September 30, 2024

Office of the New York State Attorney General
The Capitol,
Albany, NY 12224-0341

**Re: Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 et seq**

Dear Attorney General James:

I write today on behalf of the Electronic Frontier Foundation (EFF)[1] to respond to the New York State Office of the Attorney General's (OAG) questions in the Advanced Notice of Proposed Rulemaking (ANPRM) to implement the Stop Addictive Feeds Exploitation (SAFE) for Kids Act, dated August 1, 2024 and pursuant to New York General Business Law section 1500 et seq. (GBL section 1500).

Specifically, EFF seeks to respond to question 2 of the ANPRM, which asks:

> *"Currently, age determination can be carried out via a number of methods, including biometric assessment; assessment based on analyzing user activity; government-issued ID; attestation from a reliable third-party business with pre-existing age information, such as a bank via an issued credit card; attestation from other users; self-attestation; and cognitive tests.*
>
> - *How accurate is each of these methods at determining whether a user is under the age of 18?*
> - *What is the risk of falsification for each?*
> - *How much does each cost, and how is cost assessed?*
> - *How do these methods ensure that the privacy of user data is preserved?*
> - *What data do they require to function?*
> - *What are the risks of bias for each of these methods?*
> - *Are these answers potentially different for social media platforms, or for certain kinds of social media platforms? Would it be more or less reliable to have other users attesting for your age in the social media context than in other online contexts?*
> - *Are there other age-determination methods currently available? What are they? How do they compare to those previously listed?*
> - *What age-determination methods are likely to be available in the near future? How do they compare to the methods we have listed?"*

In response, we begin with the assertion that online age-verification mandates like that imposed by the New York SAFE For Kids Act are unconstitutional because they block adults from content they have a First Amendment right to access, burden their First Amendment right to

[1] The Electronic Frontier Foundation is a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including thousands of supporters in California.

browse the internet anonymously, and chill data security- and privacy-minded individuals who are justifiably leery of disclosing intensely personal information to online services. Further, these mandates carry with them broad, inherent burdens on adults' rights to access lawful speech online. These burdens will not and cannot be remedied by new developments in age-verification technology.

**The SAFE for Kids Act's Age-Verification Mandate Impermissibly Blocks Adults From Lawful Speech Online**

Document-based age-verification requirements "serve as a complete block to adults who wish to access adult material [online] but do not" have the necessary form of identification. *PSInet v. Chapman*, 362 F.3d 227, 237 (4th Cir. 2004); *see also Am. Booksellers Found. v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003*)* (invalidating age-verification requirement that would make "adults who do not have [the necessary form of identification] . . . unable to access those sites"). Under the SAFE For Kids Act, that could include millions of people who do not have a driver's license or other government-issued form of identification.

About 15 million adult U.S. citizens do not have a driver's license, while about 2.6 million do not have any form of government-issued photo ID.[2] Estimates show another 21 million adult U.S. citizens do not have a *non-expired* driver's license, and over 34.5 million adult citizens have neither a driver's license nor a state ID card with their current name or address.[3] These numbers do not include non-U.S. citizens who do not have current government-issued identification, including undocumented immigrants who cannot obtain a state ID or driver's license.

Reliance on government-issued ID for age-gating also means that certain demographics will be disproportionately burdened when trying to speak or access protected speech online. Black Americans and Hispanic Americans are disproportionately less likely to have current driver's licenses.[4] And 18% of Black adult Americans do not have a driver's license at all.[5] Young adults are also less likely to have the requisite ID: 41% of U.S. citizens between 18 and 24 do not have an up-to-date driver's license.[6] The same is true for 38% of citizens between the ages of 25 and

[2] Jillian Andres Rothschild *et al.*, *Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge* 2, Univ. Md. Ctr. for Democracy & Civic Engagement (Jan. 2024), https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf.
[3] *Id*. at 2, 5; Michael J. Hanmer & Samuel B. Novey, *Who Lacked Photo ID in 2020?: An Exploration of the American National Election Studies* 3, Univ. Md. Ctr. for Democracy & Civic Engagement (Mar. 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf.
[4] Rothschild, *supra* note 1, at 2.
[5] *Id*.
[6] *Id*.

29.[7] Americans with disabilities and Americans with lower annual incomes are also less likely to have a current driver's license.[8]

Other age-verification methods permitted by the SAFE For Kids Act will not not guarantee access to those lacking a compliant form of government ID. For one, the law does not *require* online services to use alternatives to recording a government-issued ID, and many services may not offer alternative means to adults beyond supplying their ID. If a service instead opts to use transactional data, depending on the method chosen, many adults will still not have access to the means to verify their age via this method. For example, if a service relied on mortgage documents, it would exclude an enormous amount of adults, as nearly 35% of Americans do not own a home.[9] Should credit data be used, close to 20% of U.S. households do not have a credit card.[10] Immigrants, regardless of their legal status, may not be able to obtain credit cards, either.[11]

**Age-Verification Mandates Impermissibly Chill Anonymity Online**

Even if an adult can supply the requisite proof-of-age, the SAFE For Kids age-verification requirement still impermissibly deters adult users from speaking and accessing lawful content by undermining anonymous internet browsing. Anonymity is a respected, historic tradition that is "an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334, 341–43 (1995). Online anonymity "promotes the robust exchange of ideas and allows individuals to express themselves freely[.]" *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011). Age-verification schemes "are not only an additional hassle," but "they also require that website visitors forgo the anonymity otherwise available on the internet." *Am. Booksellers Found.*, 342 F.3d at 99. Moreover, "preserv[ing] anonymity" may be essential for users who seek to have "a distinct online identity," *Cyberspace, Commc'ns, Inc. v. Engler*, 55 F. Supp. 2d 737, 742 (E.D. Mich. 1999), *aff'd and remanded*, 238 F.3d 420 (6th Cir. 2000), or who want to discuss "sensitive, personal, controversial, or stigmatized content," *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007), *aff'd sub*

[7] *Id*.
[8] *Id*. at 3-4.
[9] *See* U.S. Census Bureau, CB24-62, *Quarterly Residential Vacancies and Homeownership, First Quarter 2024*, at 5 (Apr. 30, 2024), https://www.census.gov/housing/hvs/files/currenthvspress.pdf.
[10] *See* Board of Governors, U.S. Fed. Reserve, *Economic Well-Being of U.S. Households in 2022*, at 44 (May 2023), https://www.federalreserve.gov/publications/files/2022-report-economic-well-being-us-households-202305.pdf (in 2022, 82% of American households had a credit card).
[11] *See* Sonia Lin, *Identifying and Addressing the Financial Needs of Immigrants*, Consumer Fin. Prot. Bureau (June 27, 2022), https://www.consumerfinance.gov/about-us/blog/identifying-and-addressing-the-financial-needs-of-immigrants/ (describing how "many financial institutions have policies and practices in place that effectively exclude immigrants from access to bank services and to credit due to immigration status").

*nom. ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008). Without anonymity, "the stigma associated with the content of [certain] sites may deter adults from visiting them" at all. *PSINet, Inc.*, 362 F.3d at 236; *see also NetChoice, LLC v. Griffin*, No. 23-CV-05105, 2023 WL 5660155, at *17 (W.D. Ark. Aug. 31, 2023). That chilling effect only underscores the impermissible burden on protected anonymity that New York's statute imposes on its residents.

The SAFE For Kids Act's age-verification requirement will make anonymous internet browsing on covered sites extremely difficult and deter adult users from accessing speech due to concerns about being identified. Unlike in-person age-gates, the only viable way for a website to comply with the law's mandate is to require all users to *submit*, not just momentarily display, data-rich government-issued identification or other proof-of-age. This imposes significant burdens on adults' access to constitutional speech and "discourage[s] users from accessing" the online services that require that verification. *Reno v. American Civil Liberties Union*, 521 U.S. 884 (1997). By requiring the disclosure of identifying information, the SAFE For Kids Act forces adult users to risk "relinquish[ing] their anonymity to access protected speech, and . . . create a potentially permanent electronic record" of the sites they choose to visit. *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d. Cir. 2008).

Many other entities can potentially gain access to people's personal information collected to verify their ages under the law. All online data is transmitted through a host of intermediaries. This means that when a commercial website shares identifying information with its third-party age-verification vendor, that data is not only transmitted between the website and the vendor, but also between a series of third parties.

The third parties hosted on websites include trackers managed by data brokers, advertisers, and other companies that are constantly collecting data about a user's browsing activity.[12] Because many entities derive significant profits from selling personal information collected online, an array of actors are incentivized to collect as much data as possible. Every mouse click and screen swipe can be tracked and then shared with or sold to third party ad-tech companies and the data brokers that service them. Many people take steps online to protect their anonymity and avoid this pervasive surveillance, but the SAFE For Kids Act makes this even more difficult by requiring additional and more frequent disclosure of sensitive, identifying records. The law's failure to engage with the realities of the online advertising industry thus further undermines user anonymity.

[12] *See* Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, EFF (Dec. 2, 2019), https://www.eff.org/wp/behind-the-one-way-mirror*; see also* Paige Collings, *Debunking the Myth of "Anonymous" Data*, EFF Deeplinks (Nov. 10, 2023), https://www.eff.org/deeplinks/2023/11/debunking-myth-anonymous-data.

**Online Age Verification Further Chills Adult Users By Putting Their Most Sensitive Data At Risk Of Inadvertent Disclosure, Breach, Or Attack**

Legitimate data security concerns will further deter internet users from accessing protected First Amendment content. "Requiring Internet users to provide . . . personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and . . . afraid of fraud and identity theft[.]" *Gonzales*, 478 F. Supp. 2d at 806*; see also Mukasey,* 534 F.3d at 196; *PSINet, Inc. v. Chapman*, 167 F. Supp. 2d 878, 889 (W.D. Va. 2001), *aff'd*, 362 F.3d 227 (4th Cir. 2004) ("Fear that cyber-criminals may access their [identifying information] . . . . may chill the willingness of some adults to participate in the 'marketplace of ideas' which adult Web site operators provide.").

The same issues motivating the anonymity concerns described above apply equally to data privacy and security concerns. The SAFE For Kids Act will expose users' most sensitive information to an unquantifiable vast web of websites and intermediaries, and third-party trackers and data brokers. This not only gives multiple actors access to adult users' sensitive data, but also creates even more opportunities for the data to leak or be breached. By forcing users to submit to age verification, the SAFE For Kids Act increases their risk of being victims of data breaches, which are nearly unavoidable in this digital age. And once that personal data gets into the wrong hands, victims are vulnerable to targeted attacks both online and off. These dangers are serious and legitimate, and users are right to fear them.[13]

Data breaches are an endemic and ever-increasing part of modern life. A record 3,205 data breaches occurred in 2023, up 78% from the year prior, and far exceeding the previous record of 1,860 breaches in 2021.[14] These breaches affected over 350 million people—more than the entire population of the United States—and compromised nearly 11% of all publicly traded companies.[15] Those numbers continue to rise, and some of the most significant data breaches to date have occurred in 2024. In July, AT&T revealed that criminals stole phone numbers and call

[13] *See, e.g.*, Michelle Faverio, *Key Findings About Americans and Data Privacy* (Oct. 18, 2023), https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/ (76% of U.S. adults have "very little or no trust at all" that leaders of social media companies will not sell their personal data to others without their consent). *See also* Maria Bada & Jason R.C. Nurse, *The Social and Psychological Impact of Cyber-Attacks* (2020), https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf.
[14] Press Release, Identity Theft Resource Center, *ITRC 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High* (Jan. 25, 2024), https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high; *see also* Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[15] ITRC, *supra* note 14.; *see also id.* ("69% of general consumers have been victims of an identity crime more than once").

records of around 110 million people—"nearly all" of its customers.[16] Meanwhile, other bad actors stole an alleged 560 million records from Ticketmaster, as well as the medical and billing information of a "substantial proportion" of people in the U.S. from health tech giant Change Healthcare.[17]

The likelihood a user's information will be compromised in a breach also increases every time that information is transmitted to third party online actors. The AT&T and Ticketmaster breaches, for example, occurred because both companies shared information with a third-party cloud data vendor that was breached.[18] Under the SAFE For Kids Act, regulated online services will have to contract with third-party age-verification services, creating similar risks.

Further compounding the issue, the personal data disclosed under the law is extremely sensitive and often immutable.[19] The disclosure of personal information contained in a government-issued ID is more problematic because most people cannot easily change their biographic information or their home address. Contrast this with information that *is* intended to be more frequently given to third parties, such as credit card information. As an important security measure, credit card companies typically offer a quick and straightforward process for changing information, such as the card number, in the event of identity theft or a data breach.[20]

**Age-Verification Mandates Are Inherently Broad Speech Restrictions**

Laws that seek to protect minors but affect internet access in all households, even those without minors, are inherently overinclusive. Online age verification will be imposed on many, many more users than an in-person ID check. *See Free Speech Coal., Inc. v. Colmenero*, 689 F. Supp. 3d 373, 397 (W.D. Tex. 2023) . This is true, of course, no matter what method of age verification is used or how advanced the technology purports to be. Online age-verification laws are "dramatically different" from statutes that apply "only to personally directed communication between an adult and a person that the adult knows or should know is a minor." *Am. Booksellers Found. for Free Expression v. Sullivan*, 799 F. Supp. 2d 1078, 1082 (D. Alaska 2011). And because of the sheer scale of the internet, regulations affecting online content sweep in millions of people who are obviously adults, not just those who visit physical bookstores or other places

[16] Zack Whittaker, *The Biggest Data Breaches in 2024: 1 billion Stolen Records and Rising*, TechCrunch (Aug. 12, 2024), https://techcrunch.com/2024/08/12/2024-in-data-breaches-1-billion-stolen-records-and-rising/.
[17] *Id.*
[18] *Id.*
[19] Driver Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq*.
[20] *See, e.g.*, *Have a Lost or Stolen Card?*, Visa, https://usa.visa.com/support/consumer/lost-stolen-card.html (last accessed Sep. 17, 2024); *Frequently Asked Questions: What If My Card Is Lost Stolen Or Damaged?*, Chase, https://www.chase.com/digital/digital-payments/additional-wallets/faqs/lost-or-stolen (last accessed Sep. 17, 2024).

to access adult materials, and not just those who might perhaps be 17. Age-verification laws reach into fully every U.S. adult household, despite most not having any children.[21]

Although other laws that prohibit the sale of adult content to minors result in age verification via a government ID or other proof-of-age in physical spaces, there are practical differences that make those disclosures less burdensome or even nonexistent. Most tellingly, an in-person interaction between a merchant and an adult is often enough to verify that the individual is older than 17 and can legally purchase the materials. After all, there are usually distinguishing physical differences between young adults and those older than 35.[22] An older adult who forgets their ID at home or lacks an up-to-date government ID is not likely to face difficulty in obtaining material in a physical store because a visual check by a merchant can confirm they are an adult. Yet there is no analog to such ephemeral age checks online, which inherently require the disclosure and collection of personal information to verify an internet user's age.
Additionally, online age verification is likely to notably reduce adult users' willingness to consume or create protected content on a site.[23] Internet users are highly sensitive to website access barriers, and age verification adds a significant new step to a user's visit, in which they must submit government-issued ID or other identifying information, along with, in some instances, a current photo.

In addition to constitutional concerns, there are legitimate issues with every commonly-used method of age verification. Below, we describe technical limitations, privacy and security concerns, and other limitations of those mentioned.

**Method Analysis**
No method of age verification is both privacy-protective and entirely accurate. These methods don't each fit somewhere on a spectrum of "more safe" and "less safe," or "more accurate" and "less accurate." Rather, they each fall on a spectrum of "dangerous in one way" to "dangerous in a different way."

Offering a variety of these age determination options only glosses over the fact that every solution has serious privacy, accuracy, or security problems. This puts the burden on the

[21] Approximately 60% of U.S. family households do not include children under 18, and this percentage does not even account for the number of *non-family* households without children under 18. *See* Veera Korhonen, *U.S. Family Households With Children, By Family Type 1970-2022*, Statista (Nov. 3, 2023), https://www.statista.com/statistics/242074/percentages-of-us-family-households-with-children-by-type/.
[22] *See* David Gaudet, *ID Under 35: The BARS Program Carding Policy*, BARS Program (May 3, 2016), https://www.barsprogram.com/blog/?12310/id-under-35-the-bars-program-carding-policy.
[23] *See Will Co. v. Lee*, 47 F.4th 917, 924–25 (9th Cir. 2022) ("Research shows that sites lose up to 10% of potential visitors for every additional second a site takes to load, and that 53% of visitors will simply navigate away from a page that takes longer than three seconds to load." (footnote omitted)).

individual to decide whether they are most concerned with accuracy or privacy, generally without giving them the tools they need to determine which option is safest for them. This applies to all users: Age verification requirements don't just impact young people.

Many methods are simply not available to some users, and would push them towards a method that they may not prefer. Younger users are more likely to fail biometric assessments, and they may not have IDs for document verification; immigrant users are unlikely to have credit cards; Seniors are less likely to have driver's licenses, and so on.

Multiple studies indicate the problems with each method. France's National Commission on Informatics and Liberty (CNIL) found in 2022 that no method has the following three important elements: "sufficiently reliable verification, complete coverage of the population, and respect for the protection of individuals' data and privacy and their security." CNIL reviewed[24] payment cards, facial analysis, identity documentation, central government-provided tools, inference-based systems, and offline verification.

In its Roadmap for Age Verification[25] regarding adult content, Australia's government similarly found that for age assurance or verification to function in the country to limit access to adult content, it must, "work reliably without circumvention; be comprehensively implemented, including where pornography is hosted outside of Australia's jurisdiction; and balance privacy and security, without introducing risks to the sensitive personal information of adults who choose to access legal pornography." The government concluded[26] in mid-2023 that no method could meet these requirements.

Rather than repeat the same mistakes that other governments have made regarding age verification—setting unrealistic and unworkable requirements and then backtracking after coming to terms with the technological limitations—we hope New York will carefully consider the problems with each method before issuing guidance.

Below, we address the most commonly mentioned methods, and some of the biggest problems each present.

---

[24] *Online age verification: Balancing Privacy and the Protection of Minors.* CNIL. (n.d.). https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[25] *Roadmap for age verification.* (n.d.). https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf

[26] Guardian News and Media. (2024, May 22). *"no country in the world has solved this problem": Can Australia make age verification work for social media?* The Guardian. https://www.theguardian.com/australia-news/article/2024/may/23/australia-social-media-ban-under-16-age-verification-technology

**Government-Issued ID**

Requiring users to digitally hand over government-issued ID to verify their age creates enormous security and privacy risks, regardless of the specific data flow and verification methods. This is one of the most commonly proposed categories of age verification methods, and thus various ID verification methods have been proposed. The end goal of all methods is for the website or application provider to be assured of the age of the user based on the user's government-issued ID, but the specifics of where that verification happens and what entity is checking the ID itself can vary.

The most common proposal is for the website requiring assurance to either do the verification itself, or outsource the check to a third-party ID checking service, both of which require the contents and/or image of the ID to be transmitted to them remotely over the internet. Once this information is shared, there's no way for a website visitor to be certain that the data they're handing over is not going to be retained and used by the website, or further shared or even sold. Users must trust that the website they visit which is requiring ID, or its third-party verification service, both of which could be fly-by-night companies, are following these rules. All online data is transmitted through a host of intermediaries. This means that when a commercial website shares identifying information with its third-party age-verification vendor, that data is often not only transmitted between the website and the vendor, but also between a series of third parties.

Companies responsible for storing or processing this information are also likely to encounter data breaches, potentially exposing not only personal data like users' government-issued ID, but information about the sites that they visit. (The recent hack[27] of age verification company AU10TIX, which left login credentials exposed online for more than a year, is just one example.)

If a website does misuse or mishandle the data, the user might never find out. And if they do, the only enforcement mechanism they can rely on is from this office (§ 1508. Remedies. 1.). The lack of a private right of action in this legislation, which would provide a critical adjunct to governmental enforcement, will substantially increase the OAG's need for new enforcement resources and minimize options for recompense. The OAG may fail to enforce breaches of the law due to lack of resources, or simply because the impact from a small breach or bad actor is insufficient to use those resources.

[27] Jason Kelley. (2024, July 2). *Hack of age verification company shows privacy danger of Social Media Laws.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws

**Device-Based Verification**

Another proposed method of checking a government-issued ID is to place the burden on the operating system. In this proposal, a website asks the device for a stored age assurance token. In one implementation, the pitfalls of this method are the same as the pitfalls of the remote ID check described above; a remote service would still be involved (whether operated by the operating system provider or a third party), but instead of sending the age assurance token directly to the website, it is sent back to the user and stored on the device, where it can be given out to multiple websites. Alternatively, the check could be done in an automated fashion on the device itself, without uploading the ID to any external provider. This method would likely be easy to fool with a little effort, though it would require more effort than simply self-certifying that the user is above the required age.

In either of these methods, many people will be barred from using the services because they will not wish to share such sensitive information. And because these methods rely on verifying a user's identity, age verification through government-issued ID would erase the ability to use these websites anonymously, and without surveillance.

An unusual method mentioned in France's CNIL report proposes an alternative: use offline verification to check ID. This method involves the creation of "scratch cards" that would be available for purchase in a physical store upon manual checking of a government ID, similar to the purchase of alcohol or tobacco, thereby bypassing a digital verification or upload requirement.

In any of these methods, however, the tens of millions of Americans who do not have government-issued identification would be barred from accessing services relying on them. Additionally, all of these methods make naive assumptions about the relationship between account, device, and user. Not every device is owned or used by just one person, nor every account. It's a bold failure of logic to think there's a one-to-one relationship between every device, account, and user.

**Biometric Assessment**

Biometric age assessment—often called "age estimation"—has several problems. A recent NIST review[28] of several major age estimation algorithms determined that for each, accuracy is strongly influenced by sex, image quality, region-of-birth and race, and interactions between those factors. There is also no uniformly superior algorithm.

[28] *Face Analysis Technology Evaluation (fate) age estimation & verification*. (n.d.). https://pages.nist.gov/frvt/html/frvt_age_estimation.html

For those near the age of eighteen, NIST's review indicated that the algorithms are simply not very accurate. False positive error rates are considerable when used on younger faces: every algorithm incorrectly estimated more than 40% of seventeen-year-olds to be above a challenge age of eighteen. (Pages 23,24) For eighteen to twenty-one-year olds, the mean absolute error rate of all algorithms was generally three or more years (Page 43–MAE for each algorithm across age range of 18-21). Use of this type of age estimation to determine who is eighteen or older could result in an enormous number of inaccurate estimates—both false positives and false negatives—for users within several years of the required age of eighteen, making it a poor option for those users. It's important to note that the NIST review clearly demonstrates the racialized aspect of failure for this technology; across the board these tools fail at estimating the ages of Black and Asian people, further engendering harms that facial mapping technologies cause them.

It is also profoundly dangerous that from an end-user's perspective this technology is indistinguishable from face recognition and the collection of biometric information. If a third-party company acting in bad faith *collected* biometric faceprints of users, it would be impossible for users to know. This technology also allows for dangerous and biased applications, like screening for who belongs to a religious or sexual minority.

**Assessment of User Activity**

Assessment based on analyzing user activity is an unlikely, inaccurate, and dangerous path for companies to take. While user activity may allow advertisers to make guesses about the demographics or behaviors of a user, those guesses are simply that. Nearly everyone has seen a strangely targeted ad based on an inaccurate estimation of your behavior or demographics. Perhaps an adult user clicked a link to a cartoon's website, or a young user wanted to learn how to change a tire despite not being old enough to drive. It is unlikely that a company which could be held liable for age estimation mistakes would rely on this flimsy data for most users.

**Attestation From a Third-Party Business**

Relying on financial and credit records to verify adults' identities can exclude large numbers of adults. Some 20 percent of U.S. households do not have a credit card and 35 percent do not own a home. Immigrants, regardless of their legal status, may not be able to obtain credit cards. Systems that rely on third-party data have all of the problems that this third-party data often has, such as incorrect information (one in four participants in a 2013 FTC study[29] had errors in their credit report, for example).

[29] Liu, H., & FTC, S. at the. (2024, August 20). *In FTC study, five percent of consumers had errors on their credit reports that could result in less favorable terms for loans*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports-could-result-less-favorable-terms

**Attestation from Other Users**

This method essentially puts the burdens of age verification onto others. While it may minimize some of the dangers of age verification for a few, it cannot entirely remove it. The method is also, obviously, unusable for many people. Further, it is no more reliable than self-attestation.

**Self-attestation**

This method is sufficiently privacy-protecting, but obviously not reliable.

**Cognitive Tests**

Cognitive differences are not accurate indicators of age.

---

Thank you for the opportunity to share these comments. We appreciate the intent of the New York State (SAFE) for Kids Act, but remain concerned about the burdens it will have on residents' rights to access lawful speech online. These burdens will not and cannot be remedied by new developments in age-verification technology. We urge the New York Attorney General's office to consider the points put forth to ensure that rulemaking effectively addresses the issues at hand and supports the interests of all stakeholders involved. If you have any questions or need further clarification, please feel free to reach out to hayleyt@eff.org.

Sincerely,

Hayley Tsukayama
Associate Director of Legislative Activism
Electronic Frontier Foundation
(415) 436-9333 x 161