epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

New York State Attorney General

Advance Notice of Proposed Rulemaking for the SAFE for Kids Act

Pursuant to New York General Business Law Section 1500 *et seq.*

September 30, 2024

The Electronic Privacy Information Center (EPIC) and the Center for Digital Democracy (CDD) submit these comments on the Attorney General's Advanced Notice of Rulemaking for the NY SAFE for Kids Act (the Act).

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC believes that the First Amendment is not a barrier to protecting kids online. EPIC has provided courts, legislators, and attorneys general with guidance about the constitutional, privacy, and access questions implicated by kids' online privacy and safety legislation.[2] EPIC has defended the constitutionality of the California Age-Appropriate Design Code as amicus in both the district and appellate courts. Most recently, EPIC filed an amicus brief in the U.S. Supreme Court case *Free Speech Coalition v. Paxton*, No. 23-1122, arguing that lower courts are not analyzing the constitutionality of kids' privacy and safety laws appropriately and that age determination can be implemented in constitutional ways. The brief is attached to these comments.

[1] https://epic.org/about/.
[2] https://epic.org/issues/platform-accountability-governance/platform-governance-laws-and-regulations/.

CDD is a public interest research and advocacy organization, established in 2001, which works on behalf of citizens, consumers, communities, and youth to protect and expand privacy, digital rights, and data justice.[3]

The NY Safe for Kids Act does not regulate speech. However, given the trend of Big Tech interests challenging kids' online privacy and safety laws on First Amendment grounds, we recommend that the Attorney General craft regulations anticipating a similar First Amendment challenge. To that end, the regulations should minimize the barriers to accessing the regulated platforms, in particular by emphasizing that age determination does not need to be implemented as a condition of accessing regulated platforms. The Attorney General should also ensure that approved age determination tools follow data minimization principles. The Attorney General should also incentivize the development of even more privacy-protective age determination tools in the future. Finally, the Attorney General can bolster user trust in age determination by requiring covered operators and age determination vendors publish data protection impact assessments for their age determination processes and to communicate to users the privacy protections provided both by the technology and the law.

I. Age Determination Should be Implemented in Ways that Minimize Barriers to Access.

Responsive to questions 1, 3, 10, 11

To insulate the Act from constitutional challenge, and to ensure equitable access to web services and features, the Attorney General should promulgate rules that do not make age determination an unreasonable barrier for users. Fortunately, the Act gives the Attorney General and covered operators many options to prevent age determination from being a barrier to access. Unlike many of the other laws involving age determination that state legislatures have enacted over the last

[3] https://democraticmedia.org/.

several years, the Act does not force covered operators to make age determination a condition of accessing their platforms. The regulations should encourage covered operators to implement age assurance only as a condition for accessing regulated features, to give users choice in tools to determine their age, and to use low- or no-friction methods when available, appropriate, and where the privacy risks do not outweigh the gains in accessibility.

A. Age determination should not be a condition of accessing regulated platforms.

The regulations should emphasize that the Act does not require covered operators to determine the ages of users as a condition of accessing their services and thus does not require covered operators to erect barriers to accessing their services. The regulations should incentivize covered operators to comply with the Act by either eliminating the two regulated features—addictive feeds and nighttime push notifications—for all users or turning them off by default.

First, there is no need for covered operators to use age determination at all if they apply the Act's protections to all users.[4] Covered operators who choose to eliminate addictive feeds would simply stop using certain categories of users' personal information to select and order content in their feeds. These covered operators would still be free to use various other algorithmic selection and ordering methods, including algorithms that choose and order content based on the covered operator's content moderation policies.[5] Covered operators could also simply stop sending all users push notifications at night.

Covered operators who wish to offer addictive feeds and nighttime push notifications to users can also turn these features off by default for all users and only require users who wish to turn on these features to go through the age determination process or have their parent provide verifiable

[4] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(1) (McKinney 2024).
[5] *See Moody v. NetChoice*, 144 S. Ct. 2383, 2404 n.5 (2024); Tom McBrien, *In NetChoice Cases, Supreme Court Labels a Surprisingly Narrow Class of Online Platform Company Activities as Protected Expression*, EPIC (July 10, 2024), https://epic.org/in-netchoice-cases-supreme-court-labels-a-surprisingly-narrow-class-of-online-platform-company-activities-as-protected-expression/.

consent. Under such a design, age determination would not be a barrier to accessing the covered operator's service because it would not be performed as a condition of accessing the service. Instead, age determination would only be a condition of accessing a particular type of feed—the addictive feed—or turning on nighttime push notifications. As a result, the impact of age determination would be limited only to users who want to turn addictive feeds or nighttime push notifications on. Since not every user will seek to turn these features on, this design would limit the number of users that must go through the age determination process and so limit any burdens to this (potentially small) subgroup of users. Minimizing the number of users that must go through the age determination process would also limit the compliance costs for covered operators.

Age gating specific features of a covered platform instead of age gating the platform in its entirety will also help insulate the Act from constitutional challenges. A First Amendment challenge to the Act is likely to argue that the Act requires covered operators to make age determination a condition of accessing their platforms, and that age determination will chill users' right to access speech by disincentivizing them from accessing covered platforms altogether.[6] The regulations could preempt such a challenge by only requiring users to undergo age determination as a condition of accessing specific features and settings. If users are able to access all of the content on a website without undergoing age determination, then age determination cannot be credibly posed as a burden users' access rights.

Applying the Act's protections either to all users or as a default setting would not interfere with adult users' access to content and thus would not create new First Amendment concerns. The Act's protection against addictive feeds is a content-neutral regulation of a covered operator's data

[6] *See, e.g.*, Writ for Petition of Certiorari, *Free Speech Coalition v. Paxton*, U.S. Supreme Court (No. 23-1122); *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *2 (W.D. Ark. Aug. 31, 2023); Pl.-Resp't's Res. Br., at *22–23, *25, *49–50, *NetChoice, LLC v. Bonta*, No. 23-2969, 2024 WL 3838423 (9th Cir. Aug. 16, 2024).

practices.[7] The Act does not limit the content that covered operators can include in a users' feed, it only limits the user data that the covered operator can use to select and order content. Turning addictive feeds off for all users, then, does not limit adults to viewing content suitable for children, it merely extends protections against behavioral profiling to adults as well as kids. The Act's protection against nighttime push notifications is a content-neutral time, place, and manner restriction akin to federal and state robocall protections. Like robocalls, nighttime push notifications are a nuisance and an invasion of privacy, and the Act regulates their transmission without consideration of the message transmitted.[8]

B. Low- or no-friction age determination options can minimize barriers to accessing regulated features.

The regulations should encourage covered operators to use low- and no-friction age determination methods when available. Users might decide not to undergo an age determination process if the process requires users to complete many burdensome steps. Design literature refers to this burden as "friction."[9] Covered operators may not be able to use low-friction methods to estimate the ages of all users, but they may be useful first steps that narrows the pool of users that must use higher friction methods. The regulations should also encourage the development and use of age

[7] *See* Megan Iorio, EPIC, *NetChoice v. Bonta: An Exacting Level of Scrutiny No Privacy Law Could Survive* (Jan. 15, 2024), https://epic.org/netchoice-v-bonta-an-exacting-level-of-scrutiny-no-privacy-law-could-survive/.

[8] For example, courts have repeatedly upheld the Telephone Consumer Protection Act (TCPA) as a constitutional, content-neutral time, place, and manner regulation. *See, e.g., Moser v. FCC,* 46 F.3d 970 (9th Cir.), *cert. denied*, 515 U.S. 1161 (1995); *Gomez v. Campbell-Ewald Co.*, 768 F.3d 871, 876-77 (9th Cir. 2014), *aff'd on other grounds*, 136 S. Ct. 663 (2016) (finding the TCPA constitutional post-*Reed v. Town of Gilbert*, 135 S. Ct. 2218 (2015)); *Duguid v. Facebook*, *Inc.,* 926 F.3d 1146, 1157 (9th Cir. 2019), *rev'd in part on other grounds*, 592 U.S. 395 (2021) ("Excising the debt-collection exception preserves the fundamental purpose of the TCPA and leaves us with the same content-neutral TCPA that we upheld—in a manner consistent with *Reed*—in *Moser* and *Gomez*.").

[9] *See* Brett Frischmann & Susan Benesch, *Friction-in-Design Regulation as a 21st Century Time, Place, and Manner Restriction*, 25 Yale J. L. & Tech. 376, 379 (2023).

determination methods that only require users to go through the determination process once and to use this determination to pass through age gates on other services.

Covered operators who can use existing data to estimate the age of users should be encouraged to do so. Some covered operators may already estimate users' ages to target them with ads.[10] Covered operators that have been in operation for a decade or more may also be able to estimate the age of many users based on the age of the users' accounts. These methods of age determination would be, essentially, frictionless—covered operators could make the age determination on the back end without collecting any additional information from users. The Attorney General should, however, make clear that the Act does not license covered operators to begin or increase surveillance of users for the purpose of determining age.

There are also additional, low friction methods of estimating age that covered operators may be able to deploy more easily and that follow authentication steps that users are already familiar with. For example, some third-party vendors offer tools to check the age of an email address by cross referencing with information from institutions where the user has used the email address to sign up for an account.[11] Users encounter the low, familiar friction of entering their email address. But this method does carry some privacy risks, the greatest being that vendors may rely on data brokers for their information about the age of email accounts,[12] and the data broker industry is the backbone of the surveillance capitalism ecosystem.[13] Direct verification with the email provider would be a more privacy protective method of determining the age of the email account.

---

[10] *See* Nico Grant et al., *YouTube Ads May Have Led to Online Tracking of Children, Research Says*, N.Y. Times (Aug. 17, 2023), https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html.
[11] *E.g.*, VerifyMyAge, *Email Address FAQs*, https://www.verifymyage.co.uk/email-address-age-estimation-faqs (last visited Sept. 30, 2024).
[12] *Id.*
[13] Comments of EPIC, CFPB Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information 2-14 (July 14, 2023), https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf.

Another low friction method of estimating some users' ages would be to authenticate the users' control of a university email account. Having a valid university email account is a good, although underinclusive, proxy for "not a minor," since the overwhelming majority of those in possession of a university email address are 18 or older. Covered operators also likely already have the means of authenticating users' access to an email account, since many authenticate the user's email when the user creates a login.

The regulations should also encourage the development and use of age determination methods that allow a user to go through the age determination process once and then use that determination across multiple platforms.[14] These one-and-done methods would make age determination frictionless after the initial determination. Covered operators should be required to recognize signals from these tools. It may be helpful for the Attorney General to convene a standards-setting group for these age signals to encourage uniformity and choice in the marketplace.

C. Providing users with an array of age assurance options is likely to decrease barriers to use.

Users should be offered multiple options for determining their age on each regulated platform. Offering users a wide variety of options allows a user to choose the method that they are most comfortable using and that works best for them. Different users are likely to prefer different methods. Some may be reticent to provide government ID—or not have one at all—while others may prefer this authentication method because they are familiar with the process from other authentication experiences. Some users may avoid parental attestation as an age determination method if the user does not have a reliable or safe relationship with a parent.

[14] *E.g.*, Bandio, *Learn More* (2024), https://www.bandio.com/learn-more-bandio.

Covered operators should also allow users to use multiple age determination methods in series. Some users may prefer to first try to authenticate using a biometric estimation method. But because biometric methods make predictions based on information that may not be representative of the entire U.S. population,[15] they may not be as accurate for women, people of color, and people with disabilities, and users who get an inaccurate determination through this method should be allowed to try a different method that may be more accurate for them. By facilitating user choice in age determination, the regulations can increase consumer trust and decrease barriers to use.

D. The regulations should require covered operators to institute an error-correction process.

The regulations should require covered operators to create formal processes to correct errant outcomes from age determination. Although there is a provision in the law that directs the Attorney General to receive these types of complaints,[16] the regulations should require covered operators themselves to have a swift, responsive appeals or correction process.

II. Age Determination Should be Privacy Protective.

Responsive to questions 1, 2, 3, 9, 11, 15, 18, 19, 20

Privacy must be a central consideration in how the Attorney General curates the list of acceptable age determination methods and determines the rules that will govern the age determination process. Data minimization practices like limiting data collection, use, and disclosure to what is strictly necessary for determining whether a covered user is a minor help protect users' data from misuse, theft, and abuse. Processing user data on the users' device instead of a remote server and using cryptographic techniques to protect information in transit also enhance user privacy and security. All entities involved in the age assurance process should adhere to data minimization

[15] Patrick Grother et al., Face Analysis Technology Evaluation: Age Estimation and Verification, NIST (May 2024), https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf.
[16] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1508(2) (McKinney 2024).

principles and communicate the minimum information necessary to comply with the Act. By promulgating regulations that require approved age determination vendors to process information in a privacy protective and secure manner, the Attorney General can also incentivize the development of age determination techniques that prioritize user privacy and security.

A. Strong privacy protections are necessary to counteract companies' market incentive to collect as much data as possible.

It is important for the regulations to center privacy because covered operators and age assurance vendors have market incentives to engage in privacy-invasive data management practices. The dominant business structure for social media platforms is to collect massive amounts of consumer data for the purposes of constructing user profiles for advertising. Without adequate federal data protection standards, "online firms have been allowed to deploy commercial surveillance systems that collect and commodify every bit of our personal data."[17] Platforms' and data brokers' detailed consumer profiles heighten the risk of data breaches or misuse, manipulation and discrimination and reduce users' trust.[18]

B. The Attorney General should establish privacy-protective criteria for age determination techniques.

It is critical for the Attorney General to ensure that age determination does not contribute to the commercial surveillance system and broader data protection crisis. By adopting privacy- and security-focused regulations, the Attorney General can also incentivize the development of more secure and privacy-protective age determination technology.

The privacy risks from age determination will not just vary method-to-method but tool-to-tool as different companies will have different data practices and implement different privacy and

[17] Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 7 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillanceANPRM-comments-Nov2022.pdf [hereinafter *EPIC Commercial Surveillance Comments*].
[18] *Id.*

security features. The Attorney General should assess the privacy risks posed by each potential age determination tool and prioritize tools that minimize data collection, use, and disclosure. Currently, companies determine age using a range of tools, some more privacy-protective than others.

The user information an online age assurance tool collects, processes, and stores generally defines its privacy risks. The more personal information a company collects, processes, or stores—and the more sensitive that personal information—the higher the risk to users' privacy. But companies can implement privacy and security features that mitigate these risks, so the Attorney General must look at the totality of a company's data practices and a tool's privacy and security features to determine the overall privacy risks.

The regulations should require that any approved age determination tool only collect, process, and disclose personal information that is strictly necessary to determine whether a covered user is a covered minor. The regulations should also incentivize adoption and development of more privacy-protective and secure age determination technology in the future.

i. Minimize data collection—particularly sensitive personal information.

The best way to protect users' data from misuse, theft, and abuse is to minimize the amount of data collected about users in the first place—particularly sensitive personal information. Every piece of personal information collected by a platform is inherently at risk of data breach or unauthorized access and use.[19] Limiting the data collected for age determination to what is strictly necessary will lessen the risk that the data will be used to link users' identities to their browsing history, protect against unauthorized secondary uses, and mitigate data security risks.

[19] John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

The information that is strictly necessary for a tool to make an age determination will depend on the method the tool uses to determine age. Some techniques require users to provide identifying information, like a government ID. Many require users to turn on their cameras and provide a selfie. The tools may also process the information users and third parties provide and thereby collect additional data. The Attorney General should ensure that, at each step, companies are only collecting information strictly necessary to determine whether a user is a minor.

Generally, the more sensitive personal information a tool collects, the more of a risk the tool could pose to users.[20] Sensitive personal information includes biometric identifiers, social security numbers, and other information that uniquely identifies a user or is processed or combined with other data points to reveal sensitive data about consumers, "putting them at risk of many harms, including discrimination, stalking harassment, and government scrutiny."[21] The legal landscape in the United States has long recognized the risks of collecting sensitive personal information and provides special protections for this information.[22] Because identifying information is especially useful in perpetrating identity theft, it is at heightened risk of data breach.[23] Collection of identifying information can also deter some users from using a feature if they fear that their identity will be linked to their browsing history, which itself might reveal sensitive or embarrassing information about the user.[24]

The Attorney General should prioritize age assurance tools that do not collect sensitive personal information. Where collection of sensitive personal information is strictly necessary for a

[20] EPIC Commercial Surveillance Comments, *supra* note 17 at 26.
[21] EPIC Commercial Surveillance Comments, *supra* note 17 at 35.
[22] *See* Helen Nissenbaum, Symposium, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119, 128 (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.
[23] *See* EPIC Commercial Surveillance Comments, *supra* note 17 at 183.
[24] *See* Noah Apthorpe, Brett Frischmann & Yan Shvartzsnaider, *Online Age Gating: An Interdisciplinary Investigation* 19–20 (Aug. 1, 2024).

tool to make an age determination, it will be important for the Attorney General to require the tool have additional protections against data misuse.

ii. Limit the secondary uses of data.

The Act prohibits covered entities from using information that was collected for the purpose of age determination for any other purpose.[25] The regulations should clarify that this requirement applies to all entities involved in the age determination process. The regulations should also clarify what "any other purpose" is by prohibiting out-of-context, secondary uses of data that are inconsistent with the reasonable expectations of users and lead to violations of user privacy and autonomy.[26] Limiting secondary uses of data will reduce the amount of personal data that is collected and transmitted by covered entities and age assurance vendors. Strictly prohibiting the use of age determination data for other purposes will also help increase user trust in the system, ensuring that users do not forego access to services because they fear their data will be leaked, stolen, or used to link their viewing history to their personal identity.

iii. Minimize processing of data for age determination purposes.

The processing that is strictly necessary for age determination depends on the specific technique. But one general principle does apply. Because the Act only requires covered operators to determine whether a covered user is a covered minor, age determination tools should only process the information that is strictly necessary to determine whether a user is a minor.

[25] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(3) (McKinney 2024).
[26] EPIC Commercial Surveillance Comments, *supra* note 17 at 1. *See* Suzanne Bernstein, Data Minimization: Centering Reasonable Consumer Expectation in the FTC's Commercial Surveillance Rulemaking, EPIC (April 20, 2023), https://epic.org/data-minimization-centering-reasonable-consumer-expectation-in-the-ftcs-commercial-surveillance-rulemaking/ (reasonable consumer expectation is central to an effective data minimization framework).

A few examples may be illustrative. For a tool that determines age based on a government ID, the best practice would be for the tool to extract only the year of birth from the ID—the users' name, address, and exact date of birth are not strictly necessary for making an age determination. Extracting the photo from the ID to match against a selfie taken in real-time would also be permissible as this processing can ensure that the ID actually does belong to the user without collecting other identifying information. For a tool that estimate age based on a face scan, it is important for the tool not to create a biometric identifier, but instead to collect a profile only detailed enough to estimate whether the user is a minor.

iv. Encourage on device processing and storage, particularly for sensitive personal information.

Another way that an age assurance tool can minimize data collection is by processing and storing an age determination on a user's device instead of remotely on the company's servers.[27] Tools that process and store data on users' devices do not expose users to the same privacy and security risks as tools that process on companies' servers because the companies do not collect the data at all—the data never leaves the users' devices. The company thus cannot repurpose the data, and a hacker attacking the company's servers cannot steal the data.

On device processing and storage can especially mitigate the risks associated with tools that need sensitive personal information to make an age determination. Some techniques—like those based on government ID or biometric estimation—are more amenable to on device processing, while techniques that depend on checks to a central database or authentication of a third party—like credit

[27] Scott Babwah Brennan & Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?*, Utah State University Center for Growth and Opportunity 4 (2023), https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.

card[28] and email address history[29]—will likely require that some personal information be collected and processed by remote servers.

v. Minimize data retention.

The Act requires companies to delete information collected to determine age "immediately after an attempt to determine" a user's age.[30] The regulations should make clear that this requirement applies to covered operators and any third parties that collect a users' information in the process of determining their age.

The Attorney General should also require covered operators and third-party age determination vendors only retain the minimum amount of information necessary about a user's age—that is, whether they are or are not a minor.

vi. Minimize and protect data in transit.

If a covered operator uses a third-party vendor for age determination, both parties should transfer only data that is strictly necessary for the age determination. Minimizing the data transferred helps protect against linking a users' identity with their internet activity and also protects against data breach. Regulations that minimize the amount of data transferred for age determination would also weaken the incentive for covered operators and third-party vendors to collect extraneous information from users.

Third-party age determination tools do not need covered operators to communicate much, if any, information about a user to complete an age determination—most of the required information will come directly from the user. Once a third-party age determination has been made, the company

[28] *Id*.
[29] VerifyMyAge, *Email Address FAQs*, https://verifymyage.com/email-address-age-estimation-faqs (last visited Sept. 30, 2024).
[30] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(3) (McKinney 2024).

should only need to send a yes or no signal to communicate to the covered operator that the covered user is a not a covered minor.

The optimal method for communicating age determinations would be to use modern cryptography techniques like "zero-knowledge proofs."[31] Using this technique, the age determination tool would confirm that a user is displaying a valid credential without allowing the covered operator to learn any additional information about the user, like their identity.[32] The age determination vendor also would not learn any additional information about the user from the covered operator, such as the websites the user visits.[33]

The regulations should also encourage third-party vendors to protect information it transmits by using another cryptography technique like encryption.[34] Encrypting an age determination result would encode the age information so that only authorized parties could access it. The Attorney General should prioritize tools that use zero-knowledge proofs and other cryptographic techniques for securely transferring as little information as possible between entities.

C. The regulations should prioritize privacy over accuracy.

Requiring privacy-protective age determination processes is important for insulating the SAFE for Kids Act from a potential First Amendment challenge. When deciding how to promulgate its regulations, the Attorney General may identify tradeoffs between the accuracy and privacy protectiveness of different age determination methods. To protect users' rights and to ensure the law

[31] *See* Sarah Forland, Nat Meysenburg & Erika Solis, New America Foundation Open Technology Institute, *Age Verification: The Complicated Effort to Protect Youth Online* 12 (Apr. 23, 2024), https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/.
[32] *Id.*
[33] *Id.*
[34] *See* Jérôme Gorin et al., *Demonstration of a privacy-preserving age verification process*, Commission Nationale Informatique & Libertés (June 22, 2022), https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process.

passes First Amendment muster, the Attorney General should resolve these tradeoffs in favor of methods and regulations that ensure privacy at the expense of accuracy.

Although the law clearly does not restrict access to content, a constitutional challenge would likely allege that it does and that age determination burdens adults' right to access speech.[35] These challenges will depend on claims that the privacy risks associated with age determination will chill users' right to access speech by disincentivizing them from accessing covered websites altogether.[36] These challenges could hopefully be dispensed of by establishing that the SAFE for Kids Act does not requiring age determination as a condition to access covered platforms and does not limit access to content on those platforms.[37] But Courts have struggled to make these distinctions online,[38] so the Attorney General would be wise to err on the side of caution by privileging age determination methods and regulations that minimize the privacy burdens on users.

Privacy concerns are likely to impose more of a burden on access rights than accuracy concerns will. People reasonably fear for their online privacy given the tech industry's pursuit of surveillance capitalism. Implementing age determination systems that require users to fork over a lot of sensitive personal information in exchange for accessing certain platform features may reasonably cause some users to forego accessing the platform altogether. While this chill can be mitigated by requiring covered websites to allow multiple age assurance methods and to determine age only when

[35] *See, e.g.*, Writ for Petition of Certiorari, *Free Speech Coalition v. Paxton*, U.S. Supreme Court (No. 23-1122); *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *2 (W.D. Ark. Aug. 31, 2023); Pl.-Resp't's Res. Br., at *22–23, *25, *49–50, *NetChoice, LLC v. Bonta*, No. 23-2969, 2024 WL 3838423 (9th Cir. Aug. 16, 2024).
[36] *See, e.g.*, Writ for Petition of Certiorari, *Free Speech Coalition v. Paxton*, U.S. Supreme Court (No. 23-1122).
[37] *See* supra Part I.A.
[38] *See, e.g.*, *NetChoice v.* Bonta, 692 F. Supp. 3d 924, 952–59 (N.D. Cal. 2023), *aff'd in part, vacated in part*, 113 F.4th 1101 (9th Cir. 2024).

a user wants to access certain settings,[39] requiring some of the approved methods to be highly privacy-protective could help avoid this chill.

The burden imposed by less accurate age determination is lower and more mitigable than the burden imposed by privacy-invasive age determination. If age determination is required as a condition to access a covered platform, the potential burden on access imposed by privacy-invasive systems is foregoing access to the platform altogether. But the burden imposed on an adult by being improperly labeled a covered minor is much less: a user would still have a right to view everything on a covered website—their privacy and notification settings will just be different. With an effective error-correction process and users having the option to try other age assurance methods, an adult should be able to easily remedy an inaccurate determination.

Covered operators will also not be penalized for incorrectly labeling a minor as an adult. Under the statute, users whose ages cannot be accurately determined should be treated like adults, meaning they are not barred from accessing any features on a service. Incorrectly labeling some children as adults may somewhat weaken the law's overall effect, but it will strengthen the law's defenses against First Amendment challenges by lowering its likelihood of burdening access to a website. The downsides of choosing privacy over accuracy are also likely only temporary. As more privacy-protective and accurate age determination tools are developed, the Attorney General can and should update the regulations to require covered operators to integrate these tools into their platforms.

D. The Attorney General should implement a process for evaluating and approving new age assurance methods.

The regulations should also create a formal process to incentivize the development and approval of new, privacy-protective age determination methods in the future. This process can be

[39] *See* supra Parts I.A, I.C.

modeled off the Federal Trade Commission's (FTC) process to approve new Verifiable Parental Consent (VPC) methods for the Children's Online Privacy Protection Act (COPPA). The COPPA Rule lists several acceptable VPC methods, but also invites operators or vendors to submit new VPC methods for FTC approval.[40] After a public comment period, the FTC can approve a new method that meets specific criteria set forth in the Rule: "Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[41]

The Attorney General should institute a similar process in regulations to approve new age determination tools in the future. While the law already directs the Attorney General to consider "the impact of the age determination techniques on the covered users' safety, utility and experience,"[42] the regulatory process for approving new methods should also encourage the development of more secure and privacy-protective methods of determining age. The Attorney General should consider the following factors when approving new age determination methods: the amount of personal information required to perform or transmit age determinations, whether the tool processes and stores age determinations on-device or in-browser, whether the tool uses privacy-protective communication techniques like zero knowledge proofs, whether the tool allows for once-and-done age determinations and has the potential to increase interoperability, and other privacy or data security features and risks.

E. The regulations should include strong enforcement commitments.

The regulations should include significant penalties for data misuse in the age determination process. Data misuse should include practices that run counter to data minimization: collecting,

[40] COPPA Rule, 16 C.F.R. §312.5(b)(2)(2024).
[41] *Id*. at §312.5(b)(1).
[42] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(2)(b) (McKinney 2024).

sharing, or using data for purposes beyond what is strictly necessary to determine if a covered user is a minor. The Attorney General must also demonstrate readiness to enforce these rules. Steep monetary fines are important for ensuring compliance, but so is attaching other penalties like expungement of misappropriated data and anything the data was used to build. Additionally, whenever the Attorney General brings an enforcement action for data misuse, the regulations should require companies to communicate to consumers the nature of the infraction and all privacy protections afforded by the age determination process, regulations, and provisions of the law in a clear, concise, and conspicuous manner.

III. Improve Consumer Trust and Safety Through Transparency

Responsive to questions 1, 10, 19, 20

The regulations should include strong transparency provisions to ensure that privacy and safety regulations are effective and that users are well informed about the age determination process. The Attorney General should require covered operators engaging in age determination and third-party providers of Attorney General-approved age assurance techniques to conduct ongoing Data Privacy Impact Assessments (DPIA) and make those reports publicly available to ensure compliance and increase consumer trust.

A DPIA is a tool for companies to identify and mitigate privacy and data security risks from using personal data. DPIAs have been a key component of data protection frameworks for more than thirty years and are required components of many federal and state laws.[43] To be most effective, DPIAs should initially be pre-decisional, requiring companies to evaluate privacy risks from age determination processes *before* implementing those systems and offering age determination to users. Even a baseline analysis from a DPIA enables a company to make informed decisions about whether certain data uses can be justified in light of privacy impacts. Beyond an initial assessment, the

[43] EPIC Commercial Surveillance Comments, *supra* note 17 at 162.

regulations should require periodical DPIAs to facilitate an iterative process for covered operators and third-party vendors to measure, effectuate, and demonstrate compliance with data management requirements in the law and from regulations.

Transparency around data management practices can enhance consumer trust. The Attorney General should promulgate regulations that require meaningful notice about age determination methods. First, the Attorney General should publish DPIAs from any covered operator and third-party vendor engaging in age determination under the NY Safe for Kids Act on a publicly accessible website. Additionally, regulations should require covered operators and third-party vendors to include certain disclosures on their websites. Companies should be required to give users effective notice of the privacy protections provided by the technology and the law—including the penalties companies face if they fail to provide these protections—and to provide detailed information about the data collection and use practices of each age determination tool.

For example, the regulations should direct covered operators to evaluate the extent to which their age determination practices incorporate data minimization principles in a DPIA. Any covered operator or third-party vendor performing age determination should only collect information that is strictly necessary for making the age determination, and third-party age determination tools external to the social media platform should only communicate the minimum amount necessary to the social media platform that the user is trying to access. The law also requires covered operators and vendors not use information collected for age determination for any other purpose and deletes it after an age determination attempt.[44] Meaningful transparency would both inform consumers about these privacy protections afforded by technology and the law, and include assessments of if, and whether, covered operators and vendors are effectively implementing those safeguards.

[44] NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(3) (McKinney 2024).

IV. Conclusion

EPIC and CDD applaud the Attorney General's attention to the important issues shaping privacy, security, and safety for minors and adults online. EPIC is eager to engage with the Attorney General further on age assurance, data privacy, or on any other issues raised in this comment. Please contact EPIC Counsel Suzanne Bernstein at Bernstein@epic.org with any questions.

Respectfully submitted,

/s/ *Megan Iorio*
Megan Iorio
EPIC Senior Counsel

/s/ *Thomas McBrien*
Thomas McBrien
EPIC Counsel

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Counsel