TECHFREEDOM
LAW FOR A DYNAMIC FUTURE

Comments of

TechFreedom

Berin Szóka[i]

In the Matter of

Children's Online Privacy Protection Rule Proposed Parental Consent Method;

Application of the ESRB Group for Approval of Parental Consent Method

FTC 2023-15415

August 21, 2023

---

[i] Berin Szóka is President of TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at bszoka@techfreedom.org.

INTRODUCTION

If the Commission approves this application, it should issue an accompanying statement explaining what Privacy-Protective Facial Age Estimation[1] (a/k/a "Facial Age Estimation" or "FAE") does and does not do. While FAE may be adequate to provide the age *assurance* contemplated by the Children's Online Privacy Protection Act ("COPPA"), it falls very far from providing the certainty necessary for age *verification* of older teens, such as would be necessary under legislation that has been proposed to expand or build upon COPPA.

Age verification has been a key focus of debates over Internet regulation since 1996; it remains a persistent source of confusion. The Commission should clarify the difference between age assurance and age verification. Otherwise, the lawmakers and public may misunderstand approval of this application as an endorsement of FAE as a reliable method of age verification, which it plainly is not. Such a clarification would be consistent with President Woodrow Wilson's vision for the FTC as a "clearing house for the facts by which both the public mind and the managers of great business undertakings should be guided."[2]

I. FAE Appears to Be No Less "Reasonable" a VPC Method Than Others Already Approved by the Commission

The existing COPPA rule plainly does not cover FAE as a recognized means by which parents may authorize their children to use online services.[3] Yet the COPPA statute gives the Commission significant discretion to recognize new Verifiable Parental Consent (VPC) methods: "any reasonable effort (taking into consideration available technology) . . . to ensure that a parent . . . authorizes" their use of the service will suffice.[4] Accordingly, the

---

[1] "The Commission does not approve one party's specific implementation of a VPC method or a proprietary system under the relevant provision of the Rule." Press Release, Fed. Trade Comm'n, Imperium, LLC Proposed Verifiable Parental Consent Method Application (Dec. 23, 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf.

[2] *See* Address by President Woodrow Wilson before a Joint Session of Congress on Additional Legislation for the Control of Trusts and Monopolies, Jan. 20, 1914, *reprinted at* 51 Cong. Rec. 1962-64, 1978-79 (1914), https://www.congress.gov/bound-congressional-record/1914/01/20/senate-section.

[3] 16 C.F.R. § 312.5(b)(2) (2023).

[4] 15 U.S.C. § 6501(9) ("The term 'verifiable parental consent' means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.").

COPPA rule requires only that a method be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[5]

FAE does that at least as well as other VPC methods recognized as adequate by the Commission. FAE may well prove more convenient for users than other VPC mechanisms.[6] The most notable difference between Privacy-Protective FAE and previously recognized VPC methods is that, by design, it involves no record of the parent's identity. This is more privacy-protective than requiring parents to turn over potentially sensitive information, such as government IDs, and significantly more protective than having humans match facial scans to government IDs.[7]

But this privacy protection has a downside: because the identity of a parent cannot be verified, it is also impossible to "verify" the parent-child relationship. This should not stop the Commission from approving the application: the Commission has previously decided that VPC methods need not verify the parent-child relationship.[8] It is enough that, like other VPC methods, FAE "provides a very high level of assurance that the person providing the consent is old enough to be a parent."[9]

Yet some users may not trust the privacy protections built into Privacy-Protective FAE. After all, in analyzing faces, FAE does create new, potentially identifying information about users. And it may *seem* more intrusive. Many users may reasonably worry: Will such information be used only for the purpose of VPC? Will it be deleted immediately after that use? Or can it be used to identify their faces in other contexts? Such concerns may lead some parents to refuse to use FAE. This, in turn, could limit their children's enjoyment of digital services. To

---

[5] 16 C.F.R. § 312.5(b)(1) (2023).

[6] *See* Letter from Yoti Ltd. et al. to April J. Tabor, FTC Secretary at 35-38 (June 2, 2023) [hereinafter Yoti Application], https://www.regulations.gov/document/FTC-2023-0044-0002 (APPENDIX D: The Benefits of Facial Age Estimation in Terms of Parent Access and).

[7] *See, e.g.*, Letter from Donald S. Clark, FTC Secretary, to Riyo (Nov. 18, 2015), https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf

[8] *Id.* at 4 ("CDD argues that children can easily circumvent the system because the FMVPI system authenticates the identity of the holder, not the parent-child relationship. However, the Commission addressed this concern in the 2013 Statement of Basis and Purpose for the Rule in deciding to include government-issued IDs as an enumerated VPC method."); Children's Online Privacy Protection Rule, 16 C.F.R. 312 n.208 (2023), https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule#footnote-208-p3987 ("this mechanism achieves the delicate balance of making it easy for the parent to provide consent, while making it difficult for the child to pose as the parent"). *See also* Press Release, Fed. Trade Comm'n, Imperium, LLC Proposed Verifiable Parental Consent Method Application (Dec. 23, 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf (Imperium, LLC's approved VPC method also cannot verify the parent-child relationship).

[9] Yoti Application, *supra* note 6, at 8.

avoid such consequences, parents should be given the option of using VPC methods that do not involve face scanning, just as Yoti proposes.[10]

II. FAE Offers Age Assurance, Not Age Verification

While we defer to others as to just how "privacy-protective" FAE really is, TechFreedom has significant experience with the free expression issues raised by online age verification. Given the tumultuous legal history of age verification in the United States, we are confident that approval of this application would be widely misunderstood as validation of FAE as an adequate mechanism for age *verification*.

But assurance is not verification. FAE may be adequate for establishing that a user is reasonably likely to be over the age of 25, but it cannot reliably distinguish, say, 18-year-olds, who may use a service without special conditions, from 17-year-olds, who may not. Indeed, Yoti's proposed system does not even try to predict ages of users under 25: anyone "in the 'buffer' zone of 18-24 . . . will be rejected by the system. . . ."[11] Moreover, the error rates involved in FAE are significant. As the application notes, Yoti incorrectly concludes that significant percentages of adults are under 25: 0.34% for those over age 36 and 1.68% for those 25-36.[12] Doubtless, the error rates involved for predicting whether users are under 18 would be considerably larger.

FAE is a reasonable method of age *assurance—i.e.*, for establishing that someone is likely old enough to be a parent. For most users, it offers a convenient way of clearing the hurdle set by COPPA. Anyone rejected by Yoti's system can always fall back on some other method for providing VPC, such as providing a credit card or government ID. But if a site operator fell back on such methods in attempting to prove a negative—to *verify* that users were *not* minors—these secondary methods would not suffice. Courts have already decided that they are neither sufficiently effective nor sufficiently privacy-protective to achieve a legitimate government interest while protecting anonymous communication. The courts thus have twice struck down age verification mandates as infringements on the First Amendment rights of adults and teens[13] to access content and communicate without having to provide

---

[10] *Id*. at 6 ("Operator informs parent of the requirement to verify they're an adult; offers parent a choice of verification methods.").

[11] *Ibid*.

[12] *Id*. at 30.

[13] Teens have rights to communicate and access information that children under 13 do not. *See* American Civil Liberties Union v. Gonzales, 478 F. Supp. 2d 775, 817-18 (E.D. Pa. 2007) ("COPA defines a minor as 'any person under 17 years of age.' . . . As discussed by the Third Circuit, defining minors as 'any person under 17 years of age,' creates a serious issue with interpretation of COPA since no one could argue that materials that have 'serious literary, artistic, political, or scientific value' for a sixteen-year-old would necessarily have the

information that could identify them.[14] Adding FAE as an additional tool would not change this result for a simple reason: it is not an age verification tool.

These court decisions involved the Communications Decency Act of 1996 (CDA) and the Child Online Protection Act of 1998 (COPA). Both statutes imposed criminal liability for anyone who allows minors to access potentially harmful content—unless courts determined that they had done enough to block minors.[15] The courts found CDA's protection for providers that did so was far too vague to satisfy the First Amendment.[16] In COPA, Congress attempted to mitigate the problem by removing the CDA's "effective" requirement and allowing for additional methods of age-segregating content.[17] This did not save the statute: courts found that the affirmative defense was "effectively unavailable because [the age

---

same value for a three-year old. Likewise, what would be 'patently offensive' to an eight-year-old would logically encompass a broader spectrum of what is available on the Web than what would be considered 'patently offensive' for a sixteen-year-old . . . As the Third Circuit noted, '[i]n abiding by this definition, Web publishers who seek to determine whether their Web sites will run afoul of COPA cannot tell which of these "minors" should be considered in deciding the particular content of their Internet postings.' Thus, the application of the definition of minors to COPA creates vagueness in the statute." (citations omitted) (quoting American Civil Liberties Union v. Ashcroft, 322 F.3d 240, 253-54 (3d Cir. 2003))). *See also Ashcroft*, 322 F.3d at 268 ("[S]ex education materials may have 'serious value' for, and not be 'patently offensive' as to, sixteen-year-olds. The same material, however, might well be considered 'patently offensive' as to, and without 'serious value' for, children aged, say, ten to thirteen, and thus meet COPA's standard for material harmful to minors.").

[14] In striking down COPA for the first time, the Third Circuit noted that age verification "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial." 322 F.3d at 259. In 2008, striking down COPA again for the final time, the Third Circuit reiterated that age verification "would deter users from visiting implicated Web sites" and therefore "would chill protected speech." American Civil v. Mukasey, 534 F.3d 181, 197 (3d Cir. 2008).

[15] *See, e.g.*, Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736, § 231 (codified at 47 U.S.C. § 223(e)(5) (1998)), *invalidated* by American Civil Liberties Union v. Mukasey, 534 F.3d 181 (3d Cir. 2008), cert. denied, 555 U.S. 1137 (2009) (no liability if an operator "has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology").

[16] *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 881–82 (1997) ("It is the requirement that the good-faith action be 'effective' that makes this defense illusory. . . . The Government recognizes that its proposed screening software does not currently exist. . . . Without the impossible knowledge that every guardian in America is screening for the 'tag,' the transmitter could not reasonably rely on its action to be 'effective.' . . . [T]he Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults . . . [and] thus failed to prove that the proffered defense would significantly reduce the heavy burden on adult speech. . . .").

[17] 47 U.S.C. § 231(c) (1998) provided an affirmative defense to defendants who:

> in good faith . . . restricted access by minors to material that is harmful to minors—
> (A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;
> (B) by accepting a digital certificate that verifies age; or
> (C) by any other reasonable measures that are feasible under available technology.

verification methods] do not actually verify age"[18]—*i.e.*, because they provided only some degree of age assurance. Despite technological change, effective age verification remains impossible to do with meaningful precision.[19] Yet lawmakers keep proposing bills that would, in effect, force websites to age-verify users.[20]

To date, COPPA has had negligible effects on adults because it does not require them to identify themselves as a condition of using Internet services.[21] COPPA instead has a modest goal: requiring websites to be reasonably sure that the person providing VPC is an adult. FAE may satisfy COPPA's very modest goal (age assurance for parents), but it is not remotely adequate for age verification as a requirement for adult and teen users to exercise their own First Amendment rights. The Commission should make this clear. For the larger policy debate, this is the critical point: FAE simply cannot do what many lawmakers expect.

For example, the proposed Kids Online Safety Act (KOSA) requires an online operator to apply special protections for those users that it has "actual knowledge or knowledge fairly implied on the basis of objective circumstances" are minors. KOSA purports not to require age verification, but the bill is so vague about how this requirement is to be implemented that sites will have no choice but to implement some kind of age verification technology.[22] The Commission would have to consider the "totality of the circumstances," including, but not limited to, "whether the operator, using available technology, exercised reasonable care."[23] Implementing FAE would not suffice for an operator to guard against liability under KOSA. As noted above, the hard work of drawing a line between minors and adults is, by

---

[18] 534 F.3d at 196. *See also* 322 F.2d at 260 ("[T]he affirmative defenses do not provide the Web publishers with assurances of freedom from prosecution. . . . The Government raises serious constitutional difficulties by seeking to impose on the defendant the burden of proving his speech is not unlawful.") (internal quotation marks and citation omitted).

[19] Letter from TechFreedom to Majority Leader Schumer, Speaker Pelosi, Leader McConnell, and Leader McCarthy at 2-3 (Dec. 6, 2022), https://techfreedom.org/wp-content/uploads/2022/12/Kosa-Letter-December-6-2022.pdf.

[20] *See, e.g.,* Kids Online Safety Act, S. 1409, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2023).

[21] COPPA requires VPC for the "collection, use, or disclosure of personal information from children" when a service has actual knowledge that a user is under 13 years old or when the service is "directed to" children under 13. 16 C.F.R. § 312.5(a)(1) (2013). But services directed to children under 13 are unlikely to be used by anyone other than children due to their limited functionality, effectively mandated by COPPA. Because "collection" includes allowing "[e]nabling a child to make personal information publicly available in identifiable form," 16 C.F.R. § 312.2 (2013), child-directed sites generally offer very limited functionality, preventing users from communicating with each other except in pre-set messaging options. Few adults would use such sites. Moreover, in determining whether a service is "directed to" children, the COPPA rule directs the FTC to consider the subject matter, visual content, presence of child celebrities or celebrities who appeal to children, language, and other indicia. *Id*.

[22] *Id.*

[23] Kids Online Safety Act, S. 1409, 118th Cong. § 14(b) (2023).

design, *not* performed by FAE.[24] Instead, users whom FAE concludes are likely under 25 must fall back on the very same age verification mechanisms rejected as inadequate in litigation over the CDA and COPA.[25] Moreover, it makes little difference to the First Amendment analysis how robust the privacy safeguards built into FAE are if many adults and teens reasonably fear having their faces scanned and thus refuse to do so. If facial scanning became necessary for adults and teens to use online services, privacy-sensitive users would be chilled from exercising their First Amendment rights to anonymous or pseudonymous online expression. Operators of such services would suffer their own, distinct First Amendment injury: losing such users.[26] Courts would understand that, while the technological details may have changed, the essence of the constitutional problem has not.

—

If the Commission decides to approve Yoti's application, it should supplement its approval letter with a statement signed by the full the Commission clarifying that the agency understands FAE provides only age assurance, not age verification, and explaining the difference between these two in a way that both the public and lawmakers can understand.

Respectfully submitted,

_____/s/_____

Berin Szóka
President
TechFreedom
bszoka@techfreedom.org
1500 K Street NW
Floor 2
Washington, DC 20005

Date: August 21, 2023

---

[24] *See supra* notes 11-12 and associated text.

[25] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997) (CDA); Ashcroft v. American Civil Liberties Union. 542 U.S. 656 (2004) (COPA).

[26] American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473, 495 (E.D. Pa. 1999) ("[U]nder COPA, Web site operators and content providers may feel an economic disincentive to engage in communications that are or may be considered to be harmful to minors and thus, may self-censor the content of their sites. Further, the uncontroverted evidence showed that there is no way to restrict the access of minors to harmful materials in chat rooms and discussion groups, which the plaintiffs assert draw traffic to their sites, without screening all users before accessing any content, even that which is not harmful to minors, or editing all content before it is posted to exclude material that is harmful to minors."). *See also Reno*, 521 U.S. at 857.