No. 23-2929

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC,
Plaintiff-Appellee,

v.

ROBERT BONTA, in his official capacity as
Attorney General for the State of California,
Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District California, Case No. 5:22-cv-08861-BLF
The Honorable Beth Labson Freeman, District Judge

BRIEF OF *AMICUS CURIAE* PROFESSOR ERIC GOLDMAN IN SUPPORT OF PLAINTIFF-APPELLEE

JESSICA RING AMUNSON
Counsel of Record
LINDSAY C. HARRISON
ANDREW C. DEGUGLIELMO
JENNER & BLOCK LLP
1099 New York Ave., N.W.
Suite 900
Washington, D.C. 20001
(202) 639-6000
jamunson@jenner.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

IDENTITY AND INTERESTS 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 Co-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. *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 previously submitted an *amicus* brief to the district court in this case, which the district court cited in support of its conclusions that: (1) "the

---

[1] No party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting this brief; and no person other than *amicus curiae* and his counsel contributed money that was intended to fund preparing or submitting this brief. All parties consented to the filing of 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.

steps a business would need to take to sufficiently estimate the age of child users would likely prevent both children and adults from accessing certain content," Appellant's Excerpts of Record ("ER") 16; and (2) "age estimation is in practice quite similar to age verification, and—unless a company relies on user self-reporting of age, which provides little reliability—generally requires either documentary evidence of age or automated estimation based on facial recognition," which "would appear to counter the State's interest in increasing privacy protections for children," ER 24.

Professor Goldman submits this *amicus* brief to further explain and to reinforce the district court's conclusions about how the California Age-Appropriate Design Code Act ("the CAADCA") 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.

SUMMARY OF ARGUMENT

The CAADCA imposes an age-estimation requirement that erects onerous access barriers to speech by impeding its availability and use by Internet users. The Attorney General has argued that the requirement furthers a substantial state interest in protecting children's privacy. But as the district court correctly concluded, the CAADCA actually achieves the opposite result by compelling businesses to systematically collect children's highly sensitive information, thereby exposing

children to alarming privacy intrusions that they would otherwise not experience. Though the Attorney General argues that the CAADCA only requires businesses to use minimally invasive age-estimation methods, that ignores the reality that any reliable age-estimation method is highly invasive by necessity.

Even assuming that the age-estimation requirement furthered the protection of children's privacy, the district court also correctly concluded that the barriers imposed by that requirement will meaningfully deter users from accessing a website's content. This deterrence negatively affects Internet users by reducing their willingness to consume or contribute content on a website, as well as businesses by undermining the financial viability of their websites and services. Consequently, the requirement is a substantially excessive means of achieving greater protections for children's privacy.

The Attorney General asserts that NetChoice lacks evidence on this score and relies on outdated cases. Not true. There is overwhelming evidence of the adverse effects of age-estimation requirements on users and businesses alike, and courts have consistently invalidated analogous and even less-egregious age-estimation requirements on this basis.

ARGUMENT

I. Background of the California Age-Appropriate Design Code Act

The Internet is a "the most important place[] (in a spatial sense) for the exchange of views[] today." *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017). Among its many special properties, the Internet makes it easy for users to navigate seamlessly between many websites operated by unrelated entities. *Ashcroft v. ACLU*, 535 U.S. 564, 566 (2002) ("While 'surfing' the [Internet], . . . individuals can access material about topics ranging from aardvarks to Zoroastrianism."); *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).

The CAADCA threatens this foundational principle of the Internet. Enacted under the pretext of protecting children's privacy, the CAADCA 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). Pursuant to the CAADCA, 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 CAADCA 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 CAADCA imposes on these businesses an age-estimation 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 of their online features to treat adults as if they were children. Violations of the CAADCA'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 Court should affirm the district court's findings that the CAADCA's age-estimation requirement erects onerous barriers that would endanger rather than protect children's privacy, discourage Internet usage, and chill protected speech. As *amicus* explains below, 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 CAADCA casts a "dark[] shadow over free speech, [and] threatens to torch a large segment of the Internet community." *Reno v. ACLU*, 521 U.S. 844, 882 (1997).

II. Age Estimation Creates Onerous Barriers That Exacerbate the Problem They Purport to Resolve.

The CAADCA is framed as a way to protect children online, but in fact it does the opposite. As the district court concluded, "the CAADCA generally[] and the age estimation provision specifically" have a "concern[ing] . . . vast chilling effect" with substantial and negative implications for both adults' and children's Internet experiences, ER 24, and the provision "counter[s] the State's interest in increasing privacy protections for children." ER 24.

The CAADCA does not require "age verification," which involves determining a user's age with precision. Instead, it requires "age estimation," which means determining whether a user is a minor or adult with an appropriate degree of confidence. Specifically, the CAADCA 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). As the district court rightly noted, though age estimation may sound like a less demanding requirement than age verification, "in practice" it is a distinction without a difference because they are "quite similar." ER 24. Both require websites and apps to erect access barriers that "impede the availability and use of information and accordingly . . . regulate speech." ER 16 (internal quotation marks omitted).

The CAADCA does not specify the exact method that regulated entities must use to perform age estimation. That omission was not an accident. It reflects the

fact that no one—including the California Legislature—is clear as to how businesses should implement this law. Every available estimation option is problematic in ways that undercut the Legislature's objectives 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 overviews 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. As the district court recognized, self-reporting is of "little reliability" in determining age because of the users' ability and incentive to misreport. ER 24. As a result, it probably would not satisfy the CAADCA'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 confirm the submitter's connection to the submitted documents (otherwise, the submitter can use someone else's documents), the authenticator's 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 ages. And despite these limitations, document review poses significant risks because it necessarily requires a submitter to disclose the highly sensitive information within those documents. That information is likely to include an image of the submitter's face, such as in the case of a child uploading a picture of their passport.

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. 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

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

specifying that biometric information may qualify as "[s]ensitive personal information"). Further, privacy advocates have repeatedly warned 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, especially for children.

The Attorney General argues that the Act "explicitly discourages" "the use of invasive age estimation tools," but does not refute the conclusion that the only reliable age-estimation methods are necessarily invasive. Appellant's Op. Br. at 45 n.6; *see id.* at 38–39. As a result, even though the CAADCA prohibits businesses from retaining children's information obtained through these methods, it nonetheless compels them to collect that information through highly intrusive means. And children, who are still developing their judgment and digital literacy, are not well-equipped to decide for themselves whether to disclose their sensitive information and to whom. The CAADCA would effectively require businesses to train children that disclosing highly-sensitive information to strangers who ask is a normal and ordinary fact of life. By conditioning children to make this assumption, it becomes easier for malefactors to prey on children's underdeveloped skills through

illegitimate age-estimation processes on scam websites, thereby allowing malefactors to directly obtain children's information for nefarious purposes. And the CAADCA-mandated collection of sensitive information by legitimate businesses is vulnerable to exfiltration by malefactors who may intercept that information in real time, which would moot the CAADCA's prohibition on businesses retaining the information they collect.

The CAADCA thus mandates significant privacy invasions of children while simultaneously claiming to "prioritize the[ir] privacy, safety, and well-being." Cal. Civ. Code § 1798.99.29(b). It is for these reasons that the district court correctly concluded that the CAADCA's age-estimation requirement "exacerbate[s] the problem" it purports to resolve and thus fails to further the State's interests. ER 23.

III. Age Estimation Will Deter Internet Usage and Chill Speech Online.

The district court appropriately acknowledged that the burdens imposed by the CAADCA's age-estimation requirements will chill access to online content because "the steps a business would need to take to sufficiently estimate the age of child users would likely prevent both children and adults from accessing certain content." ER 16. It is thus no surprise that the district court followed the weight of precedent in concluding that the CAADCA raises serious First Amendment issues.

A. Age Estimation Imposes Excessive Burdens on Speech.

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

Regardless of the exact form it takes, an age-estimation 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. 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.

[5] There are few good options to do persistent and reliable age estimation 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.

The Attorney General protests that "age estimation is both viable and practical," criticizing NetChoice for allegedly lacking "expert evidence" and relying on supposedly "grossly outdated cases, which commented on age-estimation methods that were available *ten to twenty years ago*." Appellant's Op. Br. at 38. But the literature on this point is overwhelming and applies to any age-estimation method, old or new.

If age-estimation barriers add a short time delay (called "latency")—even if it is only a few seconds—to a user's access to a new website or service, the literature shows that it will drive many users away. A user leaving a website after accessing the first page is called the "bounce rate." As this Court has recognized, even 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.

Like page latency, the CAADCA's age-estimation 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 estimation, 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 CAADCA's mandated age estimation will likely require users to navigate at least one screen—called an "interstitial" screen—before the users can access their desired

[6] For example, one age-estimation vendor, Yoti, touts that its automated verifications take about eight seconds. *See Identity Verification*, Yoti, http://bit.ly/3IsASgK (last visited Jan. 28, 2024).

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, and it caused 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 CAADCA's mandated age-estimation 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 ("[I]nformation privacy concerns, trust, and brand awareness are particularly important in users' decisions to disclose personal information to register on commercial websites[.]").

The age-estimation process will thus result in a combination of time delays, intrusiveness from the interstitial process, and privacy and security risks that will cause bounce rates to soar. This, in turn, will produce problematic second-order effects. For example, the CAADCA 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-estimation process for new websites or apps. 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 estimation.

The district court rightly concluded that these consequences pressure businesses to "choose[] not to estimate age[,] but instead to apply broad privacy and data protections to all consumers, . . . the inevitable effect" of which "will be to

[7] If a website or app outsources its age-estimation 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)?

impermissibly 'reduce the adult population . . . to reading only what is fit for children.'" ER 25 (quoting *Butler v. Michigan*, 352 U.S. 380, 381 (1957)). And the district court correctly held on that basis that age-estimation barriers are a "substantially excessive means of achieving greater data and privacy protections for children." ER 25 (internal quotation marks omitted).

B. The CAADCA's Mandates Exceed the Age-Estimation Requirements That Courts Have Consistently Invalidated.

Courts have repeatedly rejected age-verification requirements analogous to the regulations at issue in this case on First Amendment 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. 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 enacted 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.*

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

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 First Amendment issues' that ma[d]e the statute unconstitutional." *Id.* at 195 (citation omitted). Specifically, the court agreed 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 (internal 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" (internal quotation marks omitted)); *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 1149 (10th Cir. 1999).

The CAADCA's mandated age-estimation 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-estimation 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. Despite the many changes to the Internet over the years, the evolution of age authentication technology has solved none of the Constitutional problems. It remains expensive, a delay to readers, and a privacy and security risk.

In fact, the CAADCA goes even further than the CDA, COPA, and Baby CDA laws by imposing mandatory age-estimation barriers not only on content readers, but also on authors seeking to publish content. *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 estimation 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 as well.

Furthermore, the privacy invasions caused by age estimation can increase anonymous authors' concerns that 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*, 582 U.S. at 105. Through its age-estimation provisions,

the CAADCA 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 CAADCA violates fundamental First Amendment principles and should not be permitted to go into effect.

CONCLUSION

For the above reasons, *amicus curiae* respectfully requests that this Court affirm the district court's grant of a preliminary injunction.

Dated: February 14, 2024

Respectfully submitted,

/s/ Jessica Ring Amunson

JESSICA RING AMUNSON
LINDSAY C. HARRISON
ANDREW C. DEGUGLIELMO
JENNER & BLOCK LLP
1099 New York Ave., N.W.
Suite 900
Washington, D.C. 20001
(202) 639-6000

jamunson@jenner.com

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

Jessica Ring Amunson, counsel for *amicus curiae*, hereby certifies that:

1. This Brief complies with the type-volume limitation in Rule 29 of the Federal Rules of Appellate Procedure because, excluding the parts of the document exempted by Rule 32(f), this document contains 4,586 words.

2. This Brief complies with the typeface requirements of Rule 32(a)(5) and the type-style requirements of Rule 32(a)(6) of the Federal Rules of Appellate Procedure because this document has been prepared in a proportionally-spaced typeface using Microsoft Word 2023 in 14-point Times New Roman.

/s/ Jessica Ring Amunson
Jessica Ring Amunson

Counsel for Amicus Curiae

February 14, 2024

CERTIFICATE OF SERVICE

I certify that on February 14, 2024, the foregoing Brief was filed electronically and served on the other parties via the Court's CM/ECF system.

/s/ Jessica Ring Amunson
Jessica Ring Amunson

Counsel for Amicus Curiae

February 14, 2024