STATE OF UTAH
BEFORE THE UTAH DEPARTMENT OF COMMERCE DIVISION OF CONSUMER PROTECTION

In the Matter related to the Utah Minor Protection in Social Media Act Rule

Comments of the R Street Institute

The R Street Institute (R Street) is a nonprofit, nonpartisan public policy research organization headquartered in Washington, D.C. with multiple offices across the United States. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government. R Street submits these reply comments in response to the Notice of Comment Period issued by the Utah Department of Commerce on Aug. 15, 2024. R Street appreciates the Department encouraging the public to submit comments on the proposed rule.

Introduction

R Street has documented extensive concerns with the concept, execution, and constitutionality of age verification as a barrier for access to free speech on social media. The following comments detail our concerns with age assurance, parental consent, cybersecurity implications, First Amendment concerns, Utah residency verification, and cost.

Although both the authors of the law and the Department of Commerce revised the previous law and regulations in a way that attempts to be more privacy-protecting, fundamental complications of age assurance and parental consent bring back all the same the issues of age and identity verification. Therefore, many of R Street's previously stated concerns regarding the initial version of this law and pursuant regulations remain relevant here.

Problems with Age Assurance Methods

The proposed rule lists "Processes and Means of Age Assurance," which qualify social media companies for the originating bill's safe harbor. According to the rule, the age assurance method must be no more than 1 percent inaccurate with regard to liveness detection of the person verifying age, no more than a 3 percent false positive rate (the rate at which the age assurance system incorrectly determines an account holder is not a minor), no more than a 10 percent false negative rate (the rate at which the age assurance system incorrectly determines an account holder is a minor), 95 percent accuracy within upper and lower limit, and 1 percent outcome error parity maximum disparity. The age assurance system's results also must be "verified annually by an independent third-party auditor." Finally, the social media company must allow users to challenge an incorrect result.

Unfortunately, age assurance methods may fail when they matter most for the purposes of laws and regulations like these. A recent National Institute of Standards and Technology study of a variety of age assurance providers demonstrates that assurance algorithms usually estimate age incorrectly by a minimum of two years.[1] Further, the best algorithm estimated that about 30 percent of the images of 17-

[1] Kayee Hanaoka et al., "Face Analysis Technology Evaluation: Age Estimation and Verification," National Institute of Standards and Technology, Fig. 7, May 2024. https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf.

year-olds it was shown were above 18 years of age, with the next best estimating about 50 percent of 17-year-olds were at least 18 years of age.[2] Additionally, the best of the tested algorithms was only able to successfully estimate that a 17-year-old was within one year of age 17 30 percent of the time, with a mean average error of 2.7 years.[3]

If the relevant task were approximating a user's age within a few years, these algorithms would potentially satisfy the need. However, the relevant task is sorting minors from legal adults. And an added or subtracted few years makes a world of difference in this task when a user is in their mid-teens to early 20s.

Both the law and the regulations account for some error; unfortunately, they do not specifically outline how users must be able to counter the age estimation. Adults incorrectly determined to be minors will have to prove to platforms that they are, in fact, adults and can use social media more freely. If age estimation fails them, the best way to do this is to provide extremely sensitive information, such as their government identification, Social Security numbers, and the like.[4] With an allowed maximum 10 percent false negative rate, this could become somewhat of a norm for adults in Utah—implicating all the same problems with the previous law.

Problems with Parental Consent Methods

The Utah Minor Protection in Social Media Act requires that guardians have some oversight of minors' social media account settings. The pursuant rule requires that social media companies take into account the available technology to confirm the child-guardian relationship and "make reasonable efforts to confirm a parent's or guardian's consent for a minor to change data privacy settings in accordance with Section 13-71-202, or to overcome the presumption of confidentiality described by Subsection 13-71-204(2)." This rule allows social media companies to use "a method that complies with 16 CFR 312.5(b)(2) or (3), or has been approved by the Federal Trade Commission in accordance with 16 CFR 312.12(a)."

Regulations 16 CFR 312.5(b)(2) and (3) include a list of possible methods including a signed consent form from the parent, an online monetary transaction (such as through a credit card) from the parent, "[a] call [to] a toll-free telephone number staffed by trained personnel" or contact with representatives via video call, verification of the parent's government identification, or an email process with additional steps.[5] Meanwhile, 16 CFR 312.12(a) allows companies to file paperwork with the Federal Trade Commission to seek approval of other methods—which is undoubtedly extremely burdensome.[6]

Unfortunately, the method that is most likely to be accurate and to cause less of a regulatory headache is identity verification. Age verification is meaningless in this context, because an older sibling or older friend could otherwise help a minor evade the law's requirements here. The only way the law has force in

---

[2] Ibid, Fig. 9.
[3] Ibid, Tables 19 and 20.
[4] Shoshana Weissmann, "The technology to verify your age without violating your privacy does not exist," R Street Institute, May 16, 2023. https://www.rstreet.org/commentary/the-technology-to-verify-your-age-without-violating-your-privacy-does-not-exist.
[5] 16 CFR 312.5(b)(2) and (3).
[6] 16 CFR 312.12(a).

this regard is when platforms confirm each specific child-guardian relationship. There is no way to do this without identity verification, which is inherently invasive.

Cybersecurity Implications

To begin, scammers are now tricking people into providing face scans and using them to access people's accounts.[7] It is entirely predictable that what becomes the key to age and identity assurance and verification will become a target for hackers and scammers. The idea of using a live view of one's self may appear less risky than uploading sensitive government identification. But the core problem is that the more valuable any form of identification becomes for bad actors, the more those bad actors will seek it out. The practice of regularly using age assurance methods will mean that it is easier for bad actors to trick people into providing these face scans.

Additionally, although the proposed rule provides extensive requirements for data storage and deletion related to age assurance (and possible pursuant verification when the initial estimation is wrong), companies are hacked all the time. As R Street wrote last year:

> One survey conducted in 2023 by a major research university found that hacks designed to "steal, change or make public important data" had successfully been carried out on more than 80 percent of U.S. companies.[8] Additionally, between early 2020 and early 2021, cybercrime that involved ransomware rose 102 percent globally.[9] And more data and studies show the same kind of problem.[10]

Companies involved in age verification have already failed to protect user data, and it is always a risk that this will happen. In June, *404 Media* reported that AU10TIX—used by the largest social media companies—"exposed a set of [employee] administrative credentials online for more than a year," where bad actors could access users' "name, date of birth, nationality, identification number, and the type of document uploaded such as a drivers' license."[11]

Herein lies the wisdom in the principle of data minimization. If sensitive information is not collected in the first place, users do not have to worry about it being leaked later.[12] On the other hand, laws and regulations that force aggressive sensitive data collection will leave users more vulnerable than before.

---

[7] Mike Masnick, "As Predicted: Scammers Are Now Scanning Faces To Defeat Biometric Security Measures," *TechDirt*, Feb. 27, 2024. https://www.techdirt.com/2024/02/27/as-predicted-scammers-are-now-scanning-faces-to-defeat-biometric-security-measures.

[8] "New CFO Survey: More Than 80 Percent of Firms Say They've Been Hacked," Duke CFO Global Business Outlook, last accessed Jan. 24, 2024. https://today.duke.edu/2015/06/cfohacking.

[9] Check Point Research Team, "The New Ransomware Threat: Triple Extortion," Check Point Solutions, May 12, 2021. https://blog.checkpoint.com/security/the-new-ransomware-threat-triple-extortion.

[10] Shoshana Weissmann, "If platforms are required to have your government IDs and face scans, hackers and enemy governments can access them too," R Street Institute, May 22, 2023. https://www.rstreet.org/commentary/if-platforms-are-required-to-have-your-government-ids-and-face-scans-hackers-and-enemy-governments-can-access-them-too; Shoshana Weissmann, "Comments on Proposed Rules for the Utah Social Media Regulation Act, R Street Institute, Jan. 31, 2024. https://www.rstreet.org/outreach/comments-on-proposed-rules-for-the-utah-social-media-regulation-act.

[11] Joseph Cox, "ID Verification Service for TikTok, Uber, X Exposed Driver Licenses," *404 Media*, June 26, 2024. https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix.

[12] Shoshana Weissmann, "Age-verification legislation discourages data minimization, even when legislators don't intend that," R Street Institute, May 24, 2023. https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that.

First Amendment Concerns

Under this law, if one scans their face in order to access and engage in speech online, in cases where an adult is wrongly determined to be a minor and has to prove otherwise or where a child and a guardian must prove their relationship (and, necessarily, their identities), real anonymity online is lost and barriers to speech enacted. The First Amendment is implicated in all of these cases, because they are requirements of law. As we wrote in previous comments:

> The Supreme Court has long recognized the First Amendment right to free, anonymous speech.[13] This right applies to online speech, such as that on message boards, as well.[14] As Justice Clarence Thomas wrote in concurrence on a 1995 case, "[a]fter reviewing the weight of the historical evidence, it seems that the Framers understood the First Amendment to protect an author's right to express his thoughts on political candidates or issues in an anonymous fashion."[15] Age-verification methods that force users to provide their most sensitive, identifying information to access platforms containing constitutionally protected speech infringes on this right. In fact, not only is most speech on social media platforms protected by the First Amendment, but the Supreme Court also recognizes that children have First Amendment rights, too.[16]
>
> Additionally, if this proposed rule were to be put in place, many users would have valid concerns about their anonymous profiles being tied to their actual identities. Even if social media companies were to perfectly protect and dissociate age-verification data from user profiles, just the concern that anonymity might be compromised could cause these regulations to run afoul of the First Amendment and chill speech. And the "chilling effect"—when people self-censor or "chill" their speech—can cause laws to be ruled unconstitutional.[17] For example, anyone who wishes to share an unpopular opinion or discuss a sensitive issue like chronic disease or divorce may think twice before voicing their opinion if they fear they might be identified.[18]
>
> Another First Amendment concern is that of under-inclusivity.[19] For example, in *Brown v. Entertainment Merchants Association*, the late Justice Antonin Scalia wrote the majority opinion in which he explained that a law restricting minor access to violent video games but not violent movies, books, or other media was improperly tailored.[20] This proposed rule faces the same issue of under-inclusivity by restricting minor access to one type of media, but not others, as well as by both restricting access to some social media platforms but not others and exempting some affinity social media platforms but not others. In that majority opinion, Scalia also referenced the issue of over-inclusivity when he explained that if a minor's guardians are not concerned about their children's access to violent video games, restricting access to such games for

---

[13] Jeff Kosseff, *The United States of Anonymous: How the First Amendment Shaped Online Speech* (Cornell University Press, 2022), p. 43. https://www.cornellpress.cornell.edu/book/9781501762383/the-united-states-of-anonymous; Shoshana Weissmann, "Age-verification methods, in their current forms, threaten our First Amendment right to anonymity, R Street Institute, June 1, 2023. https://www.rstreet.org/commentary/age-verification-methods-in-their-current-forms-threaten-our-first-amendment-right-to-anonymity.

[14] Weissmann, supra note 13.

[15] *McIntyre v. Ohio Elections Commission* (93-986), 514 U.S. 334 (1995).

[16] *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969).

[17] Frank Askin, "Chilling Effect," The Free Speech Center at Middle Tennessee State University, last updated July 2, 2024. https://firstamendment.mtsu.edu/article/chilling-effect; Weissmann, supra note 10.

[18] Shoshana Weissmann, "Current age-verification methods threaten our First Amendment rights beyond anonymity, R Street Institute, June 22, 2023. https://www.rstreet.org/commentary/current-age-verification-methods-threaten-our-first-amendment-rights-beyond-anonymity.

[19] Ibid.

[20] *Brown, et al. v. Entertainment Merchants Assn. et al.,* 564 U.S. 786 (2011).

those minors was a violation of their First Amendment rights. For these reasons and more, he explained why that law could not "survive strict scrutiny."[21] The same issues exist with Utah's proposed age-based social media regulations.

Website traffic is another issue that combines First Amendment issues with website feasibility issues. In a case affirming a permanent injunction that stopped the enforcement of the Child Online Protection Act (COPA), the Third Circuit recognized that age verification would result in decreased traffic to certain websites. The court wrote that such age-verification requirements "present their own First Amendment concerns by imposing undue burdens on Web publishers due to the high costs of implementing age-verification technologies and the loss of traffic that would result from the use of these technologies."[22]

First Amendment jurisprudence holds the government to a high standard. To overcome scrutiny, the government must use the least-restrictive means of regulation to accomplish its constitutional goal. Two decades ago, Justice Anthony Kennedy wrote the majority opinion in *Ashcroft v. ACLU*—where the Court found COPA unconstitutional—explaining that filtering software, which is available to parents, would not only accomplish the age-restriction goal but would do so more effectively than the government could.[23] An added benefit of using parental control over government regulations is that the government would not have to infringe on any speech. The same holds true today and with this proposed rule: Parental filters are widely used and would address this issue more effectively than Utah government regulation.[24] In fact, many platforms already offer parental controls.

Thus, decades-old federal laws focused on verifying user age have been overturned by the courts and reduced in scope for all of these reasons and more.[25]

Verifying Utah Residency

As R Street previously noted, the rule applies only to Utah account holders, defined as "a person who is a Utah resident and an account holder." However, there is no guidance for platforms regarding how to differentiate residents and non-residents of Utah.

R Street wrote in 2023:

> [W]hile the new proposed rule would apply to all residents of Utah, it fails to explain how platforms would identify whether someone is a resident of the state or not. Whether a user legally resides in another state and is accessing social media in Utah or if a Utah resident is using a [virtual private network] that changes their virtual location, it might sometimes be impossible to know if a social media user is located in Utah, let alone a resident, and if they are subject to the age-verification process at all.[26]

Cost and Burden on Small Platforms

---

[21] Ibid.
[22] *American Civil v. Mukasey*, 534 F.3d 181 (3d Cir. 2008).
[23] *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004), 322 F.3d 240, affirmed and remanded, Supreme Court of the United States, No. 03-218. https://www.supremecourt.gov/pdfs/transcripts/2003/03-218.pdf.
[24] Weissmann, supra note 15.
[25] Ibid.; Weissmann, supra note 10.
[26] Shoshana Weissmann and Canyon Brimhall, "Age-verification laws don't exempt VPN traffic. But that traffic can't always be detected.," R Street Institute, Aug. 29, 2023. https://www.rstreet.org/commentary/age-verification-laws-dont-exempt-vpn-traffic-but-that-traffic-cant-always-be-detected; Weissmann, supra note 10.

The rule reports an estimated cost per completed age assurance attempt or parental consent verification of $0.05 to $0.45. Notably, the law and regulation cover all kinds and sizes of social media companies. Consider AllTrails, which has more than 65 million users worldwide.[27] Utah is a frequent hiking destination, and more than 5 million people hike in Zion National Park annually.[28] Zion is one of a handful of national parks in Utah, which is to say nothing of all the national forests. Because AllTrails does not release the number of Utah-based people on its app, using the count of Zion National Park visitors and not the number of hikers across the state is a far next-best, ham-handed estimate. If just the 5 million Zion National Park visitors are required to complete age assurance on AllTrails, that will cost the company as much as $2,250,000—not counting other possible contract costs with assurance providers. One estimate puts AllTrails' annual revenue at $40.4 million.[29] The American Cancer Society's Cancer Survivors Network also has millions of users.[30] Larger businesses can afford the cost far more easily than smaller or affinity platforms like AllTrails and the Cancer Survivors Network that are also covered by this law.

Conclusion

The R Street Institute thanks the Utah Department of Commerce for the opportunity to submit these comments.

Respectfully submitted,

___/s Shoshana Weissmann____

Shoshana Weissmann
Digital Director and Resident Fellow

The R Street Institute
1411 K Street NW, Suite 900
Washington, D.C. 20005
(202) 525-5717
sweissmann@rstreet.org
Sept. 16, 2024

---

[27] "Helping people across the globe get outside," AllTrails, last accessed Sept. 4, 2024. https://www.alltrails.com/press?section=press-page-about.

[28] "By the numbers in Zion National Park," National Park Service, last updated Aug. 14, 2024. https://www.nps.gov/zion/learn/management/park-visitation-statistics.htm.

[29] "AllTrails Revenue and Competitors," Growjo, last accessed Sept. 4, 2024. https://growjo.com/company/AllTrails.

[30] "Cancer Survivors Network," American Cancer Society, last accessed Sept. 4, 2024. https://csn.cancer.org; Kevin Babb, "The American Cancer Society's Cancer Survivors Network®," International Cancer Information Service Group, last accessed Sept. 4, 2024. https://icisg.org/resources/best-practices-monthly-feature/2018-2/the-american-cancer-societys-cancer-survivors-network.