AGE VERIFICATION IN THE CROSSHAIRS: HOW *NETCHOICE V. BONTA* COMPLICATES LEGISLATORS' ABILITY TO PROTECT CHILDREN ONLINE

Jake Holland[*]

* * *

Introduction

For most middle- and upper-income children born since the mid-1990s, acquisition of a personal smartphone or laptop has marked a rite of passage. With reliable internet access and the push of a few buttons, teens and tweens have a window into the world—news articles in dozens of foreign languages, social media platforms like Tumblr that enable the sharing of overwrought poetry and cringey selfies, and a host of other websites both awe-inspiring and anodyne. But while unfettered access to the Web allows for the possibility of exploration and self-growth, it also carries with it the risk of child predators and harms attendant to the viewing of offensive content such as pornography and real-world violence.

Against this backdrop, legislators in the Golden State devised the California Age-Appropriate Design Code Act (CAADCA), which was signed into law by Governor Gavin Newsom on September 15, 2022. The CAADCA regulates the collection, storage, and processing of personal data of individuals under 18 and requires covered websites to estimate the age of users and create notices that they may be tracked. Though originally set to take effect July 1, 2024, the law's future remains uncertain after a federal district court judge in September granted a preliminary injunction. The pro-internet-expression group NetChoice, which sued California Attorney General Rob Bonta in the Northern District of California, argues that the law—ostensibly aimed at protecting children and their data online—will hobble free speech on the internet and require companies to employ age-verification procedures that are both imprecise and overbroad. This Case Note examines the stakes of this litigation, explores the constitutional viability of the CAADCA, and argues for legislative amendments that could allow the law (or others in the same vein) to better weather future legal challenges.

I. Kids Online and Calls for Reform

The internet, as most users can attest, is porous. A student researching thermodynamics can toggle between Wikipedia, YouTube,

---

[*] Jake Holland is a J.D. Candidate at the University of Chicago Law School, Class of 2025. He thanks Alexandra Webb, Michael Jeung, Erin Yonchak, and the *University of Chicago Law Review Online* team.

and her professor's blog within seconds; no log ins, let alone age verifications, are required. The porousness of the internet enhances its utility—unlike libraries, where a patron has to physically roam the stacks and check out materials at a centralized front desk, Web surfers can hop to and fro with little friction. Sure, there are websites that are paywalled or require users to make accounts before accessing them, but for the most part, access is free. Even websites that require users to be over 18, like those hosting catalogues of pornography, take a viewer's word at face value when she testifies she is of age. The result? Children accessing sites at an age that many in society believe they shouldn't.

The CAADCA was the result of bipartisan efforts to rein in big tech, and the state lawmakers who proposed the legislation highlighted social media's addictive nature and adverse effect on adolescent mental health. But the CAADCA is not the first piece of legislation aimed at protecting children on the Web. At the federal level, the Children's Online Privacy Protection Act (COPPA) requires that companies obtain parental consent before collecting personal information from children under the age of 13. Utah, which has the lowest median age of any U.S. state, enacted in March 2023 the Social Media Regulation Act, which requires social media companies to obtain parental consent before opening accounts for those under 18 years of age. Across the Atlantic, the United Kingdom's Age Appropriate Design Code (also known as the Children's Code) imposes similar requirements to the CAADCA and formed the basis of California's measure. Though the CAADCA faces an uncertain future, states including Connecticut and Minnesota have floated similar proposals, and legislative attention to the issue of kids' safety is unlikely to abate.

II. Anatomy of the CAADCA

Not every company operating in California will have to comply with the CAADCA. Instead, the law applies only to for-profit California entities that proffer "an online service, product, or feature likely to be accessed by children" under 18 and either (1) make over $25 million in annual gross revenue, (2) buy or sell the personal information of over one hundred thousand users, or (3) derive at least 50% of annual revenue from the selling or sharing of consumers' personal information. At base, the CAADCA requires companies to conduct data protection impact assessments (DPIAs), provide privacy by default, and clearly identify tracking signals. Businesses must also provide clear privacy policies, estimate and tailor products by age, and allow children or their parents to exercise their privacy rights and report concerns.

Covered entities are prohibited from using dark patterns (subtle website features designed to compel users to conduct a certain action) to encourage children to provide personal information. They also may not use a child's personal data "in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child." Precise geolocation data, which poses unique privacy risks for individuals, cannot be collected, sold, or disclosed unless strictly necessary.

The CAADCA does not have a private right of action, meaning that children and their parents won't be able to sue technology companies for noncompliance. Instead, enforcement will be vested in the state's attorney general, who can fine companies up to $2,500 per affected child for negligent violations and $7,500 per affected child for intentional violations. It is unclear how much teeth these fines may have given that the attorney general must provide written notice to noncompliant businesses and allow them ninety days to cure any potential violations.

III. Industry Pushback and *NetChoice v. Bonta*

While popular among California voters, the CAADCA faced significant industry pushback during the legislative process and after its inception. Technology groups including NetChoice, the Computer and Communications Industry Association, and the Chamber of Progress lambasted legislation aimed at children online and hired lobbyists to stop their passage, arguing that increased regulations stifle speech and free expression in cyberspace. The CAADCA, however, was enacted despite these criticisms. NetChoice sued Bonta in December 2022, arguing among other things that the law facially violates the First Amendment and is preempted by COPPA and § 230 of the Communications Decency Act.

Judge Beth Labson Freeman in her September 18, 2023, order granting a preliminary injunction focused on the free speech claims:

> The Court finds that although the stated purpose of the Act—protecting children when they are online—clearly is important, NetChoice has shown that it is likely to succeed on the merits of its argument that the provisions of the CAADCA intended to achieve that purpose do not pass constitutional muster. Specifically, the Court finds that the CAADCA likely violates the First Amendment.

A. First Amendment Analysis

At a high level, an entity violates the First Amendment when it (1) regulates protected speech and (2) fails to pass the applicable level of scrutiny. In her preliminary analysis, Judge Freeman found the

CAADCA likely regulates protected speech because it targets certain speakers (some for-profit entities) and not others (governmental bodies and nonprofits). She noted that the record made it difficult to decide whether the law regulates only commercial speech (which could trigger intermediate scrutiny), or noncommercial speech that is inextricably intertwined with commercial speech (which could trigger strict scrutiny). The distinction, Judge Freeman wrote, had little import for present purposes since many of the law's prohibitions and mandates would fail the less stringent intermediate scrutiny standard. Assuming the CAADCA regulates commercial speech, it is the state's burden to show "at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest."

After establishing that the CAADCA likely regulates protected speech, Judge Freeman applied the commercial speech scrutiny standard to each of the law's prohibitions and mandates. In so doing, she found that most of them would not pass constitutional muster. For instance, the requirement that covered companies conduct DPIAs did not directly advance the government's goal of "promoting a proactive approach to the design of digital products, services, and feature[s]" for kids. Likewise, the age estimation requirements of the statute likely violate the First Amendment because they don't directly advance the state's interest in promoting minor health and well-being. Although the state had argued that more onerous verification methods existed, Freeman noted that even the "supposedly minimally invasive tools" at issue would actually worsen the problem of children's safety online by requiring them to submit to face scans that were locally analyzed and stored.

B. Severability

NetChoice in its lawsuit argued that the entire CAADCA must be struck down, and that the challenged provisions could not be severed from the Act's remaining text. Judge Freeman agreed, writing that severance would be "futil[e]" given that the only remaining provisions would be those "setting forth the statute's title, findings, and definitions; two mandates; three prohibitions; and provisions establishing a working group, DPIA report deadlines, and penalties for violating the Act."

The "only meat left," she wrote, would be the four unchallenged provisions that require businesses to provide obvious tracking signals and prominent tools for children to exercise their privacy rights and to refrain from collecting kids' precise geolocation data. But those features do little without businesses being able to vet users' ages—and Judge Freeman found the statute's age estimation provisions likely do

not pass constitutional muster. Furthermore, none of the provisions can be enforced without penalties, which require knowing whether a business is in compliance with the DPIA report requirement. Again, such a mandate is likely unconstitutional, and the intertwined nature of the challenged and unchallenged provisions means the entire statute, at least in its current form, must be axed, she said.

IV. Balancing Free Speech and Safety Online

In the digital age, there is a perennial tension between safety and individuals' rights to privacy and free expression. On the one hand, governments want to—and arguably should—clamp down on dangers such as extremism, child predation, and hate speech. But tools to do so, including age verification services, pose unique privacy concerns and threaten to undermine the internet as a public forum and one of the rare havens of anonymous expression. This tension is palpably clear in Judge Freeman's analysis, as she nods to the laudable goal of the CAADCA while still acknowledging that it is likely violative of Americans' constitutional rights. I propose tweaking the CAADCA to allay these free speech concerns and give it a better chance of surviving current and future legal challenges.

A. Practices in Lieu of Age Estimation

Age verification policies face a tough upward battle vis-à-vis free speech, and critics are right to note that they chill speech online and undermine user anonymity. Even if the statutory text regarding these tools is tweaked, they are unlikely to survive given their paradoxical nature. As Judge Freeman notes: "[T]he CAADCA's age estimation provision appears not only unlikely to materially alleviate the harm of insufficient data and privacy protections for children, but actually likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information."

Legislators should scrap the age estimation provision and instead move to a self-directed opt-in model. This could take several forms. Websites could ask users to input their birthdays, or they could make them check a box stating they are of legal age. Emerging technologies such as blockchain could be employed to verify children's ages via an ID without needing to confirm with an intermediary. Such decentralized systems could obviate free speech concerns and potentially allow the age estimation feature to survive future challenges.

It is true that such substitutions (except potentially blockchain) would substantially water down the measure. After all, kids can lie about their age and circumvent the safety measures dreamed up by

these laws. But something is better than nothing, and because so many of the CAADCA's provisions are premised on the DPIA reports and age verification, making the above changes will give them a better shot at surviving legal challenges and move the needle forward regarding children's safety without sacrificing privacy and anonymity.

B. Increasing Effectiveness of the DPIAs

Judge Freeman found that the DPIA requirement failed to address the identified harms, and thus didn't materially advance the government's interest—something required for the provisions to survive a First Amendment challenge. But Judge Freeman's own reasoning leaves wiggle room for changes. She notes that the CAADCA fails to require businesses to assess the potential harm of product designs. A legislative amendment could require businesses to do as much. Judge Freeman also notes that the CAADCA contains no actual requirement for businesses to adhere to timed plans to mitigate risks before online services are accessed by children. An amended CAADCA could impose penalties for lack of adherence or add a private right of action for individuals to sue businesses that fail to mitigate identified risks. By integrating changes based on Judge Freeman's own analysis, lawmakers could render the law more effective at achieving its stated goal of protecting kids online and thus advance an important governmental interest. Assuming the DPIA and age estimation requirements can be tweaked to pass constitutional muster—that is, by requiring product design harm analysis, adding a more robust enforcement mechanism, and using blockchain or other new technologies to remedy privacy concerns—a substantial portion of the law may be able to be severed from those provisions which remain unconstitutional.

C. Industry Next Steps

Given the preliminary injunction, it is unlikely companies will need to comply with the CAADCA by its original effective date of July 1, 2024. But that doesn't mean industry should remain complacent and ignore the broader precepts of the measure. After all, Judge Freeman's order is just a preliminary injunction, and it's well within the realm of possibility that the state proffers alternative explanations or legal arguments that lead her to view the law as constitutional. It's also plausible that an appellate court disagrees with Judge Freeman's analysis and the CAADCA rolls out as originally intended.

While the *NetChoice* ruling means companies may breathe a sigh of relief for now, compliance in the online-safety arena is not going away—and neither is Americans' budding interest in more strictly controlling the flow of their personal data. Over a dozen U.S. states

now have consumer data privacy statutes, and countries including Canada, China, and the United Kingdom have privacy and cybersecurity laws on the books that impact the data collection practices of U.S. multinational corporations. In fact, laws in each of those jurisdictions already require data protection assessments of some sort. A Pew Research Center poll from 2019 found that 75% of Americans favored more stringent government regulations regarding what companies can do with their data, and news articles published in recent years have exposed the dangers of facial recognition software and apps designed to track users' menstrual cycles. All told, these trends mean companies—especially those that deal with children or sensitive information such as biometric face scans—will likely face greater compliance requirements down the line. They would be wise to start thinking about business adjustments now.

* * *

Jake Holland is a J.D. Candidate at the University of Chicago Law School, Class of 2025. *He thanks Alexandra Webb, Michael Jeung, Erin Yonchak, and the* University of Chicago Law Review Online *team.*