No. 25-2366

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC, D/B/A NETCHOICE,
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-028861
The Honorable Beth Labson Freeman, District Court Judge

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Megan Iorio
Tom McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

Attorneys for Amicus Curiae
Electronic Privacy Information
Center

June 17, 2025

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Regulations

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC regularly participates as amicus in cases concerning the First Amendment implications of platform regulation. *See* EPIC, *The First Amendment* (2025).[2]

SUMMARY OF THE ARGUMENT

Following the Supreme Court's decision in *Moody v. NetChoice*, 603 U.S. 707 (2024), this Court directed NetChoice to build a more robust record on remand in its case challenging the California Age-Appropriate Design Code ("CAADC"). But when NetChoice returned to the district court, it did not add specificity to its legal arguments and factual assertions. Instead, it tested out a set of new legal tactics. This

---

[1] *Amicus* certifies that no person or entity, other than *Amicus*'s own staff or counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief, in whole or in part. All parties consented to the filing of this amicus brief.

[2] https://epic.org/issues/platform-accountability-governance/the-first-amendment-and-platform-regulation/.

brief concerns three of those tactics: (1) NetChoice argued that the CAADC's coverage definition renders the entire law content-based and presumptively unconstitutional; (2) NetChoice made superficial changes to the scope of its challenge to the data protection provisions at California Civil Code §§ 31(b)(1)–(4); and (3) NetChoice argued that *Moody*'s dicta renders the data protection provisions unconstitutional. The district court erroneously agreed with NetChoice on its coverage definition argument and reinstated the injunction against the data protection provision, despite finding that NetChoice had failed to meet its burden under *Moody*.

Affirming the district court's ruling that the CAADC's coverage definition renders the whole law content-based would threaten the entire regime of data protection law. Many foundational and non-controversial data protection laws, most notably the Children's Online Privacy Protection Act, contain similar types of coverage definitions. Legislatures often write data protection laws to narrowly regulate specific industries and entities for common-sense reasons related to relevance and narrow tailoring, not to censor certain topics or viewpoints. It would be nonsensical to apply strict scrutiny when, for

instance, a children's privacy law only applies to websites likely to be accessed by children, or when a video privacy law only applies to businesses that collect records of people's video-watching histories. The Supreme Court's underinclusiveness analysis is the appropriate lens for this sort of challenge, and the CAADC is not impermissibly underinclusive.

NetChoice's superficially amended challenges to the CAADC's data protection provisions otherwise fall short of the standard set in *Moody*. In its amended complaint, NetChoice challenged the data protection provisions as they apply to every use, retention, sale, and disclosure of personal information "to publish content or to make information available." FAC Prayer ¶¶ 6–7. As the district court correctly observed, it is entirely unclear what applications fall within the scope of these challenges. It is also unclear that there are any applications of the law that fall outside of these challenges, since almost everything internet companies do involves publishing content or making information available.

NetChoice also failed to show how the data protection provisions interfere with covered businesses' protected expression. The *Moody*

Court explicitly refused to recognize the rule that NetChoice attributes to it: that the use of personal information to curate content is protected editorial judgement. The Court only recognized that internet companies' content moderation practices resemble protected editorial discretion. And the CAADC's data protection provisions do not interfere with companies' content moderation practices.

The CAADC's data protection provisions protect minors' privacy by prohibiting certain invasive data practices. The provisions do not interfere with companies' protected editorial discretion. The injunction entered by the district court should be vacated and the case remanded.

ARGUMENT

I. NETCHOICE'S LEGAL THEORY WOULD RENDER MANY IMPORTANT DATA PROTECTION REGULATIONS UNCONSTITUTIONAL

The district court fundamentally mischaracterized the CAADC as a content-based speech restriction and, in doing so, has threatened decades of established data protection regulations. If selective regulation of online businesses subjects the CAADC to strict scrutiny, then numerous established data protection laws require identical treatment. All websites contain content whose subject matter varies

depending on the nature of the business. Thus, any law that regulates online businesses based on the nature of their business will also, incidentally, regulate the business based on the content they publish online. That does not mean these laws are content-based restrictions on speech deserving of strict scrutiny. There must be a distinction between highly suspect content discrimination and appropriate legislative tailoring. Otherwise, legislators face an impossible choice: apply every data protection law to every website regardless of relevance or abandon data protection altogether.

If the district court's analysis is correct, the Children's Online Privacy Protection Act ("COPPA") is also presumptively unconstitutional. Like CAADCA, COPPA only regulates "a commercial website or online service that is targeted to children." 15 U.S.C. § 6501(10). To determine whether a website is "directed to children," the Federal Trade Commission has, since COPPA was passed, examined content-related factors such as a website's subject matter, visual or audio content, language, and advertisements. Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750, 22753 (Apr. 27, 1999) (codified at 16 C.F.R. pt. 312). According to the district court, this would mean that

COPPA "divides the universe into covered and uncovered business[es] based on the type of content they publish, [so it is] content-based and subject to strict scrutiny." *See* 1-ER-19. And it is not at all clear that COPPA would pass strict scrutiny, especially as the district court applied it.

Thus, the district court's rule would lead to a cornerstone of children's privacy protection that has operated successfully for decades being, instead, presumptively unconstitutional and likely invalid. This would be an absurd outcome. Like the CAADC, identifying which companies must comply with COPPA might involve evaluating the content of websites, but the objective is to identify which websites are actually likely to have child users who need additional privacy protections, not to burden speech on topics that interest children. Something is awry with a rule that would put into question the constitutionality of a non-controversial, long-standing, and fundamentally important privacy statute.

The district court's analysis would similarly undermine other well-established data protection laws, despite the fact that courts have repeatedly found these same laws constitutional. The Video Protection

Privacy Act ("VPPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Fair Credit Reporting Act ("FCRA") all "divide the universe into covered and uncovered business[es] based on the type of content they publish." The VPPA only regulates entities that compile records of consumers' video viewing histories, Video Privacy Protection Act, 18 U.S.C. § 2710(a)(3); HIPAA only applies to "covered entities" that collect personal health information such as healthcare providers and insurers, 45 C.F.R. § 160.103; and the FCRA only applies to entities that compile credit reports, Fair Credit Reporting Act, 15 U.S.C. § 1681. Consequently, each of these laws could be characterized as applying to internet companies depending on the type of content they publish. The VPPA only applies to companies that publish videos; HIPAA only applies to companies that publish health information; and FCRA only applies to companies that publish credit reports. But that does not mean that each of these laws is content-based. Indeed, no court has found it appropriate to subject the VPPA, HIPAA, or FCRA to strict scrutiny as a content-based restriction. *See Trans Union v. FTC*, 267 F.3d 1138, 1141–42 (D.C. Cir. 2001); *Stark v. Patreon*, 656 F. Supp. 3d 1018, 1034 (N.D. Cal.

2023); *King v. Gen. Info. Servs., Inc.*, 903 F. Supp. 2d 303, 307 (E.D. Pa. 2012). Far from it, courts have overwhelmingly found that these laws are subject to and survive intermediate scrutiny. *See Trans Union*, 267 F.3d at 1142–43; *Stark v. Patreon*, 656 F. Supp. 3d at 1034; King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d at 310.

When data protection laws regulate specific entities, they usually do so for good reason: relevance and appropriate tailoring. Forcing websites that children do not use to develop child-protective privacy measures would be irrational, overbearing, and even potentially unconstitutionally overbroad if the law incidentally burdens speech. A narrow focus, reflected in a targeted coverage definition, is commonsensical and typical of data protection regulations. Netflix should not need to comply with HIPAA's medical privacy requirements because it does not handle health information, and the local library should not need to follow FCRA credit reporting rules because it does not assess people's creditworthiness. The lower court's coverage definition rule would create the wrong incentives: The only way to avoid strict scrutiny would be to make all internet companies subject to each

data protection law, even if doing so makes little sense and is not tailored to the harm sought to be addressed.

Typically, the Supreme Court analyzes laws that regulate the expression of some entities but not others according to its underinclusiveness doctrine. The Court is generally skeptical of underinclusiveness claims because of the conflict inherent in arguing that a law violates the First Amendment because it regulates too little speech. *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 448 (2015). In such circumstances, the Court has looked to whether the law is so underinclusive that it suggests that the legislature's true reason for regulating was to burden disfavored speech or disfavored speakers. *Id.*; *see also Sorrell v. IMS Health*, 564 U.S. 552, 564 (2011) (finding that a data protection law triggered First Amendment scrutiny because the law only restricted data access for disfavored speakers with a disfavored message); *Ark. Writers' Project, Inc. v. Ragland*, 481 U.S. 221, 229 (1987) (invalidating a tax that "targed[ed] a small group within the press" for disfavored treatment based on the content of the publication); *Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 592 (1983) (invalidating a tax that targeted only a small group of

newspaper publishers because it "select[ed] a narrowly defined group to bear the full burden" and was "more a penalty for the few" than an attempt to address any legitimate state interest). The CAADC does not unfairly target a small group of websites for disfavored treatment, nor is there any evidence that the CAADC was intended to suppress any viewpoint. It thus lacks the characteristics of a law with constitutionally suspect coverage.

Recently, the Supreme Court demonstrated that the bar for finding a data protection statute impermissibly underinclusive is very high. In *TikTok v. Garland*, the Supreme Court considered the constitutionality of Congress's law forcing TikTok's parent company to divest or for the app to be banned in the United States—the so-called "TikTok divest-or-ban law." 145 S.Ct. 57 (2025) (per curiam). Congress justified the law based on the threat to user privacy from Chinese ownership of the company. *Id.* at 62. TikTok argued that the divest-or-ban law impermissibly "focus[ed] on applications with user-generated or user-shared content" and included exemptions "for certain review platforms." *Id.* at 70. The Court rejected this argument, finding that the government "had good reason to single out TikTok for special

treatment." *Id.* The Court applied intermediate scrutiny because the law was justified on content-neutral privacy grounds, *id.* at 68–69, bolstering the argument that data protection laws are subject to, at most, intermediate scrutiny.

Applying strict scrutiny to any data protection law that regulates a subset of expressive websites would undermine the entire data protection regulatory framework. Under strict scrutiny, there is almost always a theoretically less restrictive alternative when it comes to data protection. A law that prohibits harmful data practices might be less restrictive if it allowed users to opt *in* instead. A law that allows users opt in to harmful data practices could be challenged as more restrictive than one that opts users in by default and provides the option to opt out. And a law that allows users to opt-out of harmful data practices might be less restrictive if it merely allocated funds to educating users about privacy risks. The end of this slippery slope would be the end of privacy law as we know it.

The district court's rule cuts against history, tradition, common sense, and Supreme Court caselaw, all of which counsel that data protection laws may coexist with the First Amendment. This Court's

ruling should be careful not to upend the entire edifice of data protection but, instead, reserve strict scrutiny for laws that actually threaten speech.

II. NETCHOICE HAS NOT RECTIFIED FATAL FLAWS IN ITS CHALLENGE TO THE DATA PROTECTION PROVISIONS.

California Civil Code sections 1798.99.31(b)(1)-(4) limit covered businesses' collection, use, retention, sale, and disclosure of minors' personal information. These provisions are, at their core, data protections that limit harmful data practices and bolster minors' privacy and autonomy online. NetChoice's amended complaint claims that the provisions burden the editorial discretion of all covered businesses (or, alternatively, all covered businesses who are members of NetChoice). But these challenges lack the specificity and evidentiary support required under *Moody v. NetChoice* and this Court's previous decision in this case.

First, instead of supplementing the record or tailoring its claims to specific applications of the law as required by *Moody*, NetChoice added a few rhetorical flourishes to its challenges to the data protection provisions that do not meaningfully limit its request for relief. Second,

the Supreme Court's guidance in *Moody* does not support NetChoice's request for relief from the data protection provisions. The Court only recognized the expressiveness of internet companies' decisions to remove or downrank content that violates their content policies and explicitly did not recognize the expressiveness of other content curation practices like surveillance targeting. Third, the CAADC's data protection provisions protect minors' important privacy interests and do not burden companies' protected editorial judgement as recognized in *Moody*.

A. NetChoice did not build a robust record as required by *Moody v. NetChoice* or meaningfully limit its challenges to the data protection provisions on remand.

Moody v. NetChoice set out a rigorous standard for First Amendment facial challenges. The Ninth Circuit previously recognized that NetChoice failed to meet this standard in its facial challenge to the CAADC's data protection provisions and remanded the case for NetChoice to further develop the record and arguments. NetChoice did not cure the defects in its challenge on remand. As the district court rightly observed, the scope of NetChoice's facial and as-applied

challenges to the data protection provisions continue to be "amorphous." 1-ER-33. NetChoice does not sufficiently describe which activities, by which actors, are within the scope of its challenges, and how those activities are protected speech.

In *Moody*, the Supreme Court explained that facial challenges are "disfavored," 603 U.S. at 744, because they "often rest on speculation" and "threaten to short circuit the democratic process by preventing duly enacted laws from being implemented in constitutional ways." *Id.* at 723 (internal citations omitted). The decision to challenge a statute on its face thus "comes at a cost." *Id.* That cost is a heightened evidentiary burden. The challenger must establish "what activities, by what actors, the law[] prohibit[s] or otherwise regulate[s]," *id.* at 724, "whether there is an intrusion on protected [speech]" for each of these activities by each of these actors, *id.* at 708, and "measure the constitutional against the unconstitutional applications," *id.* at 724.

Following *Moody*, this Court vacated the previous injunction against the CAADC's data protection provisions because NetChoice had not shown that the provisions "necessarily impact protected speech in all or even most applications." *NetChoice v. Bonta*, 113 F.4th 1101, 1123

(2024). The panel noted that the district court's previous decision was based on "speculation" about how "the editorial decisions of social media companies" might be impacted by the law and did not "consider[] any other potential applications." *Id.*

Given this Court's previous decision in this case, NetChoice had two options to cure defects in its challenges against the data protection provisions on remand: build a robust record evidencing "what activities, by what actors, the law[] prohibit[s] or otherwise regulate[s]," *Moody,* 603 U.S. at 724, and "whether there is an intrusion on protected" expression for each of these activities by each of these actors, *Id.* at 708, or limit the scope of its challenge to applications it could support with specific record evidence and constitutional arguments. NetChoice chose a third path: add rhetorical flourishes that only superficially limit the scope of its challenges.

In the amended complaint's prayer for relief, NetChoice superficially narrowed its facial challenge by asking the district court to enjoin the data protection provisions "to the extent those sections apply to covered services' use of personal information" and "retention, sale, and sharing of personal information" "to publish content or to make

information available." FAC Prayer ¶¶ 6–7. NetChoice also asked the court to enjoin the provisions "as applied to covered NetChoice members' practices to do so." *Id.* These changes do not meaningfully narrow NetChoice's previous claims. As this Court has recognized in other contexts, "publishing content" describes "just about everything [an internet company] is involved in." *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1092–93 (9th Cir. 2021). "Making information available" is a similarly broad and vague category of conduct that could include every action a company takes involving users' personal information. It is thus unclear which, if any, uses of personal information by covered businesses or by NetChoice's members fall outside the scope of NetChoice's challenges.

What's more, NetChoice did not limit the covered businesses within the scope of its facial challenge. The CAADC applies to a broad range of businesses, all of which publish content or make information available to users because they all operate on the internet. *See* Am. Compl. ¶ 26 (admitting that the CAADC "extends so widely as to sweep in the vast majority of companies operating online.") NetChoice did not attempt to describe how every category of covered business uses, retains, sells, or shares the personal information of minors to publish

information, how each of these practices is expressive, and how the CAADC interferes with this expression, as required under *Moody*.

Even NetChoice's as-applied challenge is insufficiently detailed. NetChoice did not identify which of its members are within the scope of its as-applied challenge, and because NetChoice's members are very diverse, the as-applied challenge sweeps nearly as broadly as the facial challenge. NetChoice's members include not just social media companies but also home rental services like Airbnb, HomeAway, and VRBO; travel booking sites like Travelocity, Expedia, and Hotels.com; ride booking apps like Lyft; ticket brokers like StubHub; online marketplaces like Etsy and Amazon; financial services companies like PayPal and EarnIn; telehealth companies like Hims & Hers; and sports betting websites like PrizePicks. *See* NetChoice, *About Us* (2025).[3] At least some of these non-social-media websites are likely to be subject to the CAADC. The way each of these companies use minors' personal information to publish content likely varies wildly. NetChoice did not

[3] https://netchoice.org/about/#association-members.

explain how any of these companies' data practices is expressive or how the CAADC interferes with that expression.

Instead of supplementing the record on remand with declarations from representative covered businesses, NetChoice filed supplemental declarations from two companies that had previously submitted declarations, *see* Paolucci Supp. Decl.; Masnick Supp. Decl., and otherwise relied on the evidence it submitted alongside its original complaint and motion for a preliminary injunction. That evidence comprised declarations from four companies: Dreamwidth, a social media website (Paolucci Decl.); TechDirt, an online blog (Masnick Decl.); IMDb, an online database of film and television (Cairella Decl.); and GoodReads, a book review website (Roin Decl.). These four companies are not representative of the CAADC's covered businesses or NetChoice's members. Dreamwidth is not even representative of covered social media companies, since it does not serve ads, Paolucci Decl. ¶ 3, does not "'recommend' accounts or content to users," *id.* ¶ 7, and does not "offer any 'algorithmic timeline'" that uses personal information to select content for users, *id.* The company otherwise collects and uses limited personal information, *id.* ¶ 4; Paolucci Supp.

Decl. ¶ 9, and it is not clear that any of its data practices are protected expression or that the CAADC interferes with them. Techdirt similarly collects and uses very little personal information, *see* Masnick Decl. ¶ 10; Masnick Supp. Decl. ¶ 9, and it is also not clear that any of its practices are protected expression that violate the CAADC.

In sum, NetChoice did not address the flaws this Court found in its previous challenge to the CAADC's data protection provisions. NetChoice has, essentially, renewed its overbroad challenge without following the requirements in *Moody v. NetChoice* for making such a challenge, recreating the same error that led this Court to vacate the injunction and remand the case the first time around.

B. In *Moody v. NetChoice*, the Supreme Court explicitly questioned whether the use of personal information to curate content is expressive.

In addition to finding that the evidentiary record does not support NetChoice's broad challenges to the data protection provisions, this Court should also reject NetChoice's underlying First Amendment theory, which relies on a misapplication of *Moody*. *Moody* does not support NetChoice's challenge to the data protection provisions. The

Moody Court, unlike NetChoice, approached the question of internet companies' protected editorial discretion in a nuanced way. The Court recognized that there were constitutionally salient distinctions between companies' content moderation practices and their uses of personal information to curate content. *Moody*, 603 U.S. at 736 n.5. These distinctions matter because the CAADC's data protection provisions may limit companies' use of personal information, but they do not burden their content moderation.

In dicta, the *Moody* Court identified a narrow category of platform publishing decisions that deserve First Amendment protections: content moderation decisions. Content moderation involves removing or downranking content that violates a company's content policies, which "list the subjects or messages the platform prohibits or discourages—say, pornography, hate speech, or misinformation on select topics." *Moody*, 603 U.S. at 719. The *Moody* Court signaled that content moderation is a type of protected editorial discretion. "When the platforms *use their Standards and Guidelines to decide* which third-party content those feeds will display, or how the display will be ordered and organized, they are making expressive choices." *Id.* at 740

(emphasis added). In the Court's view, a social media company, through content moderation systems, decides "whether—and, if so, how—to convey posts having a certain content or viewpoint," and "[t]hose choices rest on a set of beliefs about which messages are appropriate and which are not." *Id.* at 738. A company that does not want to spread pro-Nazi beliefs, say, acts expressively when excluding pro-Nazi media. A law that "direct[s] a company to accommodate messages it would prefer to exclude," like pro-Nazi content, thus infringes on the company's protected editorial discretion. *Id.* at 731. Protecting internet company's content moderation decisions under the First Amendment is a straightforward application of decades of Supreme Court precedent recognizing the rights of speech compilers to exclude messages and viewpoints they do not wish to carry. *See id.* at 728–33 (discussing the Court's editorial discretion precedent).

Content moderation is a distinct practice from the use of personal information to select content for users. This latter practice, which we refer to as "surveillance targeting," uses information collected through the surveillance of user behavior to select content that will lead to a desired behavior in the user. Surveillance targeting is used in a wide

variety of contexts, including social media feeds, product recommendation features, advertising, and search engine results. A popular type of surveillance targeting is the engagement-maximizing algorithm, which social media companies use to predict what content users will most likely interact with based on their past behavior on the website. *See* Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, The Knight First Amendment Institute at Columbia University 20 (2023).[4] Maximizing for engagement maximizes a user's time on the platform which, in turn, maximizes the ad revenue the user generates for the company. *See* Ravi Iyer, *Feed Algorithms Contain both Expressive and Functional Components*, USC Neely Center for Ethics and Technology (Dec. 10, 2024).[5] Surveillance advertising also relies on a wide range of personal information collected from tracking users around the web, which is used to profile a user and

---

[4] https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf.
[5] https://neely.usc.edu/2024/12/10/algorithms-contain-both-expressive-and-functional-components/.

determine what ad the user is most likely to click on. *See* EPIC, *Online Advertising & Tracking* (2025).[6]

In contrast to content moderation, which evaluates the message expressed by media and how that message will affect the feed's overall message, surveillance targeting algorithms do not evaluate the viewpoint, topic, or quality of media. The algorithms, according to at least one major social media company, are "content-neutral." Compl. ¶ 160, *Massachusetts v. TikTok Inc., et al.*, No. 2484-cv-2638-BLS-1 (Mass. Sup. Ct. Feb. 3, 2025). The primary fuel for surveillance targeting is user behavioral data collected through surveillance, not explicit user feedback or the topic, meaning, or viewpoint of content. *See* Narayanan, *supra*, at 18. Companies use surveillance targeting not to shape a coherent message out of the media selected but to accomplish the functional task of inducing profitable user behavior. *See* Iyer, *supra*; *see generally* Brett Frischmann & Evan Selinger, *Re-Engineering*

---

[6] https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/.

Humanity (2018). Any message goes—including content that violates the company's own policies—so long as it maximizes user engagement.

The *Moody* Court recognized that surveillance targeting is distinct from content moderation and that this distinction is constitutionally salient. The Court explicitly reserved the question of whether the use of "algorithms [that] respond solely to how users act online" is protected editorial discretion. *Moody*, 603 U.S. at 736 n.5. As Justice Barrett wrote in her concurrence, "The First Amendment implications . . . might be different" for "a platform's algorithm [that] just presents automatically to each user whatever the algorithm thinks the user will like—e.g., content similar to posts with which the user previously engaged." *Id.* at 746 (Barrett, J., concurring).

Because *Moody* does not establish that surveillance targeting is protected editorial judgement, NetChoice must make an independent argument for such a rule. Because NetChoice has failed to make such an argument, its First Amendment challenge should be rejected.

As it stands, though, there is little to suggest that surveillance-targeting algorithms, on their own, express any message of a company. Surveillance targeting algorithms are often created using machine

learning techniques that involve a computer deciding the rules for what content to include or exclude from a given user's feed. *See* Mackenzie Austin & Max Levy, *Speech Certainty: Algorithmic Speech and the Limits of the First Amendment*, 77 Stan. L. Rev. 1, 39–43 (2025). Because it is not clear that these decisions can be attributed to any human, it is not clear that they reflect human expression—the only kind of expression the First Amendment protects. *See Moody*, 603 U.S. at 746 (Barrett, J., concurring); *Id.* at 795 (Alito, J., concurring in the judgement).

The choices that the algorithms make also do not resemble exercises of protected editorial discretion. The algorithms do not choose or rank content based on agreement or disagreement with the message expressed, only based on a user's likelihood of interacting with the media. Perhaps the most damning evidence against the expressiveness of engagement maximization is that platforms' recommendation algorithms often promote content that violates the company's guidelines or otherwise undermines the company's express priorities. *See, e.g.,* Sam Schechner et al., *How Facebook Hobbled Mark Zuckerberg's Bid to*

Get America Vaccinated, Wall St. J. (Sep. 17, 2021);[7] Keach Hagey & Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*, Wall St. J. (Sep. 15, 2021).[8] How can the recommendation algorithm's amplification of messages the company says it disagrees with be expressive of the company's message? This conflict exists precisely because the algorithms choose media for display without regard for the underlying message expressed.

While it is true that a company may be engaged in both content moderation and surveillance targeting in the same feed, these two functions are not inextricably intertwined. A company could simply remove the surveillance targeting function from the feed, leaving the content moderation function intact. A company can also take into account a user's express preferences—which creators or posters a user follows, what issues or topics they want to see more or less of, and any other explicit signals of preference users provide to a company—without

---

[7] https://www.wsj.com/articles/facebook-mark-zuckerberg-vaccinated-11631880296.
[8] https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

engaging in surveillance targeting. Iyer, *supra*. Indeed, relying on express preferences, instead of surveillance targeting, was the prevailing model for personalized feeds until just a few years ago. *Id.* Without surveillance targeting, personalized feeds would reflect a users' actual preferences—not assumptions companies make about user preferences.

C. The CAADC's data protection provisions protect fundamental privacy interests and do not burden content moderation.

The CAADC's data protection provisions protect minors from privacy harms stemming from the misuse of their data. These provisions are similar to provisions found in other data protection laws. Nothing in the CAADC's data protection provisions would burden companies' rights to include, exclude, promote, or downrank messages the companies agree or disagree with. Companies do not generally use the personal information of users to moderate content—they use community feedback, algorithmic screening, and human intervention. *See* Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 Yale L.J. 2418, 2429–34 (2020). NetChoice certainly has not provided any

examples of how the data protection provisions would prevent companies from enforcing their content policies. To the extent the CAADC's data protection provisions impact content curation, they limit surveillance targeting, not content moderation.

1. Section 31(b)(1) restricts harmful uses of personal information, not the use of personal information to deliver harmful content.

Section 31(b)(1) prohibits covered entities from "us[ing] the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child." The provision prohibits *uses of personal information* that the business "knows, or has reason to know" are harmful to children. It does not, as NetChoice asserts, prohibit companies from "using a minor's personal information (including an IP address and browsing history) to deliver *content* the provider 'knows, or has reason to know, is materially detrimental' to the minor's 'well-being.'" 2d Mot. for Prelim. Inj. at 6 (emphasis added). Even if NetChoice's interpretation were permissible, and that interpretation were unconstitutional, the doctrine of constitutional avoidance compels the Court to avoid construing the statute in this way when other

constitutional constructions exist. *See Nat'l Fed'n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 574 (2012) (explaining a "duty to construe a statute to save it.").

Properly understood, § 31(b)(1) does not interfere with a company's right to include or exclude certain messages as recognized in *Moody*. It requires companies to change their data practices if they find those data practices harm minors, not to remove or downrank any content. For example, companies sometimes conduct experiments to see what impact changing their curation algorithms has on users. *See* Natasha Singer, *LinkedIn Ran Social Experiments on 20 Million Users Over Five Years*, N.Y. Times (Sept. 24, 2022).[9] If Meta were to discover through an experiment that including a certain category of data in its algorithm, such as "time spent lingering on a piece of content," led more girls to report high levels of anxiety, then § 31(b)(1) would require Meta not to use this data. Meta would not have to remove or downrank any content, nor would it have to change how it enforced its content policies.

---

[9] https://www.nytimes.com/2022/09/24/business/linkedin-social-experiments.html.

Indeed, content may not even be involved, since the anxiety could be caused by the girls' increased inability to turn social media off, and the follow-on effects of that on their sleep, schoolwork, and social lives.

NetChoice's hypothetical applications of this provision that purport to show its constitutional issues involve harmful *content*, not harmful *uses of personal information*. Using an IP address to deliver content is not a harmful use of personal information—it is technically necessary. Using browsing history to curate content is also not known to categorically harm the physical health, mental health, or well-being of minors. Even if using browsing history to curate content *were* categorically harmful to minors, NetChoice hasn't shown that this practice is expressive. As explained in Section I above, using browsing history to maximize engagement is not expressive. And even if using browsing history to curate content were, sometimes, expressive, and some of those applications were proscribed by § 31(b)(1), they would just be a few of the many, many applications of the provision, all of which would need to be weighed to decide NetChoice's facial challenge—which is impossible to do given the paucity of the record and arguments NetChoice provided in the district court.

2. Section 31(b)(2) requires companies to turn profiling off by default.

Section 31(b)(2) prohibits companies from "profil[ing] a child by default" unless the company can meet one of two enumerated exceptions. "Profiling" means the "automated processing of personal information to evaluate certain aspects related to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Cal. Civ. Code § 30(b)(6). This is exactly what surveillance targeting does: it profiles users to predict what content will keep them on the platform longer or what advertisements they are most likely to click on. *See* Part II.B, *supra*. The provision does not interfere with companies' ability to use algorithms to remove or downrank content that violates their guidelines. The provision also does not "end content personalization for minors." 2d Mot. for Prelim. Inj. at 7. Instead of using behavioral data to profile minors, companies can, instead, take users' explicit preferences into account by asking minors what creators they wish to

follow, what categories of content they wish to see in their feeds, and what they want to see more or less of.

In the advertising space, § 31(b)(2) would force companies to turn surveillance advertising off by default for minors. Doing this does not prevent companies from serving ads on their platforms. Companies can still provide contextual advertising, which serves ads that are relevant to the contents of a website and are not based on user profiles. *See* Nathalie Maréchal & Nick Doty, *Defining Contextual Advertising*, Ctr. for Democracy & Tech. 3 (Aug. 2024).[10]

Section 31(b)(2) also only dictates a *default setting* that companies only need to implement when profiling is not necessary to provide the feature the minor is actively engaged with. Minors can turn profiling on if they choose. NetChoice does not explain how letting minors decide whether to allow profiling impacts any companies' speech, especially when the profiling is unnecessary. Profiling that is necessary to provide the feature the minor is actively engaged in is also allowed by default. §

---

[10] https://cdt.org/wp-content/uploads/2024/08/2024-08-13-PD-Defining-Contextual-Advertising-Brief-final.pdf.

31(b)(2)(B)(i). NetChoice does not provide any examples of expressive profiling impacted by § 31(b)(2), let alone examples involving *unnecessary* profiling. Meanwhile, the harms from profiling are clear: discrimination based on race, gender, and other characteristics; exploitation of individual vulnerabilities; and the dangerous and privacy-invading accumulation of data to support profiling. *See* EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* 48–50 (2022).[11]

3. Section 31(b)(3) requires companies to minimize the personal information they collect, sell, share, and retain.

Section (b)(3) prohibits covered entities from "collect[ing], sell[ing], shar[ing], or retain[ing] any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged" unless the company can meet the exception. This provision is called a "data minimization requirement" and is a common feature of data protection laws. Kara Williams &

---

[11] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

Caitriona Fitzgerald, *Data Minimization is the Key to A Meaningful Privacy Law*, EPIC (May 9, 2024).[12] The status quo is for companies to collect as much data on users as possible, often selling that data to advertisers and data brokers, who in turn either sell or make the information available to any willing buyer. EPIC, *Online Advertising & Tracking*. Minimizing the amount of data companies have on minors minimizes the potential that their data can be stolen by identity thieves, purchased by stalkers and abusers, used for government surveillance, or otherwise weaponized against them. *See* EPIC, *Disrupting Data Abuse* at 36–46, 167–72.

NetChoice does not explain how § 31(b)(3) impacts content curation, let alone expression. To the extent that any data collection is necessary for content curation or any other functionality necessary to provide the service, this provision explicitly allows it.

---

[12] https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.

4. Section 31(b)(4) prohibits companies from using personal information collected for one purpose for another, different purpose.

Section 31(b)(4) prohibits secondary uses of minors' personal information, what is often called a "purpose limitation" on the use of data. Like data minimization, purpose limits are common components of data protection frameworks. *See* Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC (May 4, 2023).[13] Purpose limits aim to align companies' data uses with users' expectations. Users provide information to companies for specific purposes and do not expect that their information will be used for other purposes. *Id.*

Purpose limits are of special importance now as platforms increasingly use their users' personal information to train generative AI systems with dubious consent. *See* Eli Tan, *When the Terms of Service Change to Make Way for A.I. Training*, N.Y. Times (June 26, 2024).[14]

---

[13] https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/.
[14] https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html.

The information minors share on covered platforms should not be used to train AI systems. *See* EPIC, *Generating Harms II* 34 (2024).[15] Section 31(b)(4) would prevent covered entities from, for instance, using minors' photos to create deepfake child sexual abuse materials.

NetChoice does not explain how § 31(b)(4) interferes with companies' curation activities, let alone their expression. NetChoice asserts that the provision "invites government censors to evaluate whether content is in "the best interests of children." 2d Mot. for Prelim. Inj. at 8. But this language is in the exception, and what must be in "the best interest of children" is *the use of personal information for another purpose*, not the content shown. It is not at all clear how a purpose limitation impacts any aspect of content curation unless the company is using data collected for a different purpose to drive its surveillance targeting. Explicit user preferences would be collected and used for the purpose of providing users personalized feeds, while it is not clear what, if any, user data is used for content moderation.

---

[15] https://epic.org/documents/generating-harms-ii/.

* * *

In sum, the record and argument supporting NetChoice's challenges to the data protection provisions are woefully deficient. The injunction against the provisions should be vacated and the case should be remanded.

CONCLUSION

For the foregoing reasons, EPIC respectfully urges the Court to reverse the district court's determination that the CAADC's coverage definition renders the entire law content-based and subject to strict scrutiny and to vacate the district court's injunction against the data protection provisions.

Date: June 17, 2025

/s/ Megan Iorio
Megan Iorio
Tom McBrien
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 6,471 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 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.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 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; or

[ ] 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/ Megan Iorio* **Date:** June 17, 2025

CERTIFICATE OF SERVICE

I certify that on June 17, 2025, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: June 17, 2025

/s/ Megan Iorio
Megan Iorio
Tom McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center