

1 Alan Butler (SBN 281291)
2 butler@epic.org
3 ELECTRONIC PRIVACY INFORMATION CENTER
4 1519 New Hampshire Avenue NW
5 Washington, DC 20036
6 Tel: 202.483.1140

7 *Attorney for Proposed Amicus Curiae*
8 *Electronic Privacy Information Center*

9 **UNITED STATES DISTRICT COURT**
10 **NORTHERN DISTRICT OF CALIFORNIA**
11 **SAN JOSE DIVISION**

12 NETCHOICE, LLC, d/b/a NetChoice,

13 Plaintiff,

14 v.

15 ROB BONTA, ATTORNEY GENERAL OF
16 THE STATE OF CALIFORNIA, in his official
17 capacity,

18 Defendant.

Case No. 5:22-cv-08861-BLF

**BRIEF OF ELECTRONIC PRIVACY
INFORMATION CENTER AS *AMICUS
CURIAE* IN SUPPORT OF
DEFENDANT**

Hearing Date: January 23, 2025

Time: 9:00 a.m.

Judge: Hon. Beth Labson Freeman

Court: Courtroom 3, 5th Floor

Action Filed: December 14, 2022

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

Interest of the *Amicus Curiae* 1

Introduction 1

Argument..... 2

 I. Engagement maximization is not expressive 2

 II. The CAADC’s data protection provisions limit engagement maximization, not content
 moderation 6

 A. Section 31(b)(1) restricts harmful uses of personal information, not the use of
 personal information to deliver harmful content 6

 B. Section 31(b)(2) requires companies to turn profiling off by default..... 8

 C. Section 31(b)(3) requires companies to minimize the personal information they
 collect, sell, share, and retain..... 9

 D. Section 31(b)(4) prohibits companies from using personal information collected
 for one purpose for another, different purpose 10

 III. NetChoice has not shown that the data protection provisions restrict protected speech
 either facially or as applied to all of its covered members 11

Conclusion 15

TABLE OF AUTHORITIES

Cases

Moody v. NetChoice, 603 U.S. 707 (2024)passim

Nat’l Fed’n of Indep. Bus. v. Sebelius, 567 U.S. 519 (2012).....7

NetChoice v. Bonta, 113 F.4th 1101 (2024) 11, 12

Statutes

Cal. Civ. Code

§ 1798.99.30(b)(6).....8

§ 1798.99.31(b)(1).....6

§ 1798.99.31(b)(2).....8, 9

§ 1798.99.31(b)(3).....9

§ 1798.99.31(b)(4).....10

Other Authorities

Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, The Knight First Amendment Institute at Columbia University (2023)3, 4, 8

Eli Tan, *When the Terms of Service Change to Make Way for A.I. Training*, N.Y. Times (June 26, 2024)..... 10

EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* 48–50 (2022).....9, 10

EPIC, *Online Advertising & Tracking* (2024)8, 9

Goodreads, *Goodreads Interest-Based Ads Notice* (Oct. 30, 2024)..... 14

IMDb, *IMDb Privacy Notice* (Mar. 27, 2024)..... 14

Kara Williams & Caitriona Fitzgerald, *Data Minimization is the Key to A Meaningful Privacy Law*, EPIC (May 9, 2024).....9

Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 Yale L.J. 2418 (2020)3, 6

1 Keach Hagey & Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got*
2 *Angrier Instead*, Wall St. J. (Sep. 15, 2021).....5
3 Natasha Singer, *LinkedIn Ran Social Experiments on 20 Million Users Over Five Years*, N.Y.
4 Times (Sept. 24, 2022)7
5 Nathalie Maréchal & Nick Doty, *Defining Contextual Advertising*, Ctr. for Democracy & Tech.
6 (Aug. 2024).....9
7 Ravi Iyer, *Feed Algorithms Contain both Expressive and Functional Components*, USC Neely
8 Center for Ethics and Technology (Dec. 10, 2024).....4, 6
9 Sam Schechner et al., *How Facebook Hobbled Mark Zuckerberg’s Bid to Get America*
10 *Vaccinated*, Wall St. J. (Sep. 17, 2021).....5
11 Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect*
12 *Consumers*, EPIC (May 4, 2023) 10

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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* (2024).²

INTRODUCTION

The Supreme Court’s decision in *Moody v. NetChoice*, 603 U.S. 707 (2024), set out a rigorous standard for First Amendment challenges to platform regulations. Facial challenges must set out all potential applications of the law, assess the constitutionality of each, and weigh the constitutional applications against the unconstitutional ones. In assessing the constitutionality of each application, courts must insist on specificity. While some platform actions may be expressive, like removing or downranking messages based on a company’s content guidelines, other actions, like curating feeds based on users’ interactions with a site, are not evidently expressive. It is the challenger’s burden to explain what specific activities, by what specific actors, are impacted by a regulation, how those activities are expressive, and how the regulation interferes with that expression.

Recognizing that NetChoice failed to meet the *Moody* standard the first time it asked this court to enjoin the California Age-Appropriate Design Code (CAADC), the Ninth Circuit directed NetChoice to return to this court with a more robust record. But NetChoice showed up empty-handed. Instead of presenting specific facts to support specific constitutional arguments, NetChoice made superficial changes to the scope of some of its challenges. These rhetorical flourishes do not meet the rigorous standard set out in *Moody*.

This brief focuses on NetChoice’s challenges to the CAADC’s data protection

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.

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

1 provisions at §§ 31(b)(1)–(4). NetChoice argues that, facially and as applied to its members, the
2 data protection provisions violate the First Amendment “to the extent they limit an online
3 service’s rights to collect information for the purposes of curating, recommending, and
4 delivering protected speech to users.” Am. Compl. ¶ 87. NetChoice also challenges § 31(b)(3)
5 “to the extent it restricts the collection, retention, and sharing of personal information to publish
6 content or to make content available.” *Id.* at ¶ 88.

7 NetChoice does not make any specific legal arguments to support these claims, as
8 required by *Moody*. The Court in *Moody* flatly refused to adopt a categorical rule that
9 everything a platform does related to curating, recommending, delivering, or publishing content
10 is expressive. The Court only recognized one curation activity as expressive: the enforcement of
11 content moderation policies, which reflect companies’ agreement or disagreement with certain
12 messages. NetChoice fails to show how the data protection provisions interfere with expressive
13 content moderation activities, and it fails to argue that any other aspect of content curation is
14 expressive. NetChoice also fails to specify which entities are within the scope of its challenges
15 and fails to provide any record evidence or specific arguments about the full range of
16 applications within those challenges. These failures are fatal to NetChoice’s request to enjoin
17 the data protection provisions.

18 ARGUMENT

19 I. Engagement maximization is not expressive.

20 In *Moody v. NetChoice*, 603 U.S. 707 (2024), the Supreme Court signaled that one
21 specific curation practice is expressive: content moderation that reflects human value judgments
22 about the message expressed. This type of curation is distinct from engagement maximization,
23 which “respond[s] solely to how users act online—giving them the content they appear to want,
24 without any regard to independent content standards.” *Moody*, 603 U.S. at 736 n.5. Engagement
25 maximization is a harmful business practice—it relies on surveillance of users and undermines
26 their autonomy. Engagement-maximizing curation does not clearly express any message of the
27 curator, and so regulating it does not implicate the First Amendment. Limiting engagement
28 maximization does not impact companies’ ability to provide feeds that reflect the company’s

1 expressive values, and also does not prevent companies from providing users with feeds that
2 reflect their explicit preferences for the content they wish to see.

3 Content moderation is a company’s enforcement of rules about the types of content it is
4 willing to host or promote. These rules are typically set out in companies’ content moderation
5 policies and community guidelines and enforced through teams of human moderators, with
6 some assistance from algorithmic filtering. *See* Kate Klonick, *The Facebook Oversight Board:
7 Creating an Independent Institution to Adjudicate Online Free Expression*, 129 Yale L.J. 2418,
8 2423 (2020). In *Moody*, the majority agreed that content moderation activities are expressive
9 because they reflect humans’ value judgments about the message expressed by the content.
10 “When the platforms *use their Standards and Guidelines to decide* which third-party content
11 those feeds will display, or how the display will be ordered and organized, they are making
12 expressive choices.” *Moody*, 603 U.S. at 740 (emphasis added). A company that prohibits, say,
13 pro-Nazi posts is expressing its disagreement with the message of those posts, and a law that
14 “direct[s a company] to accommodate messages it would prefer to exclude” infringes on the
15 company’s protected editorial discretion. *Id.* at 710.

16 Content moderation is distinct from engagement maximization. Maximizing for
17 engagement means curating content in a way that maximizes the probability that a specific user
18 will interact with a specific piece of content. *See* Arvind Narayanan, *Understanding Social
19 Media Recommendation Algorithms*, The Knight First Amendment Institute at Columbia
20 University 20 (2023).³ In contrast to content moderation, which largely depends on human
21 decision making and intervention, engagement optimization is accomplished through machine
22 learning algorithms, called “recommendation algorithms,” which essentially crunch the numbers
23 on what will keep each user on the platform longer. *See* Ravi Iyer, *Feed Algorithms Contain
24 both Expressive and Functional Components*, USC Neely Center for Ethics and Technology

25
26
27
28 ³ [https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---
Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf](https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf).

1 (Dec. 10, 2024).⁴ The primary fuel for engagement-maximizing recommender algorithms is user
2 behavioral data collected through surveillance, not explicit user feedback. *See* Narayanan,
3 *supra*, at 18. This data can include likes, clicks, comments, time spent watching, time spent
4 lingering, and other indications that a piece of content held a user’s attention. *Id.* at 18–19. The
5 algorithms use this data to construct profiles of users. The algorithms then compare the user’s
6 profile to those of other users, showing them media that similar users engaged with heavily.
7 Narayanan, *supra*, at 22. The algorithm’s output does not reflect any human value judgment
8 about the content or messages expressed. Any message—including contradictory ones—goes,
9 so long as it maximizes the amount of time the user spends on the site.

10 Recognizing the distinction between content moderation and engagement maximization,
11 the majority in *Moody* set aside the question of whether “feeds whose algorithms respond solely
12 to how users act online—giving them the content they appear to want, without any regard to
13 independent content standards” are expressive. *Moody*, 603 U.S. at 736 n.5. Justice Barrett,
14 whose vote was necessary for the majority opinion and whose views thus matter for forming
15 future majorities on this issue, wrote in her concurrence, “The First Amendment implications . .
16 . might be different” for “a platform’s algorithm [that] just presents automatically to each user
17 whatever the algorithm thinks the user will like—e.g., content similar to posts with which the
18 user previously engaged.” *Id.* at 746 (Barrett, J., concurring). And in his concurrence, Justice
19 Alito, writing for himself and Justices Thomas and Gorsuch, contrasted newspaper editors’
20 expressive curation from algorithms that “prioritize content based on factors that the platforms
21 have not revealed and may not even know.” *Id.* at 795 (Alito, J., concurring in the judgment).

22 The fact that engagement-maximizing algorithms are inscrutable black boxes whose
23 outputs are determined by machine learning and not human value judgments undermines their
24 expressiveness. Four justices explicitly recognized that the extent to which curation is mediated
25 by black-box algorithms impacts the First Amendment analysis, even when those algorithms are
26 performing content moderation. Justice Barrett wrote in her concurrence that “technology may

27 _____
28 ⁴ <https://neely.usc.edu/2024/12/10/algorithms-contain-both-expressive-and-functional-components/>.

1 attenuate the connection between content-moderation actions (e.g., removing posts) and human
2 beings’ constitutionally protected right” of expression. *Id.* at 746 (Barrett, J., concurring). She
3 noted that “If the AI relies on large language models to determine what is ‘hateful’ and should
4 be removed, has a human being with First Amendment rights made an inherently expressive
5 ‘choice . . . not to propound a particular point of view?’” *Id.* Justice Alito added, “[W]hen AI
6 algorithms make a decision, even the researchers and programmers creating them don’t really
7 understand why the models they have built make the decisions they make. Are such decisions
8 equally expressive as the decisions made by humans?” *Id.* at 795 (Alito, J., concurring in the
9 judgment) (quotation marks and citations omitted). If using algorithms can attenuate the
10 expressiveness of otherwise-expressive *content moderation*, the case for the expressiveness of
11 value-agnostic algorithmic *engagement maximization* is even more dire. If NetChoice wishes to
12 argue that certain companies’ engagement maximizing algorithms produce protected speech,
13 they must reveal how those algorithms work and explain how they are expressive.

14 As it stands, there is nothing to suggest that engagement-maximizing algorithms, on
15 their own, express any message of a company. They do not choose or rank content based on
16 agreement or disagreement with the message expressed, only based on a user’s likelihood of
17 interacting with the media. Perhaps the most damning evidence against the expressiveness of
18 engagement maximization is that platforms’ recommendation algorithms often promote content
19 that violates the company’s guidelines or otherwise undermines the company’s express
20 priorities. *See, e.g.,* Sam Schechner et al., *How Facebook Hobbled Mark Zuckerberg’s Bid to*
21 *Get America Vaccinated*, Wall St. J. (Sep. 17, 2021);⁵ Keach Hagey & Jeff Horwitz, *Facebook*
22 *Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*, Wall St. J. (Sep. 15,
23 2021).⁶ How can the recommendation algorithm’s amplification of messages the company says
24 it disagrees with be expressive of the company’s message? This conflict exists precisely because
25 the algorithms choose media for display without regard for the underlying message expressed.

26 _____
27 ⁵ <https://www.wsj.com/articles/facebook-mark-zuckerberg-vaccinated-11631880296>.

28 ⁶ <https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215>.

1 While it is true that a company may be engaged in both content moderation and
2 engagement maximization in the same feed, these two functions are not irrevocably intertwined.
3 A company could simply remove the engagement maximization function from the feed, leaving
4 the content moderation function intact. The same is true with user’s explicit preferences—which
5 creators or posters a user follows, what issues or topics interest they want to see more or less of,
6 and any other explicit signals of preference users provide to companies. Iyer, *supra*. A company
7 can take into account a user’s explicit preferences without maximizing engagement. *Id.* Indeed,
8 this was the prevailing model for personalized feeds until just a few years ago. *Id.* Without
9 engagement maximization, a personalized user feed would reflect a user’s actual preferences—
10 not assumptions a company makes about user preference.

11 **II. The CAADC’s data protection provisions limit engagement maximization, not**
12 **content moderation.**

13 The CAADC’s data protection provisions may impact a company’s ability to use
14 engagement maximizing algorithms to curate content, but nothing in these provisions would
15 likely inhibit companies’ right to include, exclude, promote, or downrank messages the
16 companies agree or disagree with. Companies do not generally use the personal information of
17 users to moderate content—they use community feedback, algorithmic screening, and human
18 intervention. *See* Klonick, *supra*, at 2429–34. NetChoice certainly has not provided any
19 examples of how the data protection provisions would prevent companies from enforcing their
20 content policies. NetChoice instead misconstrues the statute and the few hypotheticals it does
21 offer do not clearly violate the law.

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

24 Section 31(b)(1) prohibits covered entities from “us[ing] the personal information of any
25 child in a way that the business knows, or has reason to know, is materially detrimental to the
26 physical health, mental health, or well-being of a child.” The provision prohibits *uses of*
27 *personal information* that the business “knows, or has reason to know” are harmful to children.
28 It does not, as NetChoice asserts, prohibit companies from “using a minor’s personal

1 information (including an IP address and browsing history) to deliver *content* the provider
2 ‘knows, or has reason to know, is materially detrimental’ to the minor’s ‘well-being.’” 2d Mot.
3 for Prelim. Inj. at 6 (emphasis added). Even if NetChoice’s interpretation were permissible, and
4 that interpretation was unconstitutional, the doctrine of constitutional avoidance compels the
5 Court to avoid construing the statute in this way when other constitutional constructions exist.
6 *See Nat’l Fed’n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 574 (2012) (explaining a “duty to
7 construe a statute to save it.”).

8 Properly understood, § 31(b)(1) does not interfere with a company’s right to include or
9 exclude certain messages as recognized in *Moody*. It requires companies to change their data
10 practices if they find those data practices harm minors, not to remove or downrank any content.
11 For example, companies sometimes conduct experiments to see what impact changing their
12 curation algorithms has on users. *See* Natasha Singer, *LinkedIn Ran Social Experiments on 20*
13 *Million Users Over Five Years*, N.Y. Times (Sept. 24, 2022).⁷ If Meta were to discover through
14 an experiment that including a certain category of data in its algorithm, such as “time spent
15 lingering on a piece of content,” led more girls to report high levels of anxiety, then § 31(b)(1)
16 would require Meta not to use this data. Meta would not have to remove or downrank any
17 content, nor would it have to change how it enforced its content policies. Indeed, content may
18 not even be involved, since the anxiety could be caused by the girls’ increased inability to turn
19 social media off, and the follow-on effects of that on their sleep, schoolwork, and social lives.

20 NetChoice’s hypothetical applications of this provision that purport to show its
21 constitutional issues involve harmful *content*, not harmful *uses of personal information*. Using
22 an IP address to deliver content is not a harmful use of personal information—it is technically
23 necessary. Using browsing history to curate content is also not known to categorically harm the
24 physical health, mental health, or well-being of minors. Even if using browsing history to curate
25 content *were* categorically harmful to minors, NetChoice hasn’t shown that this practice is
26 expressive. As explained in Section I above, using browsing history to maximize engagement is

27 _____
28 ⁷ <https://www.nytimes.com/2022/09/24/business/linkedin-social-experiments.html>.

1 not expressive. And even if using browsing history to curate content were, sometimes,
2 expressive, and some of those applications were proscribed by § 31(b)(1), they would just be a
3 few of the many, many applications of the provision, all of which would need to be weighed to
4 decide NetChoice’s facial challenge—which is impossible to do given the paucity of the record
5 and arguments NetChoice has provided the court.

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

7 Section 31(b)(2) prohibits companies from “profil[ing] a child by default” unless the
8 company can meet one of two enumerated exceptions. “Profiling” means the “automated
9 processing of personal information to evaluate certain aspects related to a natural person,
10 including analyzing or predicting aspects concerning a natural person’s performance at work,
11 economic situation, health, personal preferences, interests, reliability, behavior, location, or
12 movements.” Cal. Civ. Code § 30(b)(6). This is exactly what engagement maximization does:
13 profiling users to predict what content will keep them on the platform longer. *See Narayanan,*
14 *supra*, at 22. The provision does not interfere with companies’ ability to use algorithms to
15 remove or downrank content that violates their guidelines. The provision also does not “end
16 content personalization for minors.” 2d Mot. for Prelim. Inj. at 7. Instead of using behavioral
17 data to profile minors, companies can, instead, take users’ explicit preferences into account by
18 asking minors what creators they wish to follow, what categories of content they wish to see in
19 their feeds, and what they want to see more or less of.

20 In the advertising space, § 31(b)(2) would force companies to turn surveillance (or
21 behavioral) advertising off by default for minors. Surveillance advertising is similar to
22 engagement maximization insofar as the advertising engine uses a wide range of personal
23 information to profile a user and determine what ad a user is most likely to click on. *See EPIC,*
24 *Online Advertising & Tracking* (2024).⁸ Turning off surveillance advertising by default does not
25 prevent companies from serving ads on their platforms. Companies can still provide contextual
26 advertising, which serves ads that are relevant to the contents of a website and are not based on

27 _____
28 ⁸ <https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/>.

1 user profiles. See Nathalie Maréchal & Nick Doty, *Defining Contextual Advertising*, Ctr. for
2 Democracy & Tech. 3 (Aug. 2024).⁹

3 Section 31(b)(2) also only dictates a *default setting*. Minors can turn profiling on if they
4 so choose. NetChoice does not explain how letting minors decide whether to allow profiling
5 impacts any companies’ speech. Profiling that is necessary to provide the feature the minor is
6 actively engaged in is also allowed by default. § 31(b)(2)(B)(i). NetChoice does not provide any
7 examples of profiling impacted by § 31(b)(2), let alone examples involving *unnecessary*
8 profiling. Meanwhile, the harms from profiling are clear: discrimination based on race, gender,
9 and other characteristics; exploitation of individual vulnerabilities; and the dangerous and
10 privacy-invading accumulation of data to support profiling. See EPIC, *Disrupting Data Abuse:
11 Protecting Consumers from Commercial Surveillance in the Online Ecosystem* 48–50 (2022).¹⁰

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

14 Section (b)(3) prohibits covered entities from “collect[ing], sell[ing], shar[ing], or
15 retain[ing] any personal information that is not necessary to provide an online service, product,
16 or feature with which a child is actively and knowingly engaged” unless the company can meet
17 the exception. This provision is called a “data minimization requirement” and is a common
18 feature of data protection laws. Kara Williams & Caitriona Fitzgerald, *Data Minimization is the
19 Key to A Meaningful Privacy Law*, EPIC (May 9, 2024).¹¹ The status quo is for companies to
20 collect as much data on users as possible, often selling that data to advertisers and data brokers,
21 who in turn either sell or make the information available to any willing buyer. EPIC, *Online
22 Advertising & Tracking*. Minimizing the amount of data companies have on minors minimizes
23

24 ⁹ [https://cdt.org/wp-content/uploads/2024/08/2024-08-13-PD-Defining-Contextual-Advertising-
25 Brief-final.pdf](https://cdt.org/wp-content/uploads/2024/08/2024-08-13-PD-Defining-Contextual-Advertising-Brief-final.pdf).

26 ¹⁰ [https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-
27 comments-Nov2022.pdf](https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf).

28 ¹¹ <https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/>.

1 the potential that their data can be stolen by identity thieves, purchased by stalkers and abusers,
2 used for government surveillance, or otherwise weaponized against them. *See* EPIC, *Disrupting*
3 *Data Abuse* at 36–46, 167–72.

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

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

9 Section 31(b)(4) prohibits secondary uses of minors’ personal information, what is often
10 called a “purpose limitation” on the use of data. Like data minimization, purpose limits are
11 common components of data protection frameworks. *See* Sara Geoghegan, *Data Minimization:*
12 *Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC (May 4, 2023).¹²
13 Purpose limits aim to align companies’ data uses with users’ expectations. Users provide
14 information to companies for specific purposes and do not expect that their information will be
15 used for other purposes. *Id.*

16 Purpose limits are of special importance now as platforms increasingly use their users’
17 personal information to train generative AI systems with dubious consent. *See* Eli Tan, *When*
18 *the Terms of Service Change to Make Way for A.I. Training*, N.Y. Times (June 26, 2024).¹³ The
19 information minors share on covered platforms should not be used to train AI systems. *See*
20 EPIC, *Generating Harms II* 34 (2024).¹⁴ Section 31(b)(4) would prevent covered entities from,
21 for instance, using minors’ photos to create deepfake child sexual abuse materials.

22 NetChoice does not explain how § 31(b)(4) interferes with companies’ curation
23 activities, let alone their expression. NetChoice asserts that the provision “invites government
24

25 ¹² [https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-](https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/)
26 [consumers/](https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/).

27 ¹³ <https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html>.

28 ¹⁴ <https://epic.org/documents/generating-harms-ii/>.

1 censors to evaluate whether content is in “the best interests of children.” 2d Mot. for Prelim. Inj.
2 at 8. But this language is in the exception, and what must be in “the best interest of children” is
3 *the use of personal information for another purpose*, not the content shown. It is not at all clear
4 how a purpose limitation impacts any aspect of content curation unless the company is using
5 data collected for a different purpose to drive its recommendation algorithm or surveillance
6 advertising. Explicit user preferences would be collected and used for the purpose of providing
7 users personalized feeds, while it is not clear what, if any, user data is used for content
8 moderation.

9 **III. NetChoice has not shown that the data protection provisions restrict protected**
10 **speech either facially or as applied to all of its covered members.**

11 Facial challenges are “disfavored,” *Moody*, 603 U.S. at 744, because they “often rest on
12 speculation” and “threaten to short circuit the democratic process by preventing duly enacted
13 laws from being implemented in constitutional ways.” *Id.* at 723 (internal citations omitted).
14 Because of the dangers facial challenges pose, the decision to challenge a statute on its face
15 “comes at a cost.” *Id.* That cost is a heightened evidentiary burden. In the First Amendment
16 context, a court must be able to determine “a law’s full set of applications, evaluate which are
17 constitutional and which are not, and compare the one to the other.” *Id.* at 718. A law can be
18 facially invalidated “only if the law’s unconstitutional applications substantially outweigh its
19 constitutional ones.” *Id.* at 724.

20 The Ninth Circuit vacated this court’s previous injunction because NetChoice had not
21 shown that the data protection provisions “necessarily impact protected speech in all or even
22 most applications.” *NetChoice v. Bonta*, 113 F.4th 1101, 1123 (2024). The panel noted that this
23 court’s previous decision was based on “speculation” about how “the editorial decisions of
24 social media companies” might be impacted by the law and did not “consider[] any other
25 potential applications.” *Id.*

26 NetChoice has not remedied its failures on remand. NetChoice does not simply
27 challenge the data protection provisions’ application to social media companies—it challenges
28 its application to *all* covered entities and to *all* of its covered members. Am. Compl. ¶¶ 87–88.

1 Yet, in neither its facial nor its as applied challenge has NetChoice established “what activities,
2 by what actors, the law[] prohibit[s] or otherwise regulate[s].” *Moody*, 603 U.S. at 724. Nor has
3 NetChoice shown “whether there is an intrusion on protected editorial discretion” for each of
4 these activities by each of these actors. *Id.* at 708. Consequently, NetChoice “did not address the
5 full range of activities the laws cover and measure the constitutional against the unconstitutional
6 applications.” *Id.* at 724.

7 While NetChoice acknowledges that the CAADC applies to a broad range of covered
8 entities, Am. Compl. ¶ 26, NetChoice has included in the record declarations from only four
9 companies: Techdirt, Dreamwidth, Goodreads, and IMDb. These four entities and their data
10 practices do not represent the full sweep of applications that NetChoice challenges. Specifically,
11 there is no evidence in the record about how any news outlet,¹⁵ sports league, sports outlet,
12 online magazine, podcast channel, e-book, e-reader app, online education or credential program,
13 video or music streaming service, online video game, discussion forum, or online self-help and
14 suicide-prevention service uses personal information to curate content, how that use of data is
15 expressive, and how the CAADC interferes with that expression. *See* Am. Compl. ¶ 26 (listing
16 each of these categories of entities as covered by the CAADC). Indeed, NetChoice does not
17 even establish which of its own members, and which of their activities, are within the scope of
18 their challenges. Most conspicuous is the absence of declarations from major social media
19 platforms, considering that both this court and the Ninth Circuit seemed to be under the
20 impression that this was the primary application NetChoice challenges. *See Bonta*, 113 F.4th at
21 1123. Dreamwidth is the only social media platform to submit declarations, and given its
22 limited use of personal information to curate content, Paolucci Decl. ¶¶ 3, 7, it is
23 unrepresentative of these platforms.

24 The current record is even insufficient to sustain as-applied challenges to the data
25 protection provisions for the four companies that made declarations. Two of the declarants’
26 submissions, Techdirt’s and Dreamwidth’s, are irrelevant because none of the activities they

27 _____
28 ¹⁵ The New York Times amicus brief does not detail the newspaper’s data practices.

1 describe would be impacted by the data protection provisions. Techdirt does not point to any
2 website feature that uses personal information to curate content for users. The online blog
3 asserts that it “does not currently collect user data for advertising or feature any display
4 advertising.” Masnick Supp. Decl. ¶ 9. Otherwise, the company says that it collects and shares
5 only “limited” personal information, “like IP addresses and website visitation details,” to
6 “operate, maintain, and provide Techdirt’s features and services.” Masnick Decl. ¶ 10. Techdirt
7 does not say that it uses this personal information to curate content. There are no arguments that
8 any other use of this data is expressive. And besides one argument that the use of IP addresses
9 to deliver content may sometimes violate a misconstrued § 31(b)(1), *see* Section IIA, *supra*,
10 NetChoice does not otherwise argue that any of Techdirt’s uses of personal information are
11 impacted by the data protection provisions.

12 Like Techdirt, Dreamwidth “does not serve ads” on its site, Paolucci Decl. ¶ 3, nor does
13 it “‘recommend’ accounts or content to users” or “offer any ‘algorithmic timeline’ that adjusts
14 the display of content based on a prediction that a particular user will be interested in a
15 particular piece of content.” *Id.* at ¶ 7. But the company does offer a feed populated by content
16 from users a person follows, ranked in reverse chronological order. *Id.* at ¶ 7. The collection and
17 use of a person’s explicit preferences for content does not violate the CAADC. There is no
18 evidence that this data practice harms kids’ physical health, mental health, or well-being; it does
19 not constitute profiling; it is necessary to provide the feed and is collected in the course of a user
20 actively engaging with that website feature; and the information is collected for the purpose of
21 populating the feed and not for another purpose. Dreamwidth’s concern that its other data
22 practices may run afoul of the data protection provisions is vague and contradictory. *Id.* at ¶ 4;
23 Paolucci Supp. Decl. ¶ 9. For instance, Dreamwidth says it collects and shares data “to facilitate
24 the basic operation of the site” but then says “it is impossible to know” if those practices are
25 “‘necessary’ to provide the service.” *Id.* Both of these assertions cannot be true.

26 Of NetChoice’s four declarants, only two—Goodreads and IMDb—appear to have
27 features that use personal information to curate content in a way that might be regulated by the
28 CAADC. Oddly, neither of these companies filed supplemental declarations to support

1 NetChoice’s current motion, so it is not entirely clear which of their activities are within
2 NetChoice’s challenge. Regardless, both sites use surveillance advertising to target users with
3 ads. Cairella Decl. ¶ 20; Roin Decl. ¶ 10. But neither NetChoice nor Goodreads nor IMDb
4 explain how the companies’ use of personal information for surveillance advertising is
5 expressive or how the CAADC’s data protection provisions limit this expression. It is not at all
6 clear, for instance, how changing the default settings for Goodreads’ or IMDb’s surveillance
7 advertising systems from opt-in to opt-out would burden these companies’ *expression*, not just
8 their pocketbooks. *See* Cairella Decl. ¶ 21; Roin Decl. ¶ 22. It is also unclear how Goodreads’
9 and IMDb’s use of surveillance advertising is even *their own expression* because Goodreads and
10 IMDb rely, at least in part, on third parties to deliver advertisements. IMDb, *IMDb Privacy*
11 *Notice* (Mar. 27, 2024);¹⁶ Goodreads, *Goodreads Interest-Based Ads Notice* (Oct. 30, 2024).¹⁷
12 The third-party advertisers have not submitted declarations in this case, nor is it clear that they
13 are covered entities or within the scope of NetChoice’s challenge.

14 Besides surveillance advertising, Goodreads and IMDb appear to have minor website
15 features that use personal information to curate content for users. Cairella Decl. ¶ 8; Roin Decl.
16 ¶ 22. But neither declaration (nor NetChoice’s briefing) establishes the full scope of personal
17 information these feeds use, how the algorithms work, what messages the companies’ use of
18 personal information express, and how the CAADC’s data protection provisions burden that
19 expression. IMDb for instance does not say what personal information its movie
20 recommendations are based on—is it only the movies a user adds to their Watchlist, or does the
21 company also use browsing history, reviews, or other information? How the algorithms work
22 impacts whether they are expressive at all. *See* Section I, *supra*. Are the companies’ algorithms
23 based on value judgments that the companies’ human editors have made about what movies and
24 books a person may like based on their viewing or reading habits, or are they instead based on

25
26
27 ¹⁶ <https://www.imdb.com/privacy/>.

28 ¹⁷ <https://help.goodreads.com/s/article/Goodreads-Interest-Based-Ads-Notice>.

1 machine learning techniques that crunch the numbers on what users with similar viewing and
2 reading histories have also viewed or read?

3 Even if some aspects of these feeds were expressive, it is unclear how the CAADC
4 would interfere with this expression. For instance, how would it interfere with the companies'
5 expression if they redesigned their recommendation features to use affirmatively provided
6 information instead of surreptitiously collected information? How would it impact Goodreads'
7 or IMDb's expression if they asked their users to provide a list of their favorite movies or books
8 and made recommendations based on that information, instead of using their browsing histories
9 (assuming that is what they do)?

10 In sum, the record on the data protection provisions is woefully deficient, and this fact
11 alone is enough for this court to deny NetChoice's request for a preliminary injunction.

12 **CONCLUSION**

13 For the foregoing reasons, *Amicus* ask this Court to deny Plaintiff's request for a
14 preliminary injunction.

15 Dated: December 13, 2024

Respectfully submitted,

17 By: /s/ Alan Butler

18 Alan Butler (SBN 281291)
19 butler@epic.org
20 ELECTRONIC PRIVACY INFORMATION CENTER
21 1519 New Hampshire Avenue NW
22 Washington, DC 20036
23 Tel: 202.483.1140

*Attorney for Proposed Amicus Curiae Electronic
24 Privacy Information Center*