Exhibit A

JENNER & BLOCK LLP
Lindsay C. Harrison
Jessica Ring Amunson (*pro hac vice* pending)
1099 New York Avenue NW, Suite 900
Washington, DC 20001
Tel: (202) 639-6865
lharrison@jenner.com
jamunson@jenner.com

Counsel for *Amicus Curiae*

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

NETCHOICE, LLC d/b/a NetChoice,

Plaintiff,

v.

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

Defendant.

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

BRIEF OF PROFESSOR ERIC GOLDMAN AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFF

Date: February 24, 2023

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

IDENTITY AND INTEREST OF *AMICUS CURIAE*[1]

Professor Eric Goldman is a Professor of Law at Santa Clara University School of Law, where he is also Associate Dean for Research, Co-Director of the High Tech Law Institute, and Supervisor of the Privacy Law Certificate.[2] Professor Goldman has been researching Internet Law for thirty years, and he has taught Internet Law since 1996. Professor Goldman has also written extensively on a wide range of Internet Law topics. *See, e.g.*, Eric Goldman, *Content Moderation Remedies*, 28 Mich. Tech. L. Rev. 1 (2021); Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 Notre Dame L. Rev. Reflection 33 (2019); Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 Yale J.L. & Tech. 188 (2006). Professor Goldman is ranked as one of the "10 Most-Cited Law & Technology Scholars in the U.S., 2016-2020."[3]

Professor Goldman submits this *amicus* brief to explain how the California Age-Appropriate Design Code Act creates barriers for both minors and adults seeking to access websites or apps, and how those barriers impermissibly block users from engaging in activities that are protected by the First Amendment.

INTRODUCTION

The Internet is a "unique and wholly new medium of worldwide human communication." *Reno v. ACLU*, 521 U.S. 844, 850 (1997). Among its many special properties, the Internet makes it easy for users to navigate seamlessly between many websites operated by unrelated entities. *ACLU v. Reno*, 929 F. Supp. 824, 836-37 (E.D. Pa. 1996) ("[L]inks from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique[.]"), *aff'd*, 521 U.S. 844 (1997).

---

[1] *Amicus curiae* certifies that this brief was authored entirely by counsel for *amicus curiae* and not by counsel for any party, in whole or part; no party or counsel for any party contributed money to fund preparing or submitting this brief; and apart from *amicus curiae* and their counsel, no other person contributed money to fund preparing or submitting this brief.

[2] Professor Goldman submits this brief in his individual capacity and not on behalf of his employer or any other individual or entity.

[3] Brian Leiter, *10 Most-Cited Law & Technology Scholars in the U.S., 2016-2020 (CORRECTED)*, Brian Leiter's L. School Reports (Sept. 9, 2021), http://bit.ly/41fgbgR.

The California Age-Appropriate Design Code Act (AADC) threatens this foundational principle of the Internet. Enacted under the pretext of protecting children's privacy, the AADC regulates "[b]usinesses that develop and provide online services, products, or features that children are likely to access." Cal. Civ. Code § 1798.99.29(a). Under the AADC, businesses preparing to launch new online services, products, or features are required to prepare a "Data Protection Impact Assessment" detailing how the feature's design could expose minors to "potentially harmful" materials. *Id.* § 1798.99.31(a)(1)(B)(i)-(vii). The AADC also prohibits these online businesses from collecting, using, or distributing a child's personal information in any way inconsistent with "the best interests of children." *Id.* § 1798.99.31(b).

Crucially, the AADC imposes on these businesses an age-assurance requirement. Regulated businesses are required to estimate the age of their users with "a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business" or in the alternative they must "apply the privacy and data protections afforded to children to *all* consumers." *Id.* § 1798.99.31(a)(5) (emphasis added). In other words, businesses must choose between assuring the age of all users (both minors and adults alike) or redesigning all their online features to treat adults as if they were children. Violations of the AADC's requirements can result in penalties of up to $7,500 per "affected child," as well as injunctive relief. *Id.* § 1798.99.35(a).

The AADC's age-assurance requirement erects onerous barriers that would discourage Internet usage and chill protected speech. These barriers to online movements will change how people use the Internet in ways that will hinder the Internet's utility to society—and transgress basic constitutional principles. In short, the AADC casts a "dark[] shadow over free speech, [and] threatens to torch a large segment of the Internet community." *Reno v. ACLU*, 521 U.S. at 882.

ARGUMENT

I. The AADC's Age-Assurance Requirements Impede Access to Constitutionally Protected Online Speech.

The AADC is framed as a way to protect children online, but that is a gross misrepresentation. The AADC has substantial, and negative, implications for both adults' and children's Internet experiences.

A. Age Assurance Creates Onerous Barriers for Accessing Content Online.

The AADC does not require age verification, which involves determining a user's age with precision. Instead, the AADC requires "age assurance," which means determining whether a user is a minor or adult with an appropriate degree of confidence. Specifically, the Act requires covered online businesses to "[*e*]*stimate* the age of child users with a reasonable level of certainty appropriate to the risks." Cal. Civ. Code § 1798.99.31(a)(5) (emphasis added). Though age assurance may sound like a less demanding requirement than age verification, in practice it is a distinction without a difference. Both age verification and age assurance require websites and apps to erect barriers before usage.

The AADC does not specify the exact method that regulated entities must use to perform age assurance. That omission not an accident. It reflects the fact that no one—including the California Legislature—is clear how businesses should implement this law. Every available option is problematic in ways that undercut the Legislature's objective of increasing children's privacy. *See Online Age Verification: Balancing Privacy and the Protection of Minors*, CNIL (Sept. 22, 2022), http://bit.ly/3EB1ISN [hereinafter CNIL Report] ("[T]here is currently no solution that satisfactorily" provides "sufficiently reliable verification, complete coverage of the population and respect for the protection of individuals' data and privacy and their security."); Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall St. J. (Feb. 27, 2022), http://bit.ly/41ngt5m. *Amicus* below reviews three of the primary ways to determine a user's age online: self-reporting, document review, and automated estimation.

Self-reporting, sometimes called "age-gating," asks users to report their age or check a box certifying their status as an adult. Self-reporting is not considered a reliable method of determining age because of the users' ability and incentive to misreport. As a result, it probably does not satisfy the AADC's requirement that businesses estimate user ages to a "reasonable level of certainty." Cal. Civ. Code § 1798.99.31(a)(5).

Document review involves users submitting documentary evidence showing their ages. Typical evidence would be a government-issued form of identification, such as a driver's license. Document review has numerous limitations, including the need to link the submitter with the submitted documents (otherwise, the submitter can use someone else's documents), the cost and time required to review the

submitted documents, and the fact that many people (both children and adults) do not have government-issued documents confirming their age.

Automated estimation requires users to expose their faces so that software can estimate their ages or classify them as minors or adults. Age-estimation software has high, but not perfect, accuracy. It also creates significant privacy and security risks. A person's face is considered to be highly sensitive personal information because it is unique to each person but immutable, so if a person's face can be digitally "stolen," it can wreak havoc on that person's life without any good fixes. For that reason, a number of "biometric" privacy laws around the country severely restrict the use of face scans.[4] *See, e.g.*, Cal. Civ. Code § 1798.140(c) & (ae) (defining "[b]iometric information" to include "face", "vein patterns" and "faceprints" and specifying that biometric information may qualify as "[s]ensitive personal information"). Further, privacy advocates repeatedly warn consumers about face-scanning technologies due to the privacy and security risks they create. *See, e.g.*, Nigel Jones, *10 Reasons to Be Concerned About Facial Recognition Technology*, Priv. Compliance Hub (Aug. 2021), https://bit.ly/3XXLWbp. Widespread deployment of face-scanning technologies on the Internet teaches consumers to disregard that advice and thereby dramatically increases users' privacy and security risks.

B. Age Assurance Will Deter Internet Usage and Chill Speech Online.

The age-assurance methods discussed above necessarily add a new step to a user's visit to a new website or app. The user must stop what they were doing and complete the age-assurance process before they can reach their objective. For websites and apps where users create accounts (and thus, in effect, have persistent identities with the service), the users may only have to complete the age-assurance process one time. After that, the website or app can store the user's estimated age and authenticate the user when the user presents the login credentials associated with the account. Websites and apps that do not have user

[4] To the extent a scanned person's consent is required to conduct the scan, it does not solve any of the AADC's problems because minors are legally deemed to have diminished capacity to consent for themselves.

accounts will force their users to tediously repeat the age-assurance process each time the user tries to access the website or app.[5]

Regardless of the exact form it takes, the AADC's age-assurance process will act as a burdensome barrier that users must overcome before accessing any website or app. This access barrier will dramatically reduce users' willingness to consume or contribute content via the website or app. The literature on this point is overwhelming. Users are extremely sensitive to any access barriers to the online destinations they seek. Those barriers reduce consumer usage of websites and services and, as a result, undermine their financial viability.

If the age-assurance barriers add a short time delay (called "latency")—of even a few seconds—to a user's access to a new website or service, it would drive many users away. A frequency of users leaving a website after accessing the first page is called the "bounce rate." Small increases in latency can increase bounce rates, often dramatically. *See Will Co. v. Lee*, 47 F.4th 917, 924-25 (9th Cir. 2022) ("Research shows that sites lose up to 10% of potential visitors for every additional second a site takes to load, and that 53% of visitors will simply navigate away from a page that takes longer than three seconds to load." (footnote omitted)); *see also* Daniel An, *Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed*, Think with Google (Feb. 2018), https://bit.ly/3ILJccK (showing that a latency increase from one to three seconds increases the bounce probability by 32%, and an increase from one to five seconds increases the bounce probability by 90%).

The reduced audience due to increased latency can cost businesses revenues and profits. For example, "Amazon recently found that every 100 milliseconds of latency cost it 1% in sales." *Lee*, 47 F.4th at 925. Another study showed that for consumer-oriented online retailers, the "difference in e-commerce conversion rate between blazing fast sites and modestly quick sites is sizable. A site that loads in 1 second has an e-commerce conversion rate 2.5x higher than a site that loads in 5 seconds." Michael Wiegand, *Site Speed Is (Still) Impacting Your Conversion Rate*, Portent (Apr. 20, 2022), https://bit.ly/3EwJWQm.

[5] There are few good options to do persistent and reliable age assurance independent of account logins. Devices can be shared between minors and adults, or minors can easily get an adult to do a single but persistent bogus authentication.

Like page latency, the AADC's age-assurance requirement causes a lag between when the user attempts to access the desired page and when the user finally reaches that page. Depending on the exact methodology of the age assurance, those time delays are likely to be measured in seconds[6] or minutes, not milliseconds. The resulting bounce rate is therefore likely to be much higher than the numbers discussed above.

In addition to delaying users from reaching their desired content, the AADC-mandated age assurance will require users to navigate at least one screen—called an "interstitial" screen—before the users can access their desired content. Like latency, the presence of an interstitial screen also increases bounce rates. For example, Google+ used an interstitial screen to promote its mobile app before users could access the service on a mobile device, causing a 69% bounce rate. *See* David Morell, *Google+: A Case Study on App Download Interstitials*, Google Search Central Blog (July 23, 2015), https://bit.ly/3ILQY6i.

The AADC-mandated age-assurance interstitial will result in even higher bounce rates because it will require users to provide private and sensitive information. *See* CNIL Report (noting that age verification "contains particularly sensitive, private information"). These disclosure requirements will discourage users from proceeding because "[u]sers assess the costs and benefits of the personal data disclosure and if they do not consider the benefits to be larger than the costs they will defect." Miguel Malheiros & Sören Preibusch, *Sign-Up or Give-Up: Exploring User Drop-Out in Web Service Registration*, Symp. on Usable Priv. & Sec. (SOUPS) (2013), https://bit.ly/3ExraIu. The privacy and security concerns make the decision to proceed much riskier for the users than pages without privacy-invasive requests, and new users will have to make these decisions without inspecting the website or app to determine if they consider the page trustworthy enough to provide such sensitive information.[7] *See* Ting Li & Paul A. Pavlou, *What Drives Users' Website Registration?* (Dec. 18, 2013), http://bit.ly/3St0ezI

[6] For example, one age-assurance vendor, Yoti, touts that its automated verifications take about eight seconds. *See Identity Verification*, Yoti, http://bit.ly/3IsASgK (last visited Feb. 24, 2023).

[7] If a website or app outsources its age-assurance process to a third-party vendor, it will create several additional concerns: Can the user trust the third-party vendor? What is the relationship between the third-party vendor and the destination? Could a malefactor interpose itself in between the third-party vendor and the destination (sometimes called a man-in-the-middle attack)?

("[I]nformation privacy concerns, trust, and brand awareness are particularly important in users' decisions to disclose personal information to register on commercial websites[.]").

The AADC will cause a combination of the time delays, the intrusiveness of the interstitial process, and the privacy and security risks posed by the age-assurance process that will cause bounce rates to soar. This, in turn, will produce problematic second-order effects. For example, the AADC raises barriers to entry for new websites and apps that users do not yet trust. Users' lack of established trust will deter their willingness to navigate the age-assurance process. That effect, in turn, will benefit incumbents who have already established a strong enough trust relationship with users to get past their reluctance to do age assurance.

Thus, the AADC's purported ambition to protect children's privacy is in complete tension with its age-assurance requirement. As previously discussed, the decision to complete the age-assurance process can be an inherently risky one for users—i.e., users may be prompted to disclose personal and sensitive information. And children, who are still developing their judgment and digital literacy, are not well-equipped to make that decision for themselves. As a result, the AADC makes it easy for malefactors to prey on children's underdeveloped digital skills by getting them to reveal private and sensitive information through illegitimate age-assurance processes. It is hard to imagine how such a requirement advances the legislature's purported objective to "prioritize the privacy, safety, and well-being of children." Cal. Civ. Code § 1798.99.29(b).

II. Age-Verification Requirements Chill Online Readers and Authors and Therefore Violate Fundamental First Amendment Principles.

The effects of the AADC's age-assurance requirement on user behavior have major First Amendment implications. The AADC requires age assurance before readers can access and consume the content of an application or website. Some of that content may be commercial speech, such as offers to sell goods or services. But most of the content will be speech that qualifies for maximum constitutional protection, i.e., categories of content, restrictions of which face strict scrutiny. *See generally* Cal. Civ. Code § 1798.99.29 (drawing no distinction between commercial and noncommercial speech).

Courts have repeatedly rejected age-verification requirements analogous to the regulations at issue in this case on constitutional grounds. In the late 1990s, Congress and the states passed numerous laws designed to prevent children from accessing purportedly harmful material online. In response, courts thoroughly vetted the implications—and constitutional infirmities—of online age verification.

In 1996, Congress enacted the Communications Decency Act (CDA), which the Supreme Court largely struck down in *Reno v. ACLU* as a vague and content-based restriction of protected speech under the First Amendment. 521 U.S. 844 (1997). The CDA criminalized the "knowing" transmission of "obscene or indecent" messages to minors over the Internet. *Id.* at 859. The law provided an affirmative defense for those who restricted access to covered materials by implementing age-verification measures. *Id.* at 860-61. But the Court held that age-verification requirements "would not significantly narrow the statute's burden on noncommercial speech" because "it is not economically feasible for most noncommercial speakers to employ such verification." *Id.* at 881-82.

In response, in 1998, Congress the Child Online Protection Act (COPA). Pub. L. No. 105-277, tit. XIV, 112 Stat. 2681, 2681-736 (1998). Like the CDA, COPA contained an age-verification provision as an affirmative defense. COPA was the subject of lengthy constitutional litigation, including two Supreme Court rulings,[8] that ultimately ended in its invalidation as unconstitutional by the Third Circuit. The Third Circuit repeatedly emphasized that age-verification provisions—in addition to failing narrow tailoring requirements—are inconsistent with First Amendment protections. The Third Circuit reiterated the district court's factual findings that utilization of age-verification measures would burden protected speech, holding that "users could be deterred from accessing the plaintiffs' Web sites" because "many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial." *ACLU v. Ashcroft*, 322 F.3d 240, 258-59 (3d Cir. 2003), *aff'd*, 542 U.S. 656 (2004).

Five years later, when the Third Circuit struck down COPA for good, the court condemned age-verification requirements in even stronger terms. *See ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008). Not only was age verification insufficient to cure COPA's lack of narrow tailoring; it also "'raise[d] unique

[8] *See Ashcroft v. ACLU*, 535 U.S. 564 (2002); *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

First Amendment issues' that ma[d]e the statute unconstitutional." *Id.* at 195 (citation omitted). Specifically, the court agreed that the age-verification requirements "present their own First Amendment concerns by imposing undue burdens on Web publishers due to the high costs of implementing age verification technologies and the loss of traffic that would result from the use of these technologies." *Id.* at 196-97. The court found that age verification also deters "many users who are not willing to access information non-anonymously . . . from accessing the desired information." *Id.* at 196 (quotation marks omitted). "It is clear," the court concluded, "that these burdens would chill protected speech and thus that the affirmative defenses fail a strict scrutiny analysis." *Id.* at 197.

In addition, several states passed laws resembling the CDA and COPA, sometimes called "Baby CDA" laws. Those, too, were struck down as unconstitutional when challenged, with courts employing similar logic. *See, e.g.*, *PSINet, Inc. v. Chapman*, 362 F.3d 227, 236-37 (4th Cir. 2004) (finding that an age-verification requirement using credit card numbers "creates First Amendment problems of its own" because "many adults may be unwilling to provide their credit card number online" and "[s]uch a restriction would also serve as a complete block to adults who wish to access adult material but do not own a credit card"); *Se. Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773, 782 (D.S.C. 2005) (holding that age verification creates a "First Amendment problem" because "age verification deters lawful users from accessing speech they are entitled to receive"); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998) (holding that mandatory age verification "violates the First and Fourteenth Amendments of the United States Constitution because it prevents people from communicating and accessing information anonymously"), *aff'd*, 194 F.3d 1142 (10th Cir. 1999).

The AADC-mandated age-assurance barrier is unconstitutional for all the same reasons that the CDA, COPA, and the Baby CDA laws were unconstitutional. Just like the prior age verification requirements, the AADC's age-assurance provision imposes high implementation costs on regulated businesses, deters user traffic through increased latency and intrusive requests for personal information, and—as a result—chills protected speech. "The effect of the [regulation] . . . is to drive this protected speech from the marketplace of ideas on the Internet. This type of regulation is prohibited by the First Amendment." *Ashcroft*, 322 F.3d at 260-61.

In fact, the AADC goes further than the CDA, COPA, and Baby CDA laws by imposing mandatory age-assurance barriers not only on content readers, but also on content authors. *See* Cal. Civ. Code § 1798.99.31(a)(5) (requiring covered businesses to "[e]stimate the age of child *users*") (emphasis added)). Websites and apps that allow users to author and publish content must conduct age assurance on *every* prospective author before they are given access to the authoring and publication tools. This process will cause high bounce rates for prospective authors and deter their constitutionally protected speech.

Furthermore, the privacy invasions caused by age assurance can increase anonymous authors' concerns that their online posts will be attributed to them. *See* CNIL Report ("[The] need to identify Internet users is, in fact, an issue for privacy and personal data protection, since knowledge of an individual's identity can then be linked to their online activity[.]"). As the Third Circuit cautioned, "[p]eople may fear to transmit their personal information, and may also fear that their personal, identifying information will be collected and stored in the records of various Web sites." *Ashcroft*, 322 F.3d at 259.

***

In 2017, the Supreme Court suggested that "the Cyber Age is a revolution of historic proportions" and cautioned against radical changes that might disrupt such revolutions. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017). The AADC radically changes the Internet's architecture, hindering adult and child readers and authors from engaging in constitutionally protected activities and heightening the privacy and security risks faced by both adults and children. The AADC violates fundamental First Amendment principles and should not be permitted to go into effect.

CONCLUSION

For the foregoing reasons, *amicus curiae* respectfully requests that this Court grant Plaintiff's motion for preliminary injunction.

Dated: February 24, 2023

Respectfully Submitted,

By: /s/ *Lindsay C. Harrison*

Lindsay C. Harrison
Jessica Ring Amunson (*pro hac vice* pending)
JENNER & BLOCK LLP
1099 New York Avenue NW, Suite 900
Washington, DC 20001
Tel: (202) 639-6865
lharrison@jenner.com
jamunson@jenner.com

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on February 24, 2023, I filed the foregoing document via the Court's CM/ECF system. The document will be served electronically on counsel of record for the parties.

/s/ *Lindsay C. Harrison*
Lindsay C. Harrison