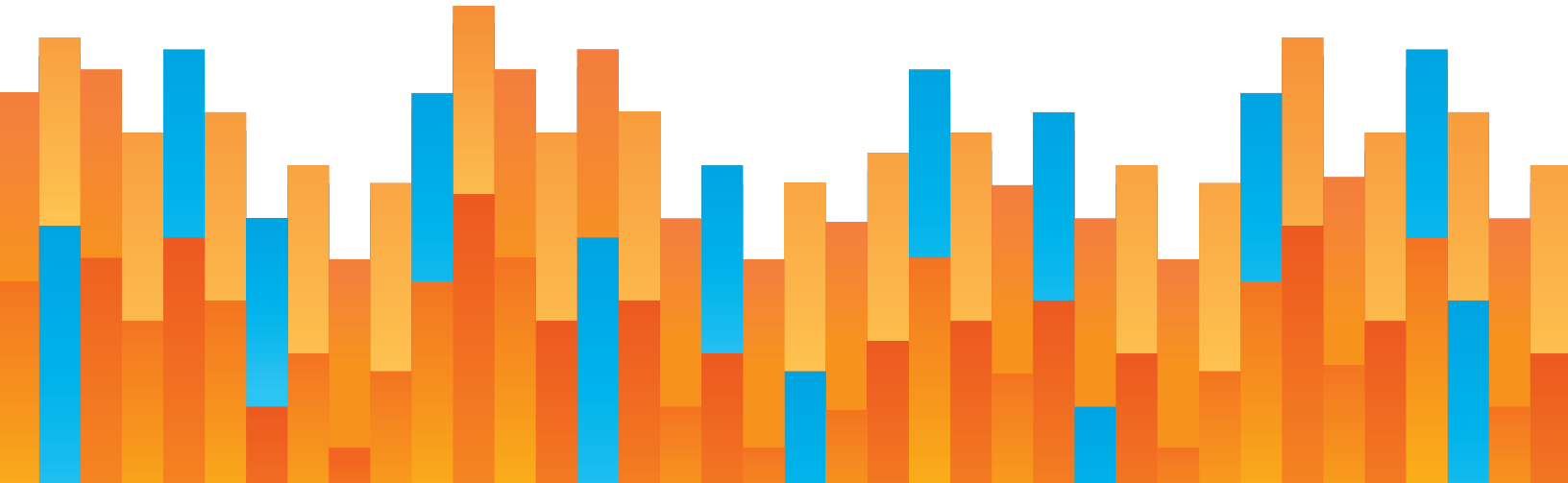
reason FOUNDATION

CALIFORNIA'S AGE-APPROPRIATE DESIGN CODE ACT: A DESIRE TO PROTECT CHILDREN DOESN'T PRODUCE GOOD LAW

by Eric Goldman and Adrian T. Moore

September 2023



Reason Foundation's mission is to advance a free society by developing, applying, and promoting libertarian principles, including individual liberty, free markets, and the rule of law. We use journalism and public policy research to influence the frameworks and actions of policymakers, journalists, and opinion leaders.

Reason Foundation's nonpartisan public policy research promotes choice, competition, and a dynamic market economy as the foundation for human dignity and progress. Reason produces rigorous, peer-reviewed research and directly engages the policy process, seeking strategies that emphasize cooperation, flexibility, local knowledge, and results. Through practical and innovative approaches to complex problems, Reason seeks to change the way people think about issues, and promote policies that allow and encourage individuals and voluntary institutions to flourish.

EXECUTIVE SUMMARY

In September 2022, California Gov. Gavin Newsom signed AB 2273, The California Age-Appropriate Design Code Act (AADC). The AADC is a far-reaching law that imposes many new requirements on most businesses in California.

Among other problematic provisions, the AADC imposes on websites 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." Alternatively, they must apply those privacy and data protections to *all* consumers.

In December 2022, NetChoice, an association of online services and platforms, filed a lawsuit seeking to overturn the law. NetChoice argues that the California law violates several amendments of the U.S. Constitution, as well as federal law designed to protect children online.

In fact, the AADC has a host of problems:

- The requirements of the law are vague: Age assurance is fundamentally the same as age verification, and available age-assurance methods all have significant flaws and risks;
- Age assurance requires children and adults alike to share—with virtually every website visited—sensitive personal information like identification documents or face

scans that, should they fall into the wrong hands, can be used for identity theft and other nefarious purposes;

- Age-assurance processes will slow down access to any website or app, which data show causes people to avoid using them, even more so when the slowdown is caused by sharing sensitive personal information. As a result, consumers will feel like they have less access to online information, goods, and services;
- The law does not just limit consumers' access to commercial speech. It equally creates barrier to accessing all forms of constitutionally protected speech. By making it harder for consumers to access their speech, the law directly chills the free speech rights of publishers;
- Moreover, the AADC also requires age assurance for websites or apps that allow users to publish any content online. This discourages the publication of user-generated content by making it harder to do so. It especially inhibits speech that requires anonymous or pseudonymous publication;
- U.S. courts have repeatedly rejected federal and state laws seeking to impose age verification requirements as violations of the First Amendment; and
- As the AADC's age-assurance requirements slow down access to online information, goods, and services, it will severely hamper the increasingly online economy and discourage new entrants in the online marketplace for ideas as well as commerce.

Imagine if, to protect children from seeing or buying potentially harmful products, you had to share your government-issued ID and wait for verification before you could enter any retail store—groceries, gas stations, liquor stores, bookstores, garden supply, etc.

Imagine if, to protect children from seeing or buying potentially harmful products, you had to share your government-issued ID and wait for verification before you could enter any retail store—groceries, gas stations, liquor stores, bookstores, garden supply, etc. That would be an extraordinary invasion of your private information just to do any shopping or browsing. And of course, children should be allowed to browse stores as well, even if they are not child-oriented stores, to find the items they are looking for. It makes no more sense for online businesses than for physical stores.

TABLE OF CONTENTS

PART 1 INTRODUCTION 1

PART 2 THE AADC'S AGE-ASSURANCE REQUIREMENTS FUNDAMENTALLY CHANGE ACCESS TO ONLINE CONTENT 4

An Age Assurance Process Is Not Simple 4

Security Concerns 6

Age Assurance Will Slow Access and Reduce Internet Use 8

PART 3 AGE-VERIFICATION REQUIREMENTS CHILL ONLINE ACCESS TO FIRST AMENDMENT PROTECTED SPEECH AND EXERCISE OF PROTECTED ONLINE SPEECH 11

Reduced Use of the Internet Reduces Access to Protected Speech 11

Age Assurance Chills Exercising Free Speech Online 12

PART 4 AGE VERIFICATION HAS BEEN REPEATEDLY REJECTED BY COURTS ON FIRST AMENDMENT GROUNDS 13

PART 5 THE AADC NEGATIVELY AFFECTS THE INCREASINGLY ONLINE ECONOMY 16

PART 6 CONCLUSION 17

ABOUT THE AUTHORS 19

PART 1

INTRODUCTION

In September 2022, California Gov. Gavin Newsom signed AB 2273, The California Age-Appropriate Design Code Act (AADC), a far-reaching law that imposes many new requirements on most businesses in California.[1] Soon after, NetChoice, an association of online firms, filed a federal lawsuit seeking to overturn the law.[2] NetChoice argues that the California law violates several amendments of the U.S. Constitution, as well as federal law designed to protect children online.[3] A number of experts, including this author, have filed *amicus* briefs to this case, highlighting important legal and policy issues the court should consider as it evaluates this case.[4]

As the U.S. Supreme Court previously declared in *Reno v. ACLU*, the internet is a "unique and wholly new medium of worldwide human communication."[5] Among its many special properties, the internet makes it easy for users to navigate seamlessly between many websites operated by unrelated entities.[6] The Supreme Court explained that "[L]inks from

1 California Legislature, AB-2273 The California Age-Appropriate Design Code Act, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273

2 NetChoice, LLC v. Bonta, 5:22-cv-08861, (N.D. Cal.), https://www.courtlistener.com/docket/66636540/netchoice-llc-v-bonta/

3 NetChoice, NetChoice v. Bonta, *https://netchoice.org/netchoice-v-bonta/*

4 This policy brief is based on the author's amicus curiae brief filed in this case.

5 *Reno v. ACLU*, 521 U.S. 844, 850 (1997).

6 Ibid., 929 F. Supp. 824, 836-37 (E.D. Pa. 1996).

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[.]"[7]

> *"Among its many special properties, the internet makes it easy for users to navigate seamlessly between many websites operated by unrelated entities."*

California's AADC threatens this foundational principle of the internet. Enacted under the pretext of protecting children's privacy, the AADC regulates businesses that develop and provide online services, products, or features that children are likely to access.[8] 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.[9] 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."[10]

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 those privacy and data protections to *all* consumers.[11] 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 though they are children. Violations of the AADC's requirements can result in penalties of up to $7,500 per affected child, as well as injunctive relief.[12]

7 *Reno v. ACLU*, *aff'd*, 521 U.S. 844 (1997).

8 Cal. Civ. Code § 1798.99.29(a).

9 Ibid., § 1798.99.31(a)(1)(B)(i)-(vii)

10 Ibid., § 1798.99.31(b).

11 Ibid., § 1798.99.31(a)(5)

12 Ibid., § 1798.99.35(a).

Imagine if, to protect children from seeing or buying potentially harmful products, you had to give your government-issued ID and wait for verification before you could enter any retail store—groceries, gas stations, liquor stores, bookstores, garden supply, etc. That would be an extraordinary invasion of your private information just to do any shopping or browsing. And of course, children should be allowed to browse stores as well, even if they are not child-oriented stores, to find the items they are looking for. It makes no more sense for online businesses than for physical stores.

The AADC's age-assurance requirement erects onerous barriers that would discourage internet use and chill protected speech.

The AADC's age-assurance requirement erects onerous barriers that would discourage internet use and chill protected speech. These barriers to online communication will change how people use the internet in ways that will hinder the internet's utility to society—and transgress basic constitutional principles as well. In short, the AADC severely restricts free speech and, as the Supreme Court said when ruling against an age verification requirement law in 1997, "threatens to torch" a large segment of the internet community.[13]

[13] *Reno v. ACLU*, 521 U.S. at 882.

PART 2

THE AADC'S AGE-ASSURANCE REQUIREMENTS FUNDAMENTALLY CHANGE ACCESS TO ONLINE CONTENT.

The AADC's proponents argue it is a way to protect children online, but it has substantial, negative implications for both adults' and children's internet experiences.

2.1 AN AGE ASSURANCE PROCESS IS NOT SIMPLE

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 *estimate* the age of children who try to access their websites "with a reasonable level of certainty appropriate to the risks."[14] 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 consumers can access or use their services.

[14] Cal. Civ. Code § 1798.99.31(a)(5)

The AADC does not specify the exact method that regulated entities must use to perform age assurance. That omission 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 objectives of increasing children's privacy.[15] There is no approach that provides reliable verification, complete coverage of the population, and still protects individuals' data and privacy.[16]

The AADC does not specify the exact method that regulated entities must use to perform age assurance. That omission reflects the fact that no one—including the California Legislature—is clear how businesses should implement this law.

Subject to those severe limitations, there are three 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 they are adults. 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.[17]

"Document review" requires users submit 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's identity with the submitted documents (otherwise, the submitter can use someone else's documents), the cost and time required to review the submitted documents,

15 See CNIL, "Online Age Verification: Balancing Privacy and the Protection of Minors," (Commission Nationale de l'Informatique et des Libertés, Paris, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

16 Jackie Snow, "Why Age Verification Is So Difficult for Websites," *Wall Street Journal*, February 27, 2022, http://bit.ly/41ngt5m

17 Cal. Civ. Code § 1798.99.31(a)(5).

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. As one example of a flaw, one study found that such software tends to overestimate age by up to two and half years if the person smiles while their face is scanned.[18]

> *Unless age-assurance is repetitively done each time a consumer accesses the service, each age-assurance method can be defeated at the device level. Devices can be shared between minors and adults, or minors may get an adult to do a single but persistent bogus authentication.*

Unless age-assurance is repetitively done each time a consumer accesses the service, each age-assurance method can be defeated at the device level. Devices can be shared between minors and adults, or minors may get an adult to do a single but persistent bogus authentication.

2.2 SECURITY CONCERNS

Sharing personal information online in order to gain access to a website creates a number of security and privacy concerns. Sharing identification documents carries many security risks, since images of those documents or their information may not be adequately secured by every website, and such information can be used to steal an identity, for example. A person's face is considered highly sensitive personal information because it is unique to each person but also immutable, so if a person's facial image is digitally stolen and

[18] Tzvi Ganel, Carmel Sofer, and Melvyn A. Goodale, "Biases in human perception of facial age are present and more exaggerated in current AI technology," *Scientific Reports*, 2022; 12 (1), https://www.nature.com/articles/s41598-022-27009-w

misused, it can wreak havoc on that person's life without any easy means of repair. For that reason, privacy advocates repeatedly warn consumers about face-scanning technologies due to the privacy and security risks they create.[19] Further, many biometric privacy laws around the country severely restrict the use of face scans. Indeed, California law defines biometric information to include face, vein patterns, and faceprints and specifies that biometric information may qualify as sensitive personal information.[20]

Widespread deployment of face-scanning technologies on the internet in order to comply with California law would teach consumers to disregard that privacy advice and thereby dramatically increases their risks.

> *… each new user will have to decide if accessing a website or an app is worth the risk* without first being able to inspect it *to determine if they consider it trustworthy.*

Because of these risks, each new user will have to decide if accessing a website or an app is worth the risk *without first being able to inspect it* to determine if they consider it trustworthy. Consumers need information about a website when deciding whether or not to disclose personal information to that site, but mandatory age-assurance before consumers access the site ironically deprives them of the information they need to make that important decision.[21] And 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)?

19 For example, Nigel Jones, "10 Reasons to Be Concerned About Facial Recognition Technology," Privacy Compliance Hub, August, 2021, https://bit.ly/3XXLWbp (Accessed June 10, 2023).

20 Cal. Civ. Code § 1798.140(c) & (ae). See Eric Goldman, "Do Mandatory Age Verification Laws Conflict with Biometric Privacy Laws?–Kuklinski v. Binance," Technology and Marketing Law Blog, April 8, 2023, https://blog.ericgoldman.org/archives/2023/04/do-mandatory-age-verification-laws-conflict-with-biometric-privacy-laws-kuklinski-v-binance.htm

21 Ting Li and Paul A. Pavlou, "What Drives Users' Website Registration?," Social Science Research Network (SSRN), December, 2013, http://bit.ly/3St0ezI

It is true that all of this involves consent—each user can decide whether accessing this website or app is worth sharing personal information. Ironically, the AADC is imposing these requirements to "protect children," yet it requires children to make these weighty decisions about which services to trust without the information they need and without acknowledging that minors are legally deemed to have diminished capacity to consent for themselves.

2.3 AGE ASSURANCE WILL SLOW ACCESS AND REDUCE INTERNET USE

The age-assurance methods discussed above necessarily add a new time-consuming and annoying 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 accounts will force their users to tediously repeat the age-assurance process each time the user tries to access the website or app. There are few good options to do persistent and reliable age assurance if consumers do not create account logins.

> *"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 and will dramatically reduce user visits and participation."*

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 and will dramatically reduce user visits and participation. The literature on this point is

overwhelming. Users are highly discouraged by any access barriers to the online destinations they seek.

If the age-assurance 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, it would drive many users away. Whenever a user leaves a website after accessing only the main page, that's called the bounce rate. Small increases in latency can increase bounce rates, often dramatically. Every additional second a site takes to load can cause up to 10% of potential visitors to go elsewhere, and if a page takes longer than three seconds to load, 53% of visitors will simply navigate away.[22] One analysis found 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%.[23]

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 or minutes.[24] While going through an age-verification process to access a website or app is not the same as latency slowing access, people's reaction to latency suggests that the delays of an age-verification process will cause many to turn away from those websites or apps.

> *The AADC-mandated age-assurance interstitial will likely result in even higher bounce rates because it will require users to provide private and sensitive information.*

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—

22 *Will Co. v. Lee*, 47 F.4th 917, 924-25 (9th Cir. 2022)

23 Daniel An, "Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed," Think with Google, February, 2018, https://bit.ly/3ILJccK

24 For example, one age-assurance vendor, Yoti, touts that its automated verifications take about eight seconds: Yoti, Identity Verification, http://bit.ly/3IsASgK (accessed June 10, 2023).

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 and saw a 69% bounce rate.[25] The AADC-mandated age-assurance interstitial will likely result in even higher bounce rates because it will require users to provide private and sensitive information.[26]

[25] David Morell, "Google+: A Case Study on App Download Interstitials," Google Search Central Blog, Google, July 23, 2015), https://bit.ly/3ILQY6i (Accessed June 10, 2023).

[26] CNIL, Online Age Verification.

PART 3

AGE-VERIFICATION REQUIREMENTS CHILL ONLINE ACCESS TO FIRST AMENDMENT PROTECTED SPEECH AND EXERCISE OF PROTECTED ONLINE SPEECH

3.1 REDUCED USE OF THE INTERNET REDUCES ACCESS TO PROTECTED SPEECH

AADC's age-assurance requirement as a condition of user participation has 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 for products or services. But most of the content will be speech that qualifies for maximum constitutional protection under the law, restrictions of which courts evaluate with strict scrutiny.[27] However, the AADC draws no distinction between commercial and noncommercial speech.

[27] "To pass strict scrutiny, the legislature must have passed the law to further a "compelling governmental interest," and must have narrowly tailored the law to achieve that interest. Strict scrutiny is the highest standard of review which a court will use to evaluate the constitutionality of governmental discrimination." Legal Information Institute, "Strict Scrutiny," Cornell Law School, https://www.law.cornell.edu/wex/strict_scrutiny (accessed June 28, 2023).

> *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 for products or services. But most of the content will be speech that qualifies for maximum constitutional protection under the law...*

3.2 AGE ASSURANCE CHILLS EXERCISING FREE SPEECH ONLINE

In fact, the AADC goes further than the previous age verification laws by imposing mandatory age-assurance barriers not only on content readers, but also on content authors.[28] Websites and apps that allow users to author and publish content, perhaps even just posting comments or reviews, must conduct age assurance on *every* prospective author before they are granted permission. This process will cause high bounce rates for prospective authors and deter them from publishing their constitutionally protected speech.

Furthermore, the privacy invasions caused by age assurance may increase anonymous authors' concerns that their online posts will be attributed to them because it creates a record linking a specific individual to where they visit, comment, and publish online.[29] The Third Circuit Court of Appeals cautioned in a 2002 case regarding an age verification law, "People 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."[30]

28 Cal. Civ. Code § 1798.99.31(a)(5) (requiring covered businesses to "[e]stimate the age of child *users*") (emphasis added)).

29 CNIL, Online Age Verification.

30 *ACLU v. Ashcroft*, 322 F.3d at 259.

PART 4

AGE VERIFICATION HAS BEEN REPEATEDLY REJECTED BY COURTS ON FIRST AMENDMENT GROUNDS

Courts have repeatedly rejected on constitutional grounds age-verification requirements analogous to the AADC requirements. In the late 1990s, Congress and some 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.[31] The CDA criminalized the knowing transmission of obscene or indecent messages to minors over the internet.[32] The law provided an affirmative defense for those who restricted access to covered materials by implementing age-verification measures.[33] But the Court held that age-verification requirements "would not significantly narrow the statute's burden on noncommercial

31 Communications Decency Act, 521 U.S. 844 (1997) and *Reno v. ACLU,* 1997.

32 *Reno v. ACLU*, at 859.

33 Ibid., at 860-61.

speech" because "it is not economically feasible for most noncommercial speakers to employ such verification."[34]

> *The Third Circuit reiterated the district court's factual findings that age-verification measures would burden protected speech, holding that people would be deterred from accessing websites because most they are unwilling to provide sensitive personal information to gain access to content, 'especially where the information they wish to access is sensitive or controversial.'*

In response, in 1998, Congress passed the Child Online Protection Act (COPA).[35] 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, that ultimately ended in its invalidation as unconstitutional.[36] The courts 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 age-verification measures would burden protected speech, holding that people would be deterred from accessing websites because most they are unwilling to provide sensitive personal information to gain access to content, "especially where the information they wish to access is sensitive or controversial."[37]

Five years later, when the Third Circuit struck down COPA for good, the court condemned age-verification requirements in even stronger terms.[38] The court concluded that age-verification requirements deter some users from accessing information; that adding age-verification technologies impose high costs; and that the loss of traffic to their website

34 *Reno v. ACLU,* at 881-82.

35 Pub. L. No. 105-277, tit. XIV, 112 Stat. 2681, 2681-736 (1998).

36 *See Ashcroft v. ACLU*, 535 U.S. 564 (2002) and *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

37 *ACLU v. Ashcroft*, 322 F.3d 240, 258-59 (3d Cir. 2003), *aff'd*, 542 U.S. 656 (2004).

38 *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008).

caused by use of those technologies created an undue burden on web publishers. They concluded that all of this adds up to a chilling of protected speech.[39]

In addition, several states have 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:

- Age-verification provisions that require credit card validation would completely block adults who don't have a credit card and would deter those unwilling to provide their credit card number online, blocking access to speech in ways that may violate the First Amendment;[40]
- Age verification violates the First Amendment because it deters lawful users from accessing speech they are entitled to see; and[41]
- Age verification violates both the First and Fourteenth Amendments by preventing people from communicating and accessing information anonymously.[42]

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 Supreme Court pointed out that age verification essentially drives protected speech from the marketplace of ideas, and that is prohibited by the First Amendment.[43]

"The Supreme Court pointed out that age verification essentially drives protected speech from the marketplace of ideas, and that is prohibited by the First Amendment."

39 *ACLU v. Mukasey,* 197.

40 *PSINet, Inc. v. Chapman*, 362 F.3d 227, 236-37 (4th Cir. 2004).

41 *Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773, 782 (D.S.C. 2005)

42 *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998), *aff'd*, 194 F.3d 1142 (10th Cir. 1999).

43 *Ashcroft*, 322 F.3d at 260-61.

PART 5

THE AADC NEGATIVELY AFFECTS THE INCREASINGLY ONLINE ECONOMY

The AADC will cause a combination of time delays, intrusive interstitial pages, and privacy and security risks, meaning ultimately that bounce rates will soar. The reduced audience may cost businesses revenues and profits. For example, an Amazon analysis found that every 100 milliseconds of latency cost it 1% in sales.[44] Another study showed that for consumer-oriented online retailers, the impact of a modest slowdown in access is sizable. A site that loads in one second has an e-commerce conversion rate 2.5 times higher than a site that loads in five seconds.[45]

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. Because users don't yet trust these platforms, they will be less willing to navigate the age-assurance process. This resistance, in turn, will benefit incumbents with whom users already have accounts or who have already established a strong enough trust relationship. Those users are more likely to get past their reluctance to do age assurance with sites and apps they're already familiar with. This in turn means it will be harder for new websites or apps to enter the market and gain users because potential users won't have a chance to learn the value of the new website or app before having to share sensitive personal information.

44 Will Co. v. Lee, at 925.

45 Michael Wiegand, "Site Speed is (Still) Impacting Your Conversion Rate," Portent, April 20, 2022, https://bit.ly/3EwJWQm

PART 6

CONCLUSION

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.[46] 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.

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."[47]

46 *Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017).

47 Cal. Civ. Code § 1798.99.29(b).

In sum, the AADC has a host of problems:

- The requirements of the law are vague: Age assurance is fundamentally the same as age verification, and available age-assurance methods all have significant flaws and risks;
- Age assurance requires sharing—with virtually every website visited—sensitive personal information like identification documents or face scans that, should they fall into the wrong hands, can be used for identity theft and other nefarious purposes;
- Age-assurance processes will slow down access to any website or app, which data show causes people to avoid using them, even more so when the slowdown is caused by sharing sensitive personal information. The result is less access to online information, goods, and services;
- The content that will be affected by this law will not just be commercial speech, but all forms of constitutionally protected speech. This loss of access directly chills free speech;
- Moreover, the AADC also requires age assurance for websites or apps that allow users to publish any content online;
- U.S. courts have repeatedly rejected federal and state laws seeking to impose age verification requirements as violations of the First Amendment; and
- As the AADC's age-assurance requirements slow down access to online information, goods, and services, it will severely hamper the increasingly online economy and discourage new entrants in the online marketplace for ideas as well as commerce.

> *… 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.*

ABOUT THE AUTHORS

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. Professor Goldman has been researching internet law for 30 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."[48]

Adrian Moore, Ph.D., is vice president of policy at Reason Foundation, a non-profit think tank advancing free minds and free markets. Moore leads Reason's policy implementation efforts and conducts his own research on a wide range of policy topics including transportation, energy, privatization, drug policy and government and regulatory reform. Moore, who has testified before Congress on several occasions, regularly advises federal, state and local officials on ways to improve policy outcomes and reduce costs. In 2008 and

[48] Brian Leiter, "10 Most-Cited Law & Technology Scholars in the U.S., 2016-2020 (CORRECTED), Weblog post, *Brian Leiter's Law School Reports,* September 9, 2021, https://leiterlawschool.typepad.com/leiter/2021/09/10-most-cited-law-technology-scholars-in-the-us-2016-2020.html (Accessed June 28, 2023).

2009, Moore served on Congress' National Surface Transportation Infrastructure Financing Commission. The commission offered "specific recommendations for increasing investment in transportation infrastructure while at the same time moving the Federal Government away from reliance on motor fuel taxes toward more direct fees charged to transportation infrastructure users." During 2009–2011 he served on California's Public Infrastructure Advisory Commission.

Moore is co-author of the book *Mobility First: A New Vision for Transportation in a Globally Competitive 21st Century* (Rowman & Littlefield, 2008). Texas Gov. Rick Perry said, "Speaking from our experiences in Texas, Sam Staley and Adrian Moore get it right in Mobility First." World Bank urban planner Alain Bartaud called it "a must read for urban managers of large cities in the United States and around the world."

Moore is also co-author of *Curb Rights: A Foundation for Free Enterprise in Urban Transit*, published in 1997 by the Brookings Institution Press, as well as dozens of policy studies. His work has been published in the *The Wall Street Journal, Los Angeles Times, Boston Globe, Houston Chronicle, Atlanta Journal-Constitution, Orange County Register*, as well as in *Public Policy and Management, Transportation Research Part A, Urban Affairs Review, Economic Affairs*, and numerous other publications.

In 2002, Moore was awarded a World Outsourcing Achievement Award by PricewaterhouseCoopers and Michael F. Corbett & Associates Ltd. for his work showing governments how to use public-private partnerships and the private sector to save taxpayer money and improve the efficiency of their agencies.

Prior to joining Reason, Moore served 10 years in the Army on active duty and reserves. As a noncommissioned officer he was accepted to Officers Candidate School and commissioned as an infantry officer. He served in posts in the United States and Germany and left the military as a captain after commanding a Heavy Material Supply company.

Moore earned a Ph.D. in economics from the University of California, Irvine. He holds a master's in economics from the University of California, Irvine and a master's in history from California State University, Chico.