



March 18, 2024

House Consumer Protection, Technology & Utilities Committee
Capitol Building
501 North Third St.
Harrisburg, PA 17120

RE: HB 2017- "An Act amending Title 50 (Mental Health) of the Pennsylvania Consolidated Statutes, providing for protection of minors on social media; and imposing penalties." (Oppose)

Dear Chair Matzie and Members of the House Consumer Protection, Technology & Utilities Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 2017 in advance of the House Consumer Protection, Technology & Utilities Committee 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. Acknowledging policymakers' valid concerns about the online privacy of young individuals, it is imperative to prioritize the establishment of a comprehensive data privacy law applicable to all consumers. This law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users.

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.

HB 2017's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

While the bill does not directly mandate age verification for minors, online businesses must adhere to provisions concerning minor users, which would likely require employing age verification methods to confirm their status. Among a host of reasons why age verification online is problematic, 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.

More broadly, the bill's inexplicit 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 parental 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.

This legislation may halt services for individuals under 16, 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

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>.

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 this population. Users between 14 and 15 could face a similar fate as HB 2017 would implement more complex vetting requirements tied to parental consent for users under 16.

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.

Serious concerns also arise when verifying whether a “parent or guardian,” undefined in the bill, is in fact a minor’s legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. If there is no authentication that a “parent or guardian” is actually a minor’s legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian to verify their age on behalf of the minor to register for an account with a “social media platform.” It is also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in Pennsylvania or is not a resident of the state creates significant confusion for consumers and businesses.

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,⁹ 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.¹⁰ 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 and parental consent 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.¹¹ After 25 years, age authentication still remains a vexing technical and social challenge.¹² California, Ohio, and Arkansas recently enacted legislation that would implement online parental consent and age verification requirements — each law is currently facing a legal

⁹ 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>.

¹⁰ 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>.

¹¹ *Reno v. ACLU*, 521 U.S. 844 (1997).

¹² 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>.



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.¹³ 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.

Algorithms are instrumental in providing better-tailored online experiences.

Like any product, there are risks and benefits inherent to algorithmic feeds. However, CCIA cautions against pursuing measures that inherently presume only negative impacts. HB 2017 would prohibit a social media platform from using a minor’s personal data in an “algorithmic recommendation system”, however, this may result in a degraded user experience. For example, algorithmic feeds serve content with increased relevance to individual users, prioritizing content that is more likely to be appropriate and of interest. By analyzing past interactions, browsing history, and other factors, algorithms contribute to curating a relevant and personalized experience. While algorithms personalize a user’s experience, they can also help to introduce new topics and interests allowing users to discover creators, ideas, and communities they would not have found otherwise. And, algorithms are able to do this efficiently — with vast amounts of content available, algorithms help users navigate information overload by prioritizing content and allowing users to find what they’re looking for faster and with less effort.

Algorithms can also be used to encourage more positive experiences online, including through the use of tools to identify and report inappropriate content such as CSAM or guiding users to helpful resources if they search for material related to self harm, suicide, or depression.

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.¹⁴

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 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.¹⁵

Under § 1131, HB 2017 includes several provisions related to data privacy for “minor” users. CCIA strongly

¹³ *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).

¹⁴ *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>.

¹⁵ *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/>.



supports the protection of consumer data and understands that Pennsylvania residents are rightfully concerned about the proper safeguarding of their data. CCIA encourages lawmakers to strike the appropriate balance for meaningful protections while preserving the benefits consumers receive and the ability for innovation to thrive. As you know, in the absence of a comprehensive law at the federal level, there is a growing number of states that have enacted their own laws. The majority of these laws harmonize a key set of definitions and concepts related to privacy. In lieu of the several provisions included under § 1131, CCIA would encourage lawmakers to refer to the comprehensive frameworks established for *all* users, including younger users, under laws in states such as Connecticut and Virginia, as these provide covered businesses with clear roadmaps for compliance and consumers with clearly defined rights.

* * * * *

While we share the concerns of the sponsor and the House Consumer Protection, Technology & Utilities Committee 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