U.S. 786, 793–94 (2011). The AADC, however, broadly reaches a diverse range of lawful content online.

Age-verification schemes like the AADC's also frustrate all users' First Amendment rights to speak anonymously online. *See Am. Booksellers Foundation v. Dean*, 342 F.3d 96, 99, 102 (2d Cir. 2003) (holding an age-verification requirement unconstitutional because it forced "website visitors [to] forgo the anonymity otherwise available on the internet."); *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008) (contrasting age-verification requirements with regulations that do not force users to "relinquish their anonymity to access protected speech"). An internet user's "decision to remain anonymous . . . is an aspect of the freedom of

speech protected by the First Amendment." *McIntyre v. Ohio*, 514 U.S. 334, 342 (1995). This Court has recognized that anonymity "facilitates the rich, diverse, and far-ranging exchange of ideas." *Doe v. Harris*, 772 F.3d 563, 581 (9th Cir. 2014).

The AADC's age-verification requirement creates other burdens, too. Many internet users will be reluctant to provide personal information necessary to verify their ages, because of reasonable doubts regarding the security of the services, and the resulting threat of identity theft and fraud. *See ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007); *see also PSINET, Inc. v. Chapman*, 167 F. Supp. 2d 878, 889 (W.D. Va. 2001), *aff'd*, 362 F.3d 227 (4th Cir. 2004).

C. The AADC's Age-Verification Regime Is Not Narrowly Tailored To California's Interest In Protecting Children.

The AADC's age-verification provision is unconstitutional because it is not narrowly tailored to the government's interest in protecting children and is far from the least restrictive means to advance the state's interest. *See Ashcroft v. ACLU*, 542 U.S. 656, 667–70 (2004) (holding an age-verification scheme unconstitutional because it burdened adults' First Amendment rights).

A content-based restriction is subject to strict scrutiny, which requires the state to identify a compelling interest and show the restriction is narrowly tailored to advance that interest. *Brown*, 564 U.S. at 799. Narrow tailoring under strict scrutiny requires that the law directly advance the government interest, that it can be neither overinclusive nor underinclusive, and that it is the least speech-

restrictive means to advance the interest. *U.S. v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 813 (2000).

The AADC's age-verification scheme is subject to strict scrutiny because it is a content-based speech restriction. The AADC requires online services to determine users' ages and imposes burdens on online services as a result, including identifying whether the service might expose children to "harmful, or potentially harmful, content" and coming up with a plan to shield children from that content. *See* Secs. 1798.99.31(a)(1)(B)(i), (a)(2) (requiring a service to mitigate or eliminate risks identified in a Data Protection Impact Assessment that determines it might expose children to harmful, or potentially harmful, content). Because AADC's age-verification requirement facilitates restricting access to content on the belief that it is harmful to children, it is subject to strict scrutiny. *Brown*, 564 U.S. at 799; *see Playboy Entertainment Group, Inc.*, 529 U.S. at 811–13.

As discussed in the previous section, the AADC's age-verification scheme is overinclusive: it burdens everyone's access to lawful content online. California cannot enact content-restrictive defaults when adults, children, and parents likely disagree with the state regarding what is harmful. *See Brown*, 564 U.S. at 804.

The AADC's burdens are also far from the least restrictive means to protect children online. California could fund parents' acquisition of internet filters or social media literacy campaigns for children, which would not directly burden

adults' access to lawful content. *See Ashcroft*, 542 U.S. at 669. Alternatively, California could adopt stronger data privacy regulations that—unlike the AADC—do not require age-verification. *See infra* Part III.[9]

Even if this Court applied intermediate First Amendment scrutiny to the AADC's age-verification rule, it would still fail for many of the same reasons above: it lacks the requisite tailoring, *McCullen v. Coakley*, 573 U.S. 464, 486 (2014), to any governmental interests. *See NetChoice, LLC v. Griffin*, 2023 WL 5660155, *17–21 (W.D. Ark. Aug. 31, 2023) (assuming intermediate scrutiny and preliminarily enjoining an age-verification mandate).

D. The AADC's Standards For Protecting Children Are Unconstitutionally Vague.

Key AADC terms are unconstitutionally vague, which provides an independent First Amendment ground for voiding the statute. To comply with the AADC, businesses must undertake the amorphous tasks of determining: whether their design might expose children to "harmful, or potentially harmful, content," Sec. 1798.99.31(a)(1)(B)(i); whether various design choices are "in the best interest of children," *id.* at (a)(6), (b)(2), (b)(3), (b)(4); and whether various activity is "materially detrimental to the physical health, mental health, or well-being of a

[9] Corynne McSherry, Mario Trujillo, Cindy Cohn, and Thorin Klosowski, *Privacy First: A Better Way to Address Online Harms*, EFF Whitepaper (Nov. 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms.

child." *Id*. at (b)(1).

Because the AADC's vague language burdens speech, it triggers review under both the First and Fourteenth Amendments. The "void for vagueness" doctrine of the Due Process Clause requires "clarity of regulation" for two reasons. First, "regulated parties should know what is required of them." *FCC v. Fox Television, Inc.*, 567 U.S. 239, 253 (2012). Second, "those enforcing the law" must be cabined from acting "in an arbitrary or discriminatory way." *Id.* A vague law regulating expression "raises special First Amendment concerns because of its obvious chilling effect on free speech." *Reno*, 521 U.S. at 871–72. Thus, "[w]hen speech is involved, rigorous adherence to those [anti-vagueness] requirements is necessary to ensure that ambiguity does not chill protected speech." *Fox Television, Inc.*, 567 U.S. at 253–54.

The AADC offers no reasonable, clear standards regarding what content an online service can disseminate, or how the service can disseminate it, in a manner that avoids a later claim by California officials that the service's actions, or the content present on its site, were "harmful" or "detrimental" to minors, Sec. 1798.99.31(a)(1)(B)(i), (b)(1), (b)(7), or not "in the best interest" of minors, *e.g.*, *id.* at (a)(6). These terms are void for vagueness because they require "wholly subjective judgments without statutory definitions, narrowing context, or settled legal meanings." *Mukasey*, 534 F.3d at 205 (internal quotations omitted). Further,

laws like this that require online platforms to guess are incompatible with the First Amendment. *See Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972).

II. THE COURT SHOULD STRIKE DOWN THE ENTIRE AADC BECAUSE ITS UNCONSTITUTIONAL PROVISIONS CANNOT BE SERVERED FROM THE REMAINDER.

California's severability doctrine requires this Court to strike down the AADC in its entirety in light of its unconstitutional age-verification scheme without addressing the validity of other provisions of the law. California requires "three criteria for severability: the invalid provision must be grammatically, functionally, and volitionally separable." *Barlow v. Davis*, 72 Cal.App.4th 1258, 1264 (1999). "All three criteria must be satisfied." *McMahan v. City & County of San Francisco*, 127 Cal.App.4th 1368, 1374 (2005).

The AADC's age-verification regime is functionally inseverable from the law's other operative provisions. Functional severability requires the remaining provisions to be effective without the voided provisions. *Hotel Emps. & Rest. Emps. Int'l Union v. Davis*, 21 Cal.4th 585, 613–14 (1999); *see Barlow*, 72 Cal.App.4th at 1265–66. The only way an online service can know whether it must comply with the AADC's duties (Sec. 1798.99.31(a)(1)-(10)) and prohibitions (*id.* at (b)(1)-(8)) regarding children is to verify its users' ages. *Id.* at (a)(5). Thus, the provisions that rely on knowing a minor's age do not retain any efficacy absent the age-verification provision. *Hotel Emps. & Rest. Emps. Int'l Union*, 21 Cal.4th at

613–14 (1999).

The AADC's duties and prohibitions are not volitionally severable either. Volitional severability requires that "[t]he remaining portions must constitute an independent operative expression of legislative intent, unaided by the invalidated provisions." *Barlow*, 72 Cal.App.4th at 1265.

The AADC's stated legislative intent is that "children should be afforded protections" for their privacy and from certain online content. Sec. 1798.99.29. The entirety of the AADC's legislative findings discuss risks and harms particular to children that the legislature intends the AADC to address, including through ensuring that online services "are designed in a manner that recognizes the distinct needs of children at different age ranges." Sec. 1(a)(5). Interpreting the AADC's remaining provisions as capable of applying to everyone—rather than to children—would run contrary to the Legislature's intent. *See Hotel Emps. & Rest. Emps. Int'l Union*, 21 Cal.4th at 613.

III. THE COURT SHOULD NOT CAST DOUBT ON THE CONSTITUTIONALITY OF CONSUMER DATA PRIVACY STATUTES NOT BEFORE THIS COURT.

Because the AADC's age-verification scheme and vague standards are unconstitutional, *supra* Part I, and cannot be severed from the remainder of the statute, *supra* Part II, this Court should strike down the entire AADC, without addressing its consumer data privacy provisions. Proceeding this way avoids

casting doubt on the validity of other consumer data privacy laws with provisions similar to the AADC.

Should this Court nonetheless address the constitutionality of the AADC's privacy provisions, it should hold that they do not raise the same First Amendment concerns as the AADC's censorship provisions. Congress and the states have long enacted data privacy laws that limit how businesses may process consumers' personal information.[10] When consumer privacy laws regulate commercial data processing that is not a matter of public concern, as here, courts apply intermediate First Amendment scrutiny, *infra* Part III(A), requiring narrow tailoring between their means and ends, *infra* Part III(B).

This Court should not follow the approach of the district court below. It narrowly focused on California's interest in blocking minors from harmful content. But the government often has several substantial interests, as here: not just protection of information privacy, but also protection of free expression, information security, equal opportunity, and reduction of deceptive commercial

[10] *E.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681; Cable Communications Privacy Act of 1984, 47 U.S.C. § 551; Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510; Video Privacy Protection Act of 1988, 18 U.S.C. § 2710; Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191; Illinois Biometric Information Privacy Act of 2007, 740 Ill. Comp. Stat. 14 *et seq.*; California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100.

speech. *Infra* Part III(C). The privacy principles that inform AADC's consumer data privacy provisions are narrowly tailored to these interests. *Infra* Part III(D).

Moreover, although the district court nominally applied intermediate scrutiny to the AADC's privacy provisions, in reality it incorrectly applied strict scrutiny. Further, the court overread *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), as casting doubt on privacy laws that except certain entities from their regulations. *See NetChoice v. Bonta*, 2023 WL 6135551, at *9 (N.D. Cal. Sept. 18, 2023). Yet many privacy laws do just that, *see, e.g.*, Cal. Civ. Code § 1798.140(d) (CCPA applies only to for-profit entities), without offending the First Amendment. *See Infra P*art III(A)(2).

A. The AADC's Consumer Data Privacy Provisions Are Subject To Intermediate Scrutiny.

Courts routinely apply intermediate First Amendment scrutiny, and not strict scrutiny, to consumer data privacy laws, for two intertwined reasons. First, "speech solely in the individual interest of the speaker and its specific business audience" that concerns "no public issue" warrants "reduced constitutional protection." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc*., 472 U.S. 749, 762 & n.8 (1985). Second, "expression related solely to the economic interests of the speaker and its audience" is "commercial speech" that receives "lesser protection" compared to "other constitutionally guaranteed expression." *Central Hudson Gas & Electric Corp. v. Public Service Commn.*, 447 U.S. 557, 561, 563 (1980).

If this Court addresses the AADC's privacy provisions (and it should not), it should apply intermediate scrutiny—which the district court performed in name only. Here, the AADC's privacy provisions limit the manner in which online services may process consumer data. *See* Sec. 1798.99.31(a)(6)-(10) & (b)(1)-(8). The context is widespread corporate tracking of consumers' online behavior across the internet and monetizing that data in various ways, such as using it to target ads.[11] This consumer data is not a matter of public concern, and the business interests are solely economic.

1. The Consumer Data Subject To The AADC's Privacy Provisions Is Not A Matter Of Public Concern.

"[W]here matters of purely private significance are at issue, First Amendment protections are often less rigorous." *Snyder v. Phelps*, 562 U.S. 443, 452 (2011). *See, e.g.*, *Dun & Bradstreet*, 472 U.S. at 759 (defamation); *Snyder*, 562 U.S. at 451–53 (intentional infliction of emotional distress); *Bartnicki v. Vopper*, 532 U.S. 514, 532–35 (2001) (wiretapping).

The Supreme Court has "pointedly refused" to hold that the First Amendment categorically precludes liability for invasions of privacy. *Florida Star v. B.J.F.*, 491 U.S. 524, 533 (1989). Rather, "clashes between First Amendment

[11] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive into the Technology of Corporate Surveillance*, EFF Whitepaper (Dec. 2, 2019), https://www.eff.org/wp/behind-the-one-way-mirror.

and privacy rights" should be resolved by "relying on limited principles that sweep no more broadly than the appropriate context of the instant case." *Id.* Thus, the First Amendment protected a newspaper publishing the name of a rape victim it had "lawfully obtain[ed]" when it concerned a "matter of public significance." *Id.* at 536–37 (internal quotations omitted, alterations in original). But if "sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition." *Id.* at 534.

This is reflected in the common law privacy torts that limit the collection of truthful private information (intrusion on seclusion) and limit its publication (public disclosure of private facts). *See* Second Restatement of Torts §§ 652B, 652D. They do not offend the First Amendment, as long as they do not restrict discussion of matters of public concern. *See, e.g.*, *Judge v.Saltz Plastic Surgery, P.C.*, 367 P.3d 1006, 1011 & n.4 (Utah 2016); *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 479 (Cal. 1998); *Virgil v. Time, Inc.*, 527 F.2d 1122, 1128–29 (9th Cir. 1975). Under a common formulation: "If the contents of a broadcast or publication are of legitimate public concern, the plaintiff cannot establish a necessary element of the tort action." *Shulman*, 955 P. 2d at 479.

Here, the individual online behavior of each of the millions of consumers is not a matter of public concern. Instead, the businesses' purpose is to monetize and otherwise use data for their own commercial interests. The overwhelming majority

of tracked and targeted consumers will not engage in matters of public concern in relation to their online behavior. Many businesses that collect this information do not distribute it. Those that do distribute it only to a select set of paying clients for their private interests.

2. Businesses Have Solely Economic Interests In Processing The Data Covered By The AADC's Privacy Provisions.

The Supreme Court defines "commercial speech" as "expression related solely to the economic interests of the speaker and its audience." *Central Hudson Gas*, 447 U.S. at 561.[12] Here, the business practices regulated by the AADC's privacy provisions are "related solely to the economic interests" of online services. *Id*. They are processing data about the online behavior of millions of consumers solely for commercial purposes, typically to target ads, to analyze it for their own business purposes, or to sell it to third parties. Thus, when faced with First Amendment challenges to laws that protect consumer privacy from commercial data processing, courts apply intermediate judicial review under the commercial speech doctrine. *See, e.g.*, *Trans Union Corp. v. FTC* (*Trans Union I*), 245 F.3d 809, 818–19 (D.C. Cir. 2001) (upholding FTC rule under Fair Credit Reporting

[12] Advertising, *i.e.*, "speech proposing a commercial transaction," is one form of commercial speech. *Central Hudson*, 447 U.S. at 562 (internal quotations omitted). There are others. *See, e.g., Greater Philadelphia Chamber of Commerce v. City of Philadelphia*, 949 F.3d 116, 136–39 (3d Cir. 2020) (questions from an employer to a job applicant about their salary history).

Act requiring opt-in consent to sell marketing lists); *Trans Union LLC v. FTC* (*Trans Union II*), 295 F.3d 42, 52–53 (D.C. Cir. 2002) (upholding FTC rule under Gramm-Leach-Bliley Act that restricted sharing and use of consumer information); *Natl. Cable Assn. v. FCC*, 555 F.3d 996, 1000–02 (D.C. Cir. 2009) (upholding FCC rule under Telecommunications Act requiring opt-in consent to disclose call records). Such decisions focused not just on the commercial motivation, but also the lack of a matter of public concern. *See, e.g., Trans Union I*, 245 F.3d at 818; *Trans Union II*, 295 F.3d 52–53.

Not to the contrary is *Sorrell*, which struck down Vermont's regulation of how drug company salespersons (known as "detailers") could process prescription information. 564 U.S. at 557. The law discriminated against speakers and viewpoints: it targeted "detailers—and only detailers," and its "purpose and practical effect" was to "diminish the effectiveness of marketing by manufacturers of brand-name drugs." *Id.* at 563–65. Vermont did this "to tilt public debate" towards generic drugs. *Id.* at 578. To prevent any over-reading of its decision, the Court specified: "This is not to say that all privacy measures must avoid content-based rules." *Id.* at 574. The court also left the door open to "more coherent" privacy legislation, *id.* at 573, and noted that "[t]he capacity of technology to find and publish personal information … presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure," *id.* at 579. After

Sorrell, courts still apply *Central Hudson* review to consumer data privacy laws. *See Boelter v. Hearst*, 192 F. Supp. 3d 427, 449–50 (S.D.N.Y. 2016); *King v. Gen. Info. Servs.*, 903 F. Supp. 2d 303, 308–09, 313 (E.D. Pa. 2012).

B. Intermediate Scrutiny Requires Narrow Tailoring Between Legislative Means And Ends.

To satisfy intermediate scrutiny, a speech restraint must "directly advance" and be "narrowly drawn" to a "substantial interest." *Central Hudson*, 447 U.S. at 564–65. Under narrow tailoring in intermediate scrutiny, the speech restriction "must not burden substantially more speech than is necessary to further the government's legitimate interests," though it "need not be the least restrictive or least intrusive means of serving the government's interests." *McCullen*, 573 U.S. at 486 (internal quotations omitted).

C. California Has Substantial Interests In Protecting Data Privacy.

Analyzed independently of the censorious and vague provisions described above, *supra* Part I, the AADC's consumer data privacy provisions advance at least five substantial government interests: information privacy, free expression, information security, equal opportunity, and reducing deceptive commercial speech.

1. Information Privacy.

California has a "substantial" interest in protecting consumer data privacy. *See Trans Union I*, 245 F.3d at 818; *Natl. Cable*, 555 F.3d at 1001; *King*, 903 F. Supp. 2d at 309–10; *Boelter*, 192 F. Supp. 3d at 448.

The state's substantial interest has increased as online services collect more personal information than necessary to provide their services and often misuse or sell that information to others. Laws advance information privacy by, for example, helping to prevent: a photo storage app from repurposing its users' photos to train its biometric algorithm;[13] a social media company from collecting user phone numbers for security then using them for ad targeting;[14] and a telehealth company

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

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

from sharing health data with advertising networks.[15] Laws also advance information privacy through limitations on government surveillance.[16]

2. Free Expression.

California has a substantial interest in protecting free speech, which often rests on privacy. "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively." *Bartnicki*, 532 U.S. at 543 (internal quotations omitted). This interest includes the First Amendment rights to confidentially engage in expressive associations, *NAACP v. Alabama*, 357 U.S. 449, 462 (1958); to speak anonymously, *McIntyre*, 514 U.S. at 357; to converse privately, *Bartnicki*, 532 U.S. at 532–33; to confidentially receive unpopular ideas, *Lamont v. Postmaster General*, 381 U.S. 301, 305–307 (1965); and to confidentially gather newsworthy information from undisclosed sources, *Shoen v. Shoen*, 5 F.3d 1289, 1293–94 (9th Cir. 1993).

Here, corporate surveillance of consumers' online activity threatens First Amendment activities that depend on privacy. For example, some data brokers compile precise phone app geolocation data about hundreds of millions of people

---

[15] *See* FTC, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[16] *See* Robyn Greene, *A new data retention requirement: uniformly opposed and bad public policy*, New America (May 2015), https://www.newamerica.org/oti/blog/a-new-data-retention-requirement/.

and use it to help police identify everyone present at a particular time and place.[17] Other data brokers compile information from social media platforms and use it to inform police about First Amendment activity, online and off.[18] With the click of a mouse, police can use these services to identify who marched in a parade, attended a protest, went to a movie, or met a reporter. This surveillance chills First Amendment activity. *Lamont*, 381 U.S. at 307 (striking down mail surveillance program given its "deterrent effect").[19]

3. Information Security.

California has a substantial interest in protecting information security. Intruders regularly obtain personal data from businesses and use or distribute it for

---

[17] Garance Burke and Jason Dearen, *Tech tool offers police 'mass surveillance on a budget,'* Associated Press (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef; Byron Tau et al., *How ads on your phone can aid government surveillance*, Wall Street Journal (Oct. 13, 2023), https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04. *See generally* EFF, *Location Data Brokers*, https://www.eff.org/issues/location-data-brokers.

[18] Brennan Center, *LAPD documents reveal use of social media monitoring tools* (Sept. 8, 2021), https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-reveal-use-social-media-monitoring-tools.

[19] Elizabeth Soycheff, *Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring*, Journalism & Mass Commc'ns Q. 296 (2016), https://journals.sagepub.com/doi/abs/10.1177/1077699016630255?journalCode=jmqc; Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia use*, Berkeley Tech. L.J. (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

their own purposes.[20] Consumer data privacy laws limit the damage: if businesses hoard less data, there will be less to steal.

4. Equal Opportunity.

California has a substantial interest in protecting equal opportunity. *E.g.*, *Roberts v. U.S. Jaycees*, 468 U.S. 609, 623 (1984). Corporate data surveillance disparately burdens people of color, women, and other vulnerable groups.[21] Lower-income people are often less able to avoid corporate harvesting of their data, because lower-priced technologies often leak more data,[22] and companies have charged a higher price for privacy.[23]

---

[20] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in theU.S.*, N.Y. Times (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; Erik Ortiz, *Marriott Says Breach of Starwood Guest Database Compromised Info of Up to 500 Million*, NBC News (Nov. 30, 2018), available at https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041; Verizon, *2022 Data Breach Investigations Report*, 37, https://www.verizon.com/business/resources/T66/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

[21] *See generally* Paige Collings and Adam Schwartz, *EFF Comments to NTIA re: Privacy, Equity, and Civil Rights* (Mar. 6, 2023), https://www.eff.org/document/2023-03-06-eff-comments-ntia-privacy-and-civil-rights.

[22] Privacy International, *Buying a smart phone on the cheap? Privacy might be the price you have to pay*, (Sept. 2019), https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay.

[23] Sophia Cope and Jeremy Gillula, *AT&T is putting a price on privacy. That is outrageous*, The Guardian (Feb. 20, 2015), https://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy.

Once harvested, this data can be used in discriminatory ways. For example, companies have used it to target vulnerable groups with ads, including for dangerous products like subprime loans,[24] and to exclude vulnerable groups from ads for important opportunities, like homes and jobs.[25] Other companies use this data to make automated decisions about such opportunities,[26] often with discriminatory results.[27] Finally, lower-income people may suffer the most from

---

[24] Jeremy B. Merrill and Hanna Kozlowska, *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; John Paul Strong, *Target Subprime Credit Using Facebook and Paid Search*, Strong Automotive (Apr. 14, 2019), https://www.strongautomotive.com/target-subprime-credit-facebook-paid-search/.

[25] Julia Angwin and Terry Parris Jr, *Facebook Lets Advertisers Exclude Users by Race*, Pro Publica (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; amicus brief of Upturn Inc. (Nov. 2018), in *Mobley v. Facebook, Inc.*, No. 16-cv-06440 (N.D. Cal.), https://www.upturn.org/static/files/2018-11-16_Upturn_Facebook_Amicus.pdf.

[26] McKinsey & Company, *AI-powered decision making for the bank of the future* (Mar 2021), https://www.mckinsey.com/industries/financial-services/our-insights/ai-powered-decision-making-for-the-bank-of-the-future; Katy McLauglin, *Robots are taking over (the rental screening process)*, Wall Street Journal (Nov. 21, 2019), https://www.wsj.com/articles/robots-are-taking-over-the-rental-screening-process-11574332200; Rebecca Heilweil, *Artificial intelligence will help determine if you get your next job*, Vox (Dec. 12, 2019), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen.

[27] Greenlining Institute, *Algorithmic Bias Explained* (Apr. 2021), https://greenlining.org/wp-content/uploads/2021/04/Greenlining-Institute-Algorithmic-Bias-Explained-Report-Feb-2021.pdf; Virginia Eubanks, *Automating inequality* (2018), https://virginia-eubanks.com/automating-inequality/.

data breaches, because it costs money and takes considerable time to freeze and monitor one's credit reports, and to obtain identify theft prevention services.[28]

5. Reducing Deceptive Commercial Speech.

California has a substantial interest in reducing deceptive commercial speech, which is entitled to little or no First Amendment protection. *See Friedman v. Rogers*, 440 U.S. 1, 9 (1979) ("Equally permissible are restrictions on false, deceptive, and misleading commercial speech."). *See also Central Hudson*, 447 U.S. at 563; *In re R.M.J.*, 455 U.S. 191, 203 (1982); *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 367 (2002).

One especially problematic example of deceptive commercial speech online is known as "dark patterns." They manipulate users' experiences to trick them into surrendering personal information, signing up for services they do not intend to use, and other harms.[29] Dark patterns can be a fraudulent omission, *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1213 (C.D. Cal. 2017), or a "deceptive

[28] Sarah O'Brien, *Here's what it costs to freeze your credit after Equifax breach*, CNBC (Sept. 15, 2017), https://www.cnbc.com/2017/09/15/heres-what-it-costs-to-freeze-your-credit-after-equifax-breach.html; Alexandria White, *How much does credit monitoring cost?* CNBC (Nov. 25, 2021), https://www.cnbc.com/select/how-much-does-credit-monitoring-cost/; Clint Proctor and Toni Perkins-Southam, *Best Identity Theft Protection Services of December 2023*, Forbes (Dec. 1, 2023), https://www.forbes.com/advisor/personal-finance/best-identity-theft-protection-services/.

[29] Shirin Mori, *Help Bring Dark Patterns to Light*, EFF (May 19, 2021), https://www.eff.org/deeplinks/2021/05/help-bring-dark-patterns-light.

visual representation," *Sterling Drug, Inc. v. FTC*, 741 F.2d 1146, 1152 (9th Cir. 1984). *See also FTC v. Cyberspace.Com LLC*, 453 F.3d 1196, 1200–01 (9th Cir. 2006).

D. AADC Privacy Principles Directly Advance Substantial State Interests and Are Narrowly Tailored.

Principles reflected in AADC privacy provisions, when stripped of their unconstitutional censorship provisions, could survive intermediate scrutiny because they directly advance the state's strong interests described above.

1. Enforcement Of Privacy Policies.

A requirement that companies adhere to the promises made in their privacy policies directly advances the state's interest in reducing deceptive commercial speech.[30] *See Friedman*, 440 U.S. at 9. Given that this enforcement relates specifically to promises about privacy, it directly advances that interest as well. The Federal Trade Commission (FTC) has based much of its privacy and security enforcement on deceptive claims made in company privacy policies.[31] The FTC's

[30] This brief does not address the required enforcement of other terms and "community standards" referenced in Sec. 1798.99.31(a)(9).

[31] *See* FTC, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

largest fine—$5 billion—stemmed from Facebook defaulting millions of users into face recognition, which allegedly contradicted its data policy.[32]

2. Data Minimization.

The data minimization principle reflected in Sec. 1798.99.31(b)(3) and (b)(4) directly advances the substantial state interest of privacy, data security, free expression, and equal opportunity of users and is not more restrictive than necessary. Data protection laws place limits on what a regulated entity can collect, sell, share, retain, or use. *See, e.g.,* HIPAA, Pub. L. 104-191.[33] Personal data can be misused at each stage of this lifecycle. It follows that effective privacy laws advance the government's interest by protecting personal data at each stage. *See ACLU v. Clearview AI, Inc.*, No. 2020 CH 4353, 10 (Ill. Cir. Ct. Aug. 27, 2021) (collection minimization advances biometric security); *Nat'l Cable & Telecommunications Ass'n*, 555 F.3d at 1001–02 (disclosure minimization advances call records privacy); *Turizo v. Subway Franchisee Advert. Fund Tr. Ltd.*, 603 F. Supp. 3d 1334, 1349 (S.D. Fla. 2022) (use minimization furthers telephone

[32] *United States v. Facebook*, Case No. 19-cv-2184, Complaint, ¶¶ 153-54 (July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

[33] HHS, *Summary of the HIPAA Privacy Rule* (May 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

number privacy); *King*, 903 F. Supp. 2d at 310 (disclosure minimization of old criminal history advances consumer credit privacy).

These data minimization principles are not overinclusive and leave open ample alternative avenues for businesses to use the information. Companies could collect, sell, share, or retain data that is "necessary" to provide the service requested by a user. Section 1798.99.31(b)(3). Companies could also use data for the reason that it was collected, such as: processing an IP address to provide access to its platform, or a user's precise location data to provide map or ride hailing service. Section 1798.99.31(b)(4). Companies could share that data with law enforcement under specific circumstances with legal process. Sec. 1798.145(a)(1)-(4).

3. Regulation Of Precise Geolocation Data.

The data minimization and notice provisions that specifically govern precise geolocation information in Sec. 1798.99.31(b)(5) and (b)(6) directly advance the state's interest in protecting the privacies of life. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018). When not properly protected, precise geolocation

data has been used to target gay priests,[34] to give away U.S. troop positions,[35] and for law enforcement purposes without proper oversight.[36] Journalists and researchers have also found it can be used to track an individual to a Planned Parenthood clinic[37] or to enable stalking.[38]

---

[34] Michelle Boorstein and Heather Kelly, *Catholic group spent millions on app data that tracked gay priests*, The Washington Post (Mar. 9, 2023), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.

[35] Alex Hern, *Fitness tracking app Strava gives away location of secret US army base*, The Guardian (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[36] Joseph Cox, *ICE, CBP, Secret Service All Illegally Used Smartphone Location Data*, 404 Media (Oct. 5, 2023), https://www.404media.co/ice-cbp-secret-service-all-broke-law-with-smartphone-location-data/.

[37] Jennifer Valentino-deVries, Natasha Singer, Michael Keller, Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, The New York Times (Dec. 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[38] Alexis Hancock and Eva Galperin, *The Industry Discussion About Standards for Bluetooth-Enabled Physical Trackers Is Finally Getting Started*, EFF (Aug. 14, 2023), https://www.eff.org/deeplinks/2023/08/industry-discussion-about-standards-bluetooth-enabled-physical-trackers-finally.

4. Regulation Of Dark Patterns.

A law that regulates dark patterns[39] directly advances the substantial state interest of limiting deceptive commercial speech, which enjoys little to no First Amendment protection. *Friedman*, 440 U.S. at 9.

Regulating dark patterns also advances the interests of privacy, speech, security, and equal opportunity because companies often use dark patterns to trick customers into giving up their data rights.[40] *See, e.g.*, *In re Vizio*, 238 F. Supp. 3d at 1213 (allowing fraudulent omission action to move forward against company that engaged in automatic data collection that was difficult to discover or turn off); *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 857–58 (9th Cir. 2022) (finding no user consent to inconspicuous arbitration terms, which allowed telephone privacy lawsuit to move forward in federal court).

The regulation of dark patterns is already found in contract formation and online consent flows. *See* Cal. Bus. & Prof. Code § 17602(d)(1) (companies must

---

[39] The AADC validly prohibits two kinds of dark patterns — (1) those that encourage people to provide more personal information than is reasonably expected, and (2) those that encourage people to forgo privacy protections. The third regulation of dark patterns that are "materially detrimental" to a child is impermissibly vague. *See* Sec. 1798.99.31(b)(7). *See also* Cal. Civ. Code 1798.140(L) (CCPA's definition of "dark pattern"); 1798.99.30(a) (AADC incorporating this definition).

[40] FTC, Staff Report, *Bringing Dark Patterns to Light* 15-19 (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

allow opt-out of autorenewal without obstruction or delay); CCPA Regulations, Section 999.306(f) (opt-out must be same size as other icons); Cal. Civ. Code § 1670.5 ("unconscionable" contracts can be unenforceable); *United States v. GoodRX*, No. 3:23-cv-460 (N.D. Cal. Feb. 1, 2023) (stipulated order that "affirmative consent" to share health data cannot be obtained through dark patterns).

CONCLUSION

This Court should affirm the judgment below, striking down the entire AADC on its face, because the age-verification scheme and vague terms are unconstitutional, and inseverable from the remainder of the statute.

Dated: February 14, 2024

By: /s/ *Aaron Mackey*

Aaron Mackey

Adam Schwartz
David Greene
F. Mario Trujillo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
amackey@eff.org

Samir Jain
Eric Null
Kate Ruane
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street, NW

Washington, DC 20005

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae the Electronic Frontier Foundation and the Center for Democracy & Technology in Support of Plaintiff-Appellee NetChoice and Affirmance complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,912 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: February 14, 2024

By: /s/ *Aaron Mackey*
Aaron Mackey

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on February 14, 2024.

I certify that all participants in the case are registered CM/ECF users, and that service will be accomplished by the appellate CM/ECF system.

Dated: February 14, 2024

By: /s/ *Aaron Mackey*
Aaron Mackey

Counsel for Amici Curiae