March 19, 2024

Senate Committee on Business, Labor, and Technology
Attn: Jeanette Chapman, Legislative Assistant
Colorado State Capitol
200 East Colfax Ave
Denver, CO 80203

RE: SB 24-158 - "Social Media Protect Juveniles Disclosures Reports" (Oppose)

Dear Chair Danielson and Members of the Senate Committee on Business, Labor, and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 24-158 in advance of the Senate Committee on Business, Labor, and Technology hearing on March 19, 2024.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members. CCIA and our member companies have a shared interest in ensuring strong protections are in place to protect children and provide parents and adults with simple but effective tools to provide a safe online environment for their families.

CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Presently, our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.[2] CCIA's members have been leading the effort to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to their unique lived experience and developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools to allow parents to block specific sites entirely.[3] This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on what mechanisms presently exist that they can use now to protect their children the way they see fit and based on their family's lived experiences.[4]

It should also be recognized that protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Speech that is neither obscene to young people nor subject to other legitimate laws cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors. Proposals to keep children safe online should be established through a risk-based approach to developing protections for different ages of users and by focusing on tangible harm. While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[3] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[4] *See supra* note 2.

SB 24-158's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

SB 24-158 would hold covered social media companies liable for failing to perform age verification but also requires a social media company to dispose of any identifying information about the user after verifying their age. However, by requiring covered businesses to delete relevant information, the law would leave businesses without a means to document their compliance. This becomes especially problematic in instances where a user decides to use deceptive verification information such as using an identification card that is not their own. Additionally, it is unclear what impact users' employment of virtual private networks (VPNs)[5] and other mechanisms to avoid location-specification age verification requirements could have on organizations' liability under this bill. It does not advance the bill's goal to place covered companies in a Catch-22 where they cannot be fully compliant without incurring new liability.

More broadly, the bill's obligation to collect additional information associated with age verification is itself likely to conflict with data minimization principles inherent in typical federal and international privacy and data protection compliance practices. If the state were to force companies to collect a higher volume of data on users even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to unintentionally violate.[6] A recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. 59% also say that tech companies bear the responsibility while 46% believe the government does. The study also highlights why it is important to consider the tradeoffs associated with age verification and consent proposals that would require the additional collection data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[7]

Further, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population, and; 3) respecting the protection of individuals' data, privacy, and security.[8] Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

Colorado should not impede continuing efforts by private businesses to moderate content on their services, including through the use of algorithms.

Just as digital services do not serve all users, they do not publish all content. In addition to prohibiting illegal content as required by relevant state and federal laws, many digital services remove content that is

[5] Cristiano Lima, *Utah's porn crackdown has a VPN problem*, The Washington Post (May 5, 2023), https://www.washingtonpost.com/politics/2023/05/05/utahs-porn-crackdown-has-vpn-problem/.
[6] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[7] Colleen McClain, *How americans view data privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[8] *Online age verification: balancing privacy and the protection of minors,* CNIL, (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

dangerous, though not inherently illegal. This includes, for example, content that exhorts users to self-harm or encourages young people to engage in dangerous or destructive behavior.

Specifically, this bill requires all platforms to state that "the use of the social media platform for the promotion, sale, or advertisement of any illicit substance" is prohibited and that users who violate this rule must be removed. However, under the definition of an "illicit substance," legal prescription drugs like anti-anxiety medications and cough syrup would be captured. This definition would make it unlawful for businesses to promote them for sale or even for users to mention their benefits online.[9]

Setting aside the matter of whether the government should impose upon private companies the obligation to host or take down lawful speech, which raises First Amendment concerns, digital services are already taking aggressive steps to moderate and remove dangerous and illegal content consistent with their terms of service. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review. In 2021, a number of online businesses announced that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices to ensure a safer and more trustworthy internet, and have recently reported on the continuing efforts to implement and strengthen these commitments.[10]

As U.S. federal law limits the liability of both digital service providers and their users with regard to content created by third parties, this is a subject of ongoing federal attention. Recently, the U.S. Supreme Court declined to recommend any changes to a key tenet of U.S. Internet law in *Gonzalez v. Google*,[11] in which the Court was considering issues related to content moderation and organization methods, including through the use of algorithms. Additionally, *NetChoice & CCIA v. Moody*[12] and *NetChoice & CCIA v. Paxton*[13] are both cases this term in which the Supreme Court will examine how digital service providers may display third-party content. CCIA recommends taking on board the results of relevant legal proceedings so legislators can act with fuller knowledge of the constitutional boundaries. Otherwise, any potential statute may be at greater risk of protracted, expensive litigation.

This legislation may halt services for individuals under 18, hindering teenagers' internet access and, consequently, restricting their First Amendment right to information. This includes access to supportive online communities that might not be available in their physical location.

The Children's Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright line that was a result of a lengthy negotiation process that accounted for the rights of all users, including children, while also considering the compliance burden on businesses. To avoid collecting data from users under 13, some businesses chose to shut down various services when COPPA went into effect due to regulatory complexity — it became easier to simply not serve

[9] Shoshana Weissmann, *Colorado bill would ban users from talking about marijuana and medication, compromise law enforcement investigations, and stop people from knowing when they're being investigated,* R Street (March 12, 2024), https://www.rstreet.org/commentary/colorado-bill-would-ban-users-from-talking-about-marijuana-and-medication-compromise-law-enforcement-investigations-and-stop-people-from-knowing-when-theyre-being-investigated/.
[10] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.
[11] Trevor Wagener, *A Ruling Against Google in Gonzalez Could Create a "World of Lawsuits" and "Economic Dislocation,"* Disruptive Competition Project (Feb. 27, 2023), https://www.project-disco.org/competition/gonzalez-v-google-could-create-a-world-of-lawsuits-and-economic-dislocation/.
[12] *NetChoice & CCIA v. Moody*, https://ccianet.org/litigation/netchoice-ccia-v-moody/.
[13] *NetChoice & CCIA v. Paxton*, https://ccianet.org/litigation/netchoice-ccia-v-paxton/.

this population. Users between 14 and 17 could face a similar fate as SB 24-158 would implement more complex vetting requirements tied to age verification for all users in order to verify if they are a "juvenile."

When businesses are required to deny access to social networking sites or other online resources, this may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, in instances where children may be in unsafe households, this could create an impediment for children seeking communities of support or resources to get help.

The hyperconnected nature of social media has led many to allege that online services may be negatively impacting teenagers' mental health. However, some researchers argue that this theory is not well supported by existing evidence and repeats a "moral panic" argument frequently associated with new technologies and new modes of communication. Instead, social media effects are nuanced,[14] small at best, reciprocal over time, and gender-specific. Additionally, a study conducted by researchers from Columbia University, the University of Rochester, the University of Oxford, and the University of Cambridge found that there is no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[15] Particularly, the study shows that depression's relation to both TV and social media use was practically zero. The researchers also acknowledged that it is possible, for example, that as a given technology becomes adopted by most individuals in a group, even individuals who do not use that technology could become indirectly affected by it, either through its impacts on peers or by them being deprived of a novel communication platform in which social life now takes place.

Age verification requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[16] After 25 years, age authentication still remains a vexing technical and social challenge.[17] California, Ohio, and Arkansas recently enacted legislation that would implement online parental consent and age verification requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put all three laws on hold until these challenges can be fully reviewed. The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[18] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers.

[14] Amy Orben *et al.*, *Social Media's enduring effect on adolescent life satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[15] Amy Orben, Andrew K. Przybylski, Matti Vuorre, *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.
[16] *Reno v. ACLU*, 521 U.S. 844 (1997).
[17] Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[18] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).

The proposed regulations would impose duplicative responsibilities on businesses without tangible consumer benefits.

SB 24-158 would require companies to compile and submit annual reports about their designs and features, including content moderation practices. Many online platforms already voluntarily and regularly generate detailed transparency reports and make them publicly available on their websites. Doing so is in fact an evolving industry practice: since its launch, DTSP has quickly developed and executed initial assessments of how its member companies are implementing the DTSP Best Practices Framework, which provides a roadmap to meaningfully increase trust and safety online. This roadmap includes several commitments to transparency and content moderation disclosures, in addition to others, to which DTSP members are expected to adhere.[19]

Further, SB 24-158 does not detail who within the Attorney General's Office would have access to these required reports. The designs, algorithms, and features that would be required to be disclosed under this bill are considered proprietary information, containing trade secrets and other kinds of intellectual property. Without a further definition of who would be receiving these reports and how they would be maintained, provisions may be both overly prescriptive and counterproductive to the legislation's intended goals — rather than protecting children from harmful content, they might have the unintended adverse consequence of giving nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services' safety mechanisms. CCIA recommends narrowing the type of information requested in the reports and to whom this information is shared to allow businesses to be more candid, avoid overburdening regulators and businesses, and protect potentially sensitive information.

As currently defined under Section 6-1-1602, covered entities would be required to disclose internal content moderation practices. Without a further definition of "published policies," the provisions may be both overly prescriptive and counterproductive to the legislation's intended goals — rather than protecting consumers from harmful content, they might have the adverse unintended consequence of giving nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services' policies.

Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

Existing U.S. law provides websites and online businesses with legal and regulatory certainty that they will not be held liable for third-party content and conduct. By limiting the liability of digital services for misconduct by third-party users, U.S. law has created a robust internet ecosystem where commerce, innovation, and free expression thrive — all while enabling providers to take creative and aggressive steps to fight online abuse. Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers.[20]

Additionally, research suggests that aggressive regulations, bills, and enforcement actions targeting tech would increase operating costs for regulated U.S. companies, reducing their market value and harming their

[19] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* at 37 (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources).

[20] *More than just a number: How determining user age impacts startups*, Engine (February 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.

shareholders. State and local government employee pension plans are leading shareholders in companies that would be targeted by such anti-tech policies, jeopardizing the retirement benefits of 27.9 million pension plan members nationwide, including teachers, firefighters, nurses, and police.[21]

* * * * *

While we share the concerns of the sponsor and the Senate Committee on Business, Labor, and Technology regarding the safety of young people online, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association

[21] *The cost of tech regulatory bills to state and local pension plans – state by state aggregates*, CCIA Research Center (Nov. 1, 2022), https://research.ccianet.org/stats/cost-of-tech-regulation-bills-state-map/.

Testimony for the Colorado Senate Business, Labor, and Technology Committee by Aliya Bhatia, Policy Analyst at the Center for Democracy & Technology's Free Expression Project

March 19, 2024

Madam Chair, Mr Vice Chair, and members of the committee. My name is Aliya Bhatia and I work at the Center for Democracy & Technology, a nonprofit, nonpartisan organization established in 1994 to advance civil rights and civil liberties online[1].

I thank you for the opportunity to speak to you today about one of several significant concerns we have with SB 158. While protecting children's safety online is a laudable goal, this bill is likely to do the opposite. By requiring social media companies to collect more data on users to verify their ages, this bill puts children and all other internet users' privacy at risk and creates barriers for all internet users' ability to access information online.

Currently, many of the online services covered by this bill may ask for your date of birth when you create an account. But this bill will require social media services to go a step beyond that and "use a commercially reasonable method to verify" age. Available methods may include collecting proof of ID like driver's licenses, machine learning methods like facial scanning or voice pattern analysis, or signal analysis like using search terms or a user's friends to estimate a user's age.[2] Each of these methods raises significant equity, free expression, and privacy concerns.

Age verification methods can impact specific communities differently. Young children often don't have ID or do not have access to their own since in most cases parents or guardians hold onto minors' credentials. Thus, for any company that uses an ID-based age verification method, this requirement will become akin to a parental consent law even for teenagers who have a reasonable need to access information online privately. Colorado has been a leader in ID-inclusivity but even the best systems have gaps.[3] Immigrants, individuals who have transitioned but not changed their IDs, and many others may have outdated or limited access to IDs.

Social media companies that instead rely on machine learning methods to estimate a user's age based on their facial features, voice patterns or other proxy signals for age such as search queries will fare no better. These methods are more likely to be error prone for people with disabilities, people of color, and non-binary people and may incorrectly assign an adult user of color or non-binary adult as a child user, limiting their ability to use online services freely. Even if

---

[1] Learn more about the Center for Democracy & Technology at cdt.org.
[2] Scott Brennan and Matt Perault, "Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?", The Center for Growth & Opportunity at Utah State University, June 2023.
[3] "Colorado Legal Services sees uptick in number of Coloradans seeking help to obtain IDs", Colorado Legal Services, August 2023.

online services create a backstop by requiring those users who appeal an age decision a machine learning system makes to provide proof of ID, that will further download greater risks to privacy onto an already marginalized group.

Mandating the use of age verification technologies will bake these inequities into law and result in limiting users' access to information online. Those services that require users to provide proof of ID to verify age will limit users' ability to access sensitive information anonymously. 1609(1) of SB24-158 requires social media companies to preserve data and metadata associated with the user's identities and activities online for at least one year and share it with law enforcement upon request.[4] This is likely to chill users' ability to express themselves and access information freely. Individuals looking for resources from Alcoholics Anonymous or information related to LGBTQ+ identity, domestic violence, or reproductive healthcare are unlikely to want to show ID before accessing this content.[5] Having their online identity be traced could potentially put all users in harm's way, particularly children who have unsupportive parents or those facing abuse.

Age verification processes will require all online services to collect, process, and temporarily preserve even more sensitive user data than they already do. Adding to the trove of user data an online service already processes will put users' privacy at risk should the online service face a security breach by malicious actors.[6]

I thank you for the opportunity to speak today in front of the Senate committee and I am happy to answer any questions from the Chair and members.

---

[4] Colorado Senate Bill 24-158 "Social Media Protect Juveniles Disclosure Reports" introduced in the Senate Business, Labor, and Technology Committee.

[5] Shoshana Weissman, "Age-verification methods, in their current forms, threaten our First Amendment right to anonymity", R Street Institute, June 2023.

[6] Emma Roth, Online age verification is coming, and privacy is on the chopping block, The Verge, May 2023.

Thank you Madame chair and committee members. I'm Anaya Robinson, Senior Policy Strategist with the ACLU of Colorado, in an amend position to SB24-158. We absolutely understand the intent of this bill. We simply have some concerns with some areas of the language in the introduced version of the bill. We want to ensure that the threading of the needle that DA Daugherty spoke of is actualized in both protecting youth, and protecting the constitutional rights of the millions of both youth and adults who are not engaging in illegal activity or unprotected speech on these platforms.

- Age verification requirements burden all users in a virtual environment, and there are many reasons someone might not want to verify their age, which often requires verifying their identity, to a social media company because of immigration status, inaccurate gender markers, or interest in protected anonymous speech. Those reasons shouldn't preclude people from participating in the vast amount of first amendment protected activity that occurs online.
- The numerous exceptions to the definition of "social media company" might make the law underinclusive to address whatever the state's interest in 'protecting children' is, while at the same time the law is overinclusive for burdening all users with the age verification requirements.
- Law enforcement needs to get a warrant (or at least comply with the Stored Communications Act) to get data from the companies (6-1-1609(2) seems to require fulfilling "any inquiry" from a LEA within 30 days and (3) forbids notice to the user even in cases where a warrant was not provided)
- Parental control & surveillance requirements infringe on minors' First Amendment rights arguably supported by Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 790 (2011), which struck down a law prohibiting the sale of violent video games to minors and distinguished between enforcing parental authority over children and imposing governmental authority subject to parental veto

We've been in conversations with the proponents of the bill and are optimistic that forthcoming amendments will address many of our areas of concern and look forward to continued conversations as the bill moves forward. Thank you.