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, Hon. Beth Labson Freeman

BRIEF FOR NEVADA, THE DISTRICT OF COLUMBIA, ARIZONA, ARKANSAS, COLORADO, CONNECTICUT, DELAWARE, FLORIDA, ILLINOIS, MARYLAND, MICHIGAN, MINNESOTA, MISSISSIPPI, NEW JERSEY, NEW MEXICO, NEW YORK, NORTH CAROLINA, OREGON, PENNSYLVANIA, RHODE ISLAND AND WASHINGTON AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

AARON D. FORD
Attorney General for the
State of Nevada

HEIDI P. STERN
Solicitor General

KIEL B. IRELAND
Deputy Solicitor General

Office of the Attorney General
for the State of Nevada
100 N. Carson Street
Carson City, NV 89701
hstern@nevada.gov

BRIAN L. SCHWALB
Attorney General for the
District of Columbia

CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

RUSSELL C. BOGUE
Assistant Attorney General

Office of the Attorney General
for the District of Columbia
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-6609
caroline.vanzile@dc.gov

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Other

INTRODUCTION AND INTEREST OF AMICI CURIAE

Nevada and the District of Columbia, on behalf of themselves and the States of Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Michigan, Minnesota, Mississippi, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, and Washington (collectively, the "Amici States"), submit this brief as amici curiae on behalf of appellant.

"It is evident beyond the need for elaboration that a State's interest in safeguarding the physical and psychological wellbeing of a minor is compelling." *New York v. Ferber*, 458 U.S. 747, 756-57 (1982) (internal quotation marks omitted). With that understanding, jurisdictions across the country are actively confronting novel and unprecedented threats posed by online businesses to the health of their youngest residents. These threats range from data-collection practices that violate individuals' privacy, to website design choices that induce addiction and over-use, to violations of published terms and conditions that mislead young consumers about companies' policies. Responding to the magnitude of the danger, states have already sought solutions through legislation, investigation, and litigation. And they have done so in good faith, seeking to balance their concern that children are uniquely vulnerable to harmful online practices with the important constitutional protections implicated by regulation of the Internet.

Properly interpreted, the First Amendment does not prohibit these efforts. However, the district court in this case—on the apparent assumption that the First Amendment is implicated by any regulation of "information"—applied a one-size-fits-all test to enjoin entirely enforcement of the California Age-Appropriate Design Code Act ("CAADCA"), a comprehensive suite of protections passed by California to protect children online. The court's overbroad—and mistaken—application of general free-speech principles to CAADCA disregarded California's sovereign prerogative to protect the health of its children. It also ignored relevant First Amendment doctrine and overlooked the actual operation of CAADCA, subjecting ordinary consumer-protection regulations to inappropriate means-end scrutiny. If widely adopted, the court's reasoning could strangle state efforts to regulate harmful internet practices in their infancy. This Court should correct the district court's erroneous reasoning and reverse its order enjoining CAADCA.

SUMMARY OF ARGUMENT

1. It is well-established that children face serious and pervasive threats to their welfare online. Social-media use is correlated with teen depression and anxiety, and various practices by social-media companies—like addictive design features that keep teens online for hours each day—exacerbate these effects. Meanwhile, intrusive data-collection practices by online businesses violate minors'

privacy and permit companies to target them with potentially harmful content or advertising without their consent.

2. States possess long-recognized police powers to protect children from these threats. Since at least the nineteenth century, states have used these powers to ensure that their most vulnerable residents are not exploited by new industries or technologies, including threats on the Internet. CAADCA is just one effort of many by states and local jurisdictions across the nation to combat the dangers that minors face online. These efforts range from new data-privacy laws that ensure online service providers handle children's data appropriately, to laws and lawsuits targeting the deployment of design choices that manipulate young users, to attempts to investigate and gather more information about the severity of the challenges states are facing. That landscape of state action is varied, evolving, and nascent, as each state makes an individualized judgment about how best to protect young people online. But it represents a growing consensus that states must proactively address these real and novel harms.

3. The district court's erroneous application of the First Amendment to strike down all of CAADCA could stymie these efforts. In asserting that all regulations of information implicate the First Amendment, the court needlessly subjected every challenged provision to means-end scrutiny. That contravenes established First Amendment jurisprudence, including from this Court. For instance, mandatory

reporting requirements like CAADCA's Data Protection Impact Assessments are common across the economy, from banking to securities regulation to vehicle safety, and are not thought to raise First Amendment concerns, let alone trigger intermediate scrutiny. Likewise, mandatory disclosures of product dangers to consumers are commonplace and widely considered to comply with the First Amendment, and compelling truthful commercial speech does not receive intermediate scrutiny. As another example, regulating website design choices like dark patterns amounts to regulating conduct or commercial speech that is unprotected by the First Amendment. And mandates that companies follow their *own* published terms and conditions also do not implicate First Amendment interests. This Court should correct the many errors in the district court's analysis rather than bless an interpretation of the First Amendment that has the potential to undermine the efforts of Amici States and others to protect children from online dangers.

ARGUMENT

I. The Internet Presents An Increasing Threat To Children's Health And Welfare.

In the past couple of decades, states have faced a new and growing threat to the wellbeing of their children: harmful and addictive online services. *See* Off. of Surgeon Gen., *Social Media and Youth Mental Health: The U.S Surgeon General's Advisory* 5, 9-10 (2023), https://tinyurl.com/2a774n5v [hereinafter *Surgeon General Advisory*]. Children's mass adoption of social media in the early 2010s correlates

with a significant decrease in their mental and physical wellbeing—provoking depression, anxiety, and even drug use. *See, e.g.*, *Surgeon General Advisory*, *supra*, at 5; Colo. Att'y Gen., *Social Media, Fentanyl & Illegal Drug Sales: A Report From the Colorado Department of Law* 8-9, 33-34 (2022), https://tinyurl.com/y684c6ka.

The practices of online service providers exacerbate these harms. For instance, social media platforms are intended to monopolize users' time throughout the day and night. Design features like push notifications, infinite scroll, and displaying "likes" trigger reward pathways in the brain and ensure that users want to return again and again. *Surgeon General Advisory*, *supra*, at 9. Children are particularly vulnerable to these enticements and the negative outcomes that result. *See id.* at 4-5. Even a child's right to a quality education is impacted by social media, as the compulsion to return to the platform leads to classroom distractions during the day and poor sleep at night. *See id.* at 7, 9; Christina Koessmeier & Oliver B. Buttner, *Why Are We Distracted by Social Media? Distracting Situations and Strategies, Reasons for Distraction, and Individual Differences*, 12 Frontiers Psych., Dec. 2021, at 1, 2. The results for children are predictable and tragic: "body dissatisfaction, disordered eating, and depressive symptoms," among other things. *Surgeon General Advisory*, *supra*, at 8.

Online service providers' own research has revealed the threat that their products pose to children. In 2021, the *Wall Street Journal* reported that "Facebook

Inc. [now Meta Platforms, Inc.] knows, in acute detail, that its platforms are riddled with flaws that cause harms, often in ways only the company fully understands." *The Facebook Files*, Wall St. J., https://tinyurl.com/4jch323a (last visited Dec. 6, 2023). Meta meticulously studies its applications, and its own researchers have found that "Instagram is harmful for a sizable percentage of [its users], most notably teenage girls." Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sept. 14, 2021), https://tinyurl.com/2x227yea.

Social media is not the only online threat. Children face a confusing landscape of data-collection practices from all online businesses, often hidden behind unclear privacy policies. Those risks can include damaging leaks of personal information and the use of targeted advertising on the basis of data collected on various websites. *See* Piers Gooding, Rys Farthing & Emily Painter, *Data Protection Is a Mental Health Issue for Young People*, Univ. of Melbourne (Oct. 25, 2021), https://tinyurl.com/4899bjyb. For instance, a study from Privacy International revealed that popular websites about depression in France, Germany, and the United Kingdom—all accessible by young people—were sharing user data with advertisers and data brokers, permitting them to "target people when they are at their most vulnerable." Priv. Int'l, *Your Mental Health for Sale* 3 (Sept. 2019), https://tinyurl.com/2w7xyc4b.

Despite these risks, online service providers continue to market their products with few protections—or even warnings—for children. That is likely because their business models rely on maximizing the amount of time that users (including children) spend on their apps and websites. More time on a service equals more revenue, as it allows the service to show more ads and generate more data used in targeting or to be sold to others. *See* Jeff Horwitz & Salvador Rodriguez, *Meta Embraces AI as Facebook, Instagram Help Drive a Rebound*, Wall St. J. (Jan. 27, 2023), https://tinyurl.com/4exxpx7f; Pia Gadkari, *How Does Twitter Make Money?*, BBC (Nov. 7, 2013), https://tinyurl.com/v3jd9n4w.

Online service providers specifically value and target young users because they set cultural trends and present the opportunity to gain lifelong customers for the platform. According to a recent complaint filed by 33 attorneys general, one Meta product designer wrote in an internal email that the "young ones are the best ones" and that "[y]ou want to bring people to your service young and early." Complaint for Injunctive and Other Relief at 14, *California v. Meta Platforms, Inc*., No. 4:23-CV-5448 (N.D. Cal. Nov. 22, 2023), ECF No. 73-2. Said another way, young users are not just the collateral damage of general business practices; they are, in many cases, the target market.

II. States Have Broad And Historic Powers To Promote Children's Wellbeing, And They Are Exercising That Power To Protect Children From The Increased Harms Posed By The Internet.

A. States have long exercised their police powers to protect children's health and welfare.

Child safety "lies at the heart of the states' police powers." *Toy Mfrs. of Am., Inc. v. Blumenthal*, 986 F.2d 615, 620 (2d Cir. 1992). For centuries, states have exercised their power to protect the health and welfare of children, especially in the face of new technologies.

In the nineteenth century, new industrial technology prompted businesses to assign children grueling, dangerous work for long hours. Robert Whaples, *Child Labor in the United States*, Econ. Hist. Ass'n (Oct. 7, 2005), https://tinyurl.com/3a2ta2fy. States responded by enacting a host of laws targeting this new problem, including age minimums, workhour maximums, and bans on children working in certain especially dangerous occupations. *Id.*; *see, e.g.*, *Ex parte Weber*, 86 P. 809, 809 (Cal. 1906); *State v. Shorey*, 86 P. 881, 881 (Or. 1906). While businesses argued that state regulation of child labor violated the Fourteenth Amendment's Due Process and Equal Protection Clauses, courts wisely rejected these overbroad readings of the Constitution, recognizing that the power to protect children "inheres in the government for its own preservation and for the protection of the life, person, health, and morals of its future citizens." *Shorey*, 86 P. at 399. Even during the *Lochner* era, when the U.S. Supreme Court overturned some laws protecting adult

workers, the Court still upheld state child-labor laws as within states' authority. *See, e.g.*, *Sturges & Burn Mfg. Co. v. Beauchamp*, 231 U.S. 320, 325 (1913).

In the modern era, states have continued responding to new threats to children's health and welfare—efforts that courts have upheld. For instance, when New York passed a law prohibiting selling to minors under seventeen any material defined to be obscene "on the basis of its appeal to them," the U.S. Supreme Court upheld the law against First Amendment attack. *Ginsberg v. New York*, 390 U.S. 629, 631, 637-40 (1968) (acknowledging the state's "independent interest in the well-being of its youth"). When "the exploitive use of children in the production of pornography" subsequently became a "serious national problem," the Court permitted states to advance their compelling interest in "safeguarding [children's] physical and psychological wellbeing" by prohibiting the distribution of material that shows children engaged in sexual conduct. *Ferber*, 458 U.S. at 749, 756-57, 774. And when pornography and sexual exploitation moved online, courts continued to bless states' efforts to protect children from sexual exploitation. *See, e.g.*, *State v. Robins*, 646 N.W.2d 287, 296-97 (Wisc. 2002) (rejecting a First Amendment challenge to the application of a state child-enticement statute to communications in an online chat room); *People v. Hsu*, 99 Cal. Rptr. 2d 184, 188 (Ct. App. 2000) (rejecting a First Amendment challenge to a state law that prohibited knowingly sending obscene material to a minor with the purpose to seduce them).

B. States and the federal government are currently engaged in a wide range of initiatives to regulate online service providers.

In line with this tradition, a politically diverse array of states and localities across the country are responding to the emerging threat posed by online service providers to children, fulfilling their duty to protect children's health and welfare. They have developed a multitude of policies to combat these new threats—some tackling discrete issues, some seeking more comprehensive solutions.

CAADCA is one example of a more comprehensive approach. Among other things, the law strictly regulates the collection, sale, sharing, or retention of children's personal information. *See generally* Cal. Civ. Code § 1798.99.31(b). It also requires covered entities to analyze and report on the risks of their services to children, *see id.* § 1798.99.31(a)(1)-(4), prohibits the use of "dark patterns" in website design, *id.* § 1798.99.31(b)(7), requires the use of accessible language in privacy policies, *see id.* § 1798.99.31(a)(7), and mandates enforcement of covered entities' own published policies, *see id.* § 1789.99.31(a)(9).

Other states have taken different but related approaches. For instance, some states have instituted protective measures that reflect the unique risk that children face online, including special rules for minor-created accounts, *see, e.g.*, Ark. Code Ann. § 4-88-1402, options for parent-imposed time limits and restrictions on nighttime usage, *see, e.g.*, Utah Code § 13-63-105(1), (3), and protection from direct messages by accounts that are not friends with a minor website user, *see, e.g.*,

La. Stat. Ann. § 51:1753(1) (effective July 1, 2024). States have also enacted laws that, like CAADCA, regulate online service providers' harvesting, selling, and using children's data. *See, e.g.*, Colo. Rev. Stat. § 61-1308(7) (prohibiting processing of a child's personal data without parental consent); Conn. Gen. Stat. § 42-520(a)(4), (7) (prohibiting selling data or processing data for marketing if the consumer is between 13 and 16 years of age and limiting the processing of data for consumers under 13); Del. Code Ann. tit. 6, § 1204C (prohibiting targeted advertising of specific products to minors based on personal information); La. Stat. Ann. § 51:1753(2)-(3) (same) (effective July 1, 2024); Utah Code § 13-63-103(3)-(5) (prohibiting collection of personal information and all advertising to minors) (effective March 1, 2024).

Like California, many states across the political spectrum have also tackled the risk posed by "dark patterns," which are "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm." FTC Bureau of Consumer Prot., *Bringing Dark Patterns to Light* 2 (2022), https://tinyurl.com/4p2kubhy. Such practices can include formatting advertisements to appear as neutral content, designing websites to hide important information, and deploying features that obscure or subvert consumers' privacy choices. *See id.* at 4-19. In response, several states have passed laws to, for instance, bar companies from obtaining consent to process personal data through the use of

dark patterns. *See, e.g.*, Colo. Rev. Stat. § 6-1-1303(5)(c); Conn. Gen. Stat. § 42-515(7)(C); Del. Code Ann. tit. 6, § 12D-102(7)(c) (effective Jan. 1, 2025); Fla. Stat. § 501.702(7)(c) (effective July 1, 2024); Mont. Code Ann. § 30-14-2802(5)(b)(iii) (effective Oct. 1, 2024); Tex. Bus. & Com. Code Ann. § 541.001(6)(C) (effective July 1, 2024). Some states have acted to protect children specifically from manipulation through these design choices. For example, Florida law mimics CAADCA in prohibiting online platforms from "us[ing] dark patterns to lead or encourage children to provide personal information beyond what personal information would otherwise be reasonably expected to be provided for" that platform. Fla. Stat. § 501.1735(2)(g).

Other states have focused on obtaining more data on the consequences of mass social media adoption by children. For example, New Jersey established a Commission on the Effects of Social Media Usage on Adolescents, which will study the physical, mental, and emotional effects that social media has on children in and out of school. N.J. Pub. L. 2023, ch. 126. Likewise, Colorado commissioned and issued a report on "the use of the internet, including retail, payment, and social media platforms, for the purpose of trafficking fentanyl" and similar narcotics. Colo. Rev. Stat. § 24-31-116 (automatically repealed effective July 1, 2023). Relatedly, at least nine states (in addition to California) require or will soon require that companies that control or process personal data perform Data Protection Impact Assessments

("DPIAs").[1] These assessments must explain how the company uses personal data—including children's data—and weigh the costs and benefits of that use. *See, e.g.*, Conn. Gen. Stat. § 42-522(b). The provisions usually allow the state attorney general or another investigatory body to access the assessments for public-protection purposes. *See, e.g.*, *id.* § 42-522(c).

On top of these laws that have already passed, many states are considering additional measures to protect children's health and wellbeing from the new threats of online platforms.[2] For instance, New York has proposed a "child data privacy and protection act" that, among other protective rules, requires companies that

---

[1] *See* Colo. Rev. Stat. § 6-1-1309; Conn. Gen. Stat. § 42-522; Del. Code Ann. tit. 6, § 12D-108 (effective Jan. 1, 2025); Fla. Stat. § 501.713 (effective July 1, 2024); Ind. Code Ann. § 24-15-6-2 (effective Jan. 1, 2026); Mont. Code Ann. § 30-14-2814 (effective Oct. 1, 2024); Tenn. Code Ann. § 47-18-3307 (effective July 1, 2025); Va. Code Ann. § 59.1-580; Tex. Bus. & Com. Code Ann. § 541.105 (effective July 1, 2024).

[2] *See, e.g.*, H.B. 3880, 103d Gen. Assemb., § 10 (Ill. 2023) (requiring completion of DPIAs and prohibiting collection and use of personal information from children for purpose other than provision of service); H.F. 2257, 93d Leg., § 5 (Minn. 2023) (same); Assemb. 4919 [First Reprint], 220th Leg., §§ 2, 5 (N.J. 2022) (same); H.F. 712, 90th Gen. Assemb., § 2 (Iowa 2023) (prohibiting collecting personal information from children without parental consent); H. 80, 193d Gen. Ct., § 1 (Mass. 2023) (prohibiting targeted advertising of specific products to children); H.B. 644 [Edition 2], 2023-2024 Sess., § 1 (N.C. 2023) (prohibiting targeting of content or advertising to children based on personal information); S. 7694, 2023-2024 Reg. Sess., § 1501 (N.Y. 2023) (prohibiting addictive targeting of content to children without parental consent); Assemb. B. 373, 2023-2024 Leg., § 1(3) (Wis. 2023) (prohibiting collection of personal information from and advertising to children, among other protective measures).

market online products to children to "proactively alert[ ] child users, in a manner likely to be understood by a child in the age range targeted," when "their personal data is being collected." S. 3281, 2023-2024 Reg. Sess., § 4 (N.Y. 2023). And Wisconsin has proposed a law that would require social media platforms to create a "youth account" designation that comes with a suite of protections for young users. Assemb. B. 373, 2023-2024 Legis., § 1(3) (Wis. 2023).

In addition to new laws and proposals, states are using preexisting laws to hold online service providers accountable. This year, a bipartisan coalition of 33 attorneys general filed a 54-claim complaint against Meta for violating the Children's Online Privacy Protection Act and various state unfair-practices laws through the deployment of dark patterns and the unlawful collection of children's data. *See generally* Complaint for Injunctive and Other Relief, *supra*. The complaint alleges that Meta "has profoundly altered the psychological and social realities of a generation of young Americans" while "repeatedly misle[ading] the public about the substantial danger" of its platforms. *Id.* at 1. That complaint joins 140 other actions brought on behalf of individuals, school districts, and states' attorneys general, which are being heard together in a multidistrict litigation proceeding in the U.S. District Court for the Northern District of California. *See In re Soc. Media Adolescent/Pers. Inj. Prods. Liab. Litig.*, No. 4:22-MD-3047, 2023 WL 7524912, at *1 (N.D. Cal. Nov. 14, 2023). These other actions charge five social

media companies—including the owners of Instagram, YouTube and TikTok—with violations of state products-liability and tort law by allegedly "creat[ing] a youth mental health crisis" through their addictive platforms. *Id.* at *2. Another bipartisan group of states filed analogous complaints in their respective state courts. *See* Press Release, Off. of Att'y Gen. for N.J., *AG Platkin, 41 Other Attorneys General Sue Meta for Harms to Youth from Instagram, Facebook* (Oct. 24, 2023), https://tinyurl.com/3ub92vr8.

These varied state laws and enforcement actions target an array of online harms through differing strategies. Yet they share a core understanding that meeting the threats faced by young people online requires the creative deployment of the sovereign powers of the states to protect their most vulnerable residents.

III. The District Court's Flawed Analysis Could Undermine These Vital Regulatory Efforts.

The district court's reasoning threatens to upend these many state efforts to protect children online. Despite the distinct First Amendment issues presented by CAADCA's various requirements—requiring a tailored analysis for each provision—the court subjected the entire Act to the same exacting scrutiny and struck it down. But a review of CAADCA's individual provisions shows that many are straightforward disclosure or consumer-protection rules, merely applied to a new context. This Court should correct the district court's missteps to avoid impeding ongoing efforts to address online harms.

A. The court elided relevant distinctions among CAADCA's provisions and applied an incomplete reading of the First Amendment.

To determine whether a law violates the First Amendment, courts must resolve two questions. First, courts must decide whether the First Amendment is appropriately invoked at all, as "there are many, many uses of language, the regulation of which is generally understood to raise *no* First Amendment issues." Ashutosh Bhagwat, *When Is Speech Not "Speech,"* 78 Ohio St. L.J. 839, 843 (2017). If the First Amendment *does* apply, courts must then determine how stringently to scrutinize the speech regulation—a test that varies based on the type of speech and restriction at issue. *See NetChoice, L.L.C. v. Moody*, 34 F.4th 1196, 1226 (11th Cir. 2022) (courts must "proceed on a . . . nuanced basis to determine what sort of scrutiny each provision—or category of provisions—triggers"), *cert. granted*, No. 22-277 (U.S. Sept. 29, 2023). That fine-grained analysis is even more important when evaluating regulations of the Internet, a domain that is "so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." *Packingham v. North Carolina*, 582 U.S. 98, 105 (2017).

The district court's reasoning fails to heed this warning at both steps of the First Amendment analysis. Observing only that CAADCA "limit[s] the availability and use of information" through certain prohibitions and "regulate[s] the distribution of speech" through certain mandatory reporting requirements or default settings,

ER 14 (internal quotation marks omitted), the court concluded that all of the challenged provisions received First Amendment protection, *see* ER 16-17. But, on that logic, virtually all regulations of the modern information economy would be subject to judicial scrutiny. Even assuming the First Amendment does apply, the court further erred in assuming that its only real choice was to decide whether to evaluate the *entire* law under strict scrutiny or the "lesser standard of intermediate scrutiny for commercial speech" as outlined in *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980)—a false binary that overlooked other relevant standards. *See* ER 19. Three notable examples from the district court's analysis demonstrate how these fundamental errors pervade its decision.

1. Mandatory reports and disclosures

Several provisions of CAADCA require covered businesses to provide certain information to consumers or regulators. Most prominently, Sections 1798.99.31(a)(1)-(4) of CAADCA require businesses to complete a DPIA for each "online service, product, or feature." Cal. Civ. Code § 1798.99.31(a)(1)(A). These DPIAs must address multiple types of risk, including from targeted advertising systems, addictive design features, and the collection of sensitive personal information. *See id.* § 1798.99.31(a)(1)(B)(i)-(viii). Businesses must then "create a timed plan to mitigate or eliminate the risk" outlined in the DPIA before offering the

online service, product, or feature, *id.* § 1798.99.31(a)(2), and must be prepared to make the DPIAs available to the California Attorney General on request, *see id.* § 1798.99.31(a)(3)-(4). The district court invalidated these provisions by applying intermediate scrutiny from *Central Hudson*, holding that they did not "directly advance the government's substantial interest in promoting a proactive approach to the design of digital products, services, and feature[s]." ER 22.

This analysis is erroneous for multiple reasons. The court's first error was to hold that the First Amendment necessarily applies to DPIAs at all. The sum total of the court's reasoning on this point was that a DPIA "facially requires a business to express its ideas and analysis about likely harm" and thus "regulate[s] the distribution of speech." ER 14. But that cannot be correct. Mandatory reporting requirements are common across the economy, from banking, *see Reporting Forms*, Fed. Fin. Insts. Examination Council, https://www.ffiec.gov/forms041.htm (mandatory reports for banks covered by the Federal Deposit Insurance Corporation), and securities, *see Exchange Act Reporting and Registration*, U.S. Sec. & Exch. Comm'n (April 6, 2023), https://tinyurl.com/bdcrwa4f (detailed reporting requirements for public companies), to commercial transport, *see* 49 C.F.R. § 396.11(a) (driver vehicle inspection reports required of drivers of commercial motor carriers). Federal law even requires publicly listed companies to include in their annual reports "a discussion of the material factors that make an

investment" in the company "speculative or risky" and how each risk "affects the [company] or the securities being offered." 17 C.F.R. § 229.105(a), (b). If requiring a business to "express its ideas and analysis about likely harm" were enough to invoke the First Amendment, vast areas of uncontroversial federal and state regulation in diverse industries could be subject to constitutional challenge.

Yet the district court failed to explain how DPIAs differ materially from other mandatory reports or disclosures. Indeed, DPIAs under California's law are even *less* likely candidates for commercial-speech scrutiny than, for example, securities disclosures because DPIAs are made available only to the Attorney General—not the general public. *See* Cal. Civ. Code § 1798.99.31(a)(3)-(4); *id.* § 1789.99.31(a)(4)(B) (DPIAs are confidential and exempt from the California Public Records Act); *see Full Value Advisors, LLC v. SEC*, 633 F.3d 1101, 1109 (D.C. Cir. 2011) (applying rational-basis review to certain U.S. Securities and Exchange Commission ("SEC") disclosures made only to the SEC).

Moreover, even if DPIAs did qualify as commercial speech, they should be evaluated under the standard for compelled commercial speech, *see Zauderer v. Off. of Disciplinary Couns. of the Sup. Ct. of Ohio*, 471 U.S. 626, 651 (1985), not the more exacting *Central Hudson* standard applicable to *restrictions* on commercial speech. Under *Zauderer*, businesses may be required to disclose information about a product or service if the disclosure is "(1) purely factual, (2) noncontroversial, and

(3) not unjustified or unduly burdensome." *Am. Beverage Ass'n v. City and County of San Francisco*, 916 F.3d 749, 765 (9th Cir. 2019). This more forgiving standard makes sense. As the *Zauderer* Court explained, "because the extension of First Amendment protection to commercial speech is justified principally by the value to consumers of the information such speech provides," a business's "constitutionally protected interest in *not* providing any particular factual information" is "minimal." *Zauderer*, 471 U.S. at 651; *see* Robert Post, *Compelled Commercial Speech*, 117 W. Va. L. Rev. 867, 877 (2015) ("Regulations that force a speaker to disgorge more information to an audience do not contradict the constitutional purpose of commercial speech doctrine. They may even enhance it.").

Under the *Zauderer* standard, the provisions here pass constitutional muster. The district court "accept[ed] the State's statement of the harm it seeks to cure," yet it invalidated the DPIA provisions on the basis that they do not "directly and materially" advance California's stated interest. ER 22. Even assuming that is true, *Zauderer* does not require such close tailoring, instead focusing attention on whether the compelled disclosure is factual, noncontroversial, and not unjustified or unduly burdensome. *Cf. Am. Meat Inst. v. U.S. Dep't of Agric.*, 760 F.3d 18, 26 (D.C. Cir. 2014) (en banc) (noting that compelled truthful disclosure "will almost always demonstrate a reasonable means-ends relationship"). Those first two conditions are met here: the DPIA provisions require businesses to provide factual information

about well-documented harms and ways to mitigate them. What is more, because the compelled speech at issue here is to California, not the consumer, there is even less danger that businesses' own commercial messages will be unduly burdened. *See Milavetz, Gallop & Milavetz, P.A. v. United States*, 559 U.S. 229, 250 (2010) (equating the "unduly burdensome" requirement with the "chilling [of] protected speech"). The district court's confusion over the type of speech at issue in the DPIA provisions resulted in the erroneous application of an overly stringent level of commercial-speech scrutiny.

The district court's failure to appreciate the doctrinal differences between *compulsions* and *restrictions* of commercial speech also impoverishes its analysis of other provisions of CAADCA that "require businesses to affirmatively provide information to users." ER 15. Those provisions require covered businesses to publish their privacy policies in age-appropriate language, *see* Cal. Civ. Code § 1798.99.31(a)(7), mandate the use of "an obvious signal" to children when their guardian can monitor their activity or track their location, *id.* § 1798.99.31(a)(8), and require providing "prominent, accessible, and responsive tools" to children and their guardians to "exercise their privacy rights and report concerns," *id.* § 1798.99.31(a)(10). Even if each of these provisions were properly analyzed under the First Amendment, mandatory disclosures of this type have long been thought unproblematic. *See Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 138 S. Ct. 2361,

2376 (2018) ("[W]e do not question the legality of health and safety warnings long considered permissible, or purely factual and uncontroversial disclosures about commercial products."). By ensuring that adequate and accurate information is available for consumers to assess online businesses' services or products, these provisions align with the values of commercial-speech doctrine. *See Zauderer*, 471 U.S. at 651. The district court's suggestion to the contrary was erroneous.

2. "Dark patterns"

The district court also held that Section 1798.99.31(b)(7)—which prohibits businesses from using "dark patterns to lead or encourage children . . . to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or wellbeing"—"fails commercial speech scrutiny." ER 33. Yet nowhere in the opinion does the court explain how, if at all, "dark patterns" qualify as speech under the First Amendment or, if they do, why *Central Hudson* scrutiny should apply. Although the constitutional status of dark patterns is unresolved,[3] *see* Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 Fordham L. Rev. 129, 133 (2019) ("[C]ourts have hardly begun to address the First Amendment status of software's technical and nonexpressive components."),

[3] The separate and distinct question of whether online companies' *content-moderation* decisions are constitutionally protected is before the U.S. Supreme Court this term. *See Moody v. NetChoice*, No. 22-277 (U.S.); *NetChoice v. Paxton*, No. 22-555 (U.S.).

even a cursory examination of the issue reveals that the court's analysis misses the mark.

First, dark patterns should not be considered "speech" at all for the purposes of the First Amendment. The district court credited testimony that dark patterns are "*design features* that 'nudge' individuals into making certain decisions, such as spending more time on an application." ER 33 (emphasis added); *see also supra* pp. 11-12. But features of a website designed to manipulate individuals are a type of commercial conduct, not speech, and "the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567 (2011). Indeed, in the context of a Section 230 challenge to certain Snapchat design features, *see* 47 U.S.C. § 230, this Court held that the allegations asserted a cause of action for negligent design—"a common products liability tort"—and did not seek to hold Snapchat liable "as a publisher or speaker." *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1092 (9th Cir. 2021). So too here: Section 1798.99.31(b)(7) holds an online business liable in "its distinct capacity as a product designer," *id.*, not as a speaker.

Second, even if dark patterns qualified as commercial speech under the First Amendment—as the district court assumed—they do not merit protection. For one thing, false or misleading commercial speech may be restricted without "constitutional objection" because commercial-speech protections are premised on

"accurately inform[ing] the public about lawful activity." *Central Hudson*, 447 U.S. at 563. Like misleading advertising, dark patterns "frustrate[] listeners' interests by seeking to covertly influence those listeners' choices to the speaker's advantage without their conscious awareness and by targeting and exploiting their vulnerabilities." Helen Norton, *Manipulation and the First Amendment*, 30 Wm. & Mary Bill Rts. J. 221, 234 (2021). Courts thus have good reason to treat manipulative commercial speech as exempted from *Central Hudson*'s standard, the same as false or misleading commercial speech.

Even if that standard applies, commercial speech "that subverts the fairness of the bargaining process may more easily survive scrutiny." Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103 Geo. L.J. 497, 541-42 (2015). The manipulative design features targeted by CAADCA easily fit this description, as they "lead or encourage" children to "provide personal information beyond what is reasonably expected to provide" the online offering. Cal. Civ. Code § 1798.99.31(b)(7). Protecting children from such coercion sits at the core of the state's police powers, yet the district court barely mentioned that important interest. Commercial actors have minimal First Amendment interests in consummating a transaction through covert "design features" that manipulate—rather than persuade—consumers.

3. Internal policy enforcement

As a final example, the district court invalidated a provision of CAADCA requiring businesses to enforce their own "published terms, policies, and community standards," Cal. Civ. Code § 1798.99.31(a)(9), on the basis that this obligation "would essentially press private companies into service as government censors," ER 15. Putting aside whether the First Amendment protects the content-moderation decisions of online companies at all, a question the Supreme Court may soon answer, *see supra* note 3, the district court still misconstrued the question.

Requiring companies to adhere to their own published policies is a staple of consumer-protection law. *See, e.g.*, D.C. Code § 28-3904; 815 Ill. Comp. Stat. 505/2. These laws ensure that consumers have an accurate understanding of the bargain when they purchase a business's goods or services. Importantly, false or misleading commercial speech—which includes "published terms, policies, and community standards" that are not, in fact, adhered to—merits no First Amendment protection. The First Amendment "does not prohibit the State from insuring that the stream of commercial information flow cleanly as well as freely." *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 772 (1976). And companies cannot immunize themselves from liability under these regulations just because the policies in question concern commercial activities that may, on their own, constitute protected speech. *See Twitter, Inc. v. Paxton*, 26 F.4th 1119, 1124-

25 ("Even if content moderation is protected speech, making misrepresentations about content moderation policies is not."), *amended and superseded on denial of reconsideration*, 56 F.4th 1170 (9th Cir. 2022). The district court's invalidation of Section 1798.99.31(a)(9) under intermediate scrutiny thus erroneously conflated businesses' speech *about* their policies with the policies themselves. In doing so, the court created a safe harbor for online businesses—uniquely among commercial actors—to violate their own policies.

B. The court's reasoning could sow chaos among states seeking to confront novel challenges in good faith.

In addition to its legal infirmities, if affirmed on appeal, the district court's decision may obstruct the numerous good-faith efforts underway across the country to address the known harms that children face online. This Court should reject the district court's overbroad reading of the First Amendment and permit the Amici States to continue developing public policy responses to the online crisis.

First, the district court's analysis of the DPIA provisions calls into question all current and future attempts to require companies to evaluate the harms of their online practices. If any regulation that "facially requires a business to express its ideas and analysis about likely harm" constitutes First Amendment speech, ER 14, that could call into question multiple state laws across the country that—like CAADCA—require regulated businesses to complete DPIAs. *See supra* note 1. It

would also place an unnecessary roadblock in front of similar legislation actively pending elsewhere. *See supra* note 2.

Likewise, the district court's assumption that "design features" implemented by online businesses should be evaluated under commercial-speech scrutiny threatens ongoing efforts to hold online companies to account for their use of dark patterns. As indicated, *supra* p.14, multidistrict litigation pending in this circuit alleges that major social-media platforms have implemented design features in their products that "appeal to and addict" children users. *In re Soc. Media Adolescent Addiction*, 2023 WL 7524912, at *2. That suit covers a number of dark patterns, including "endless content," "intermittent variable rewards," the algorithmic prioritization of content, and filters that permit the presentation of "idealized" body images. *Id.* at *3-*4. And, as noted, *supra* p.15, states are engaged in similar litigation in their own courts. For instance, the District of Columbia has filed its own suit against Meta for unfair and deceptive practices for having "knowingly designed Instagram and its other social media platforms with features that lure in and addict children and cause harm to their mental, emotional, and physical health." Press Release, Off. of Att'y Gen. for D.C., *Attorney General Brian Schwalb Sues Meta for Endangering Youth Through Addictive Social Media Platforms* (Oct. 24, 2023), https://tinyurl.com/4hkyf5t2. And just this year, a bipartisan group of U.S. Senators introduced a bill to prohibit online platforms from using dark patterns

to encourage compulsive usage of their products or manipulate consumers into divulging personal information. *See* Deceptive Experiences To Online Users Reduction Act ("DETOUR Act"), S. 2708, 118th Cong. (2023). The district court's conflation of "design features" with protected speech, with no apparent limitation, could stymie these important efforts to address the harms of dark patterns.

Finally, the district court's invalidation of the CAADCA provisions requiring online businesses to enforce their own published policies threatens to limit consumer-protection law as applied to the Internet and conflicts with the reasoning of decisions of other courts. *See Meta Platforms, Inc. v. District of Columbia*, 301 A.3d 740, 757 (D.C. 2023) (recognizing that requiring companies to adhere to their stated policies is at the heart of consumer-protection law, and such requirements in no way purport to exercise control over a company's "editorial judgment when it comes to its content moderation"); *Twitter*, 56 F.4th at 1175 (rejecting the allegation that disclosure of content-moderation decisions for the purposes of a deceptive-trade-practices claim alleges a First Amendment injury). Online companies should not be immunized from these consumer-protection laws simply because they profit from the dissemination of information.

CONCLUSION

The Court should reverse the decision below.

Respectfully submitted,

AARON D. FORD
Attorney General for the State of Nevada

HEIDI P. STERN
Solicitor General

KIEL B. IRELAND
Deputy Solicitor General

Office of the Attorney General
for the State of Nevada
100 N. Carson Street
Carson City, NV 89701
hstern@nevada.gov

BRIAN L. SCHWALB
Attorney General for
the District of Columbia

/s/ Caroline S. Van Zile
CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

RUSSELL C. BOGUE
Assistant Attorney General

Office of the Attorney General
for the District of Columbia
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-6609
caroline.vanzile@dc.gov

December 2023

KRISTIN K. MAYES
Attorney General
State of Arizona
2005 North Central Avenue
Phoenix, AZ 85004

TIM GRIFFIN
Attorney General
State of Arkansas
323 Center Street, Suite 200
Little Rock, AK 72201

PHILIP J. WEISER
Attorney General
State of Colorado
Colorado Department of Law
1300 Broadway, 10th Floor
Denver, CO 80203

WILLIAM TONG
Attorney General
State of Connecticut
165 Capitol Avenue
Hartford, CT 06106

KATHLEEN JENNINGS
Attorney General
State of Delaware
820 N. French Street
Wilmington, DE 19801

ASHLEY MOODY
Attorney General
State of Florida
PL-01, The Capitol
Tallahassee, FL 32399

KWAME RAOUL
Attorney General
State of Illinois
100 West Randolph Street
Chicago, IL 60601

ANTHONY G. BROWN
Attorney General
State of Maryland
200 Saint Paul Place
Baltimore, MD 21202

DANA NESSEL
Attorney General
State of Michigan
P.O. Box 30212
Lansing, MI 48909

KEITH ELLISON
Attorney General
State of Minnesota
102 State Capitol
75 Rev. Dr. Martin Luther
King Jr. Blvd.
St. Paul, MN 55155

LYNN FITCH
Attorney General
State of Mississippi
550 High Street, Suite 1200
Jackson, MS 39201

MATTHEW J. PLATKIN
Attorney General
State of New Jersey
Richard J. Hughes Justice Complex
25 Market Street
Trenton, NJ 08625

RAÚL TORREZ
Attorney General
State of New Mexico
408 Galisteo Street
Santa Fe, NM 87501

LETITIA JAMES
Attorney General
State of New York
28 Liberty Street
New York, NY 10005

JOSHUA H. STEIN
Attorney General
State of North Carolina
114 West Edenton Street
Raleigh, NC 27603

ELLEN F. ROSENBLUM
Attorney General
State of Oregon
1162 Court Street NE
Salem, OR 97301

MICHELLE A. HENRY
Attorney General
Commonwealth of Pennsylvania
Strawberry Square, 16th Floor
Harrisburg, PA 17120

PETER F. NERONHA
Attorney General
State of Rhode Island
150 South Main Street
Providence, RI 02903

ROBERT W. FERGUSON
Attorney General
State of Washington
P.O. Box 40100
Olympia, WA 98504

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-2969

I am the attorney or self-represented party.

This brief contains 6,474 **words,** including _____ words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Caroline S. Van Zile **Date** 12/20/2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*