Privacy Considerations for Age-Based Restrictions on Web Content Access

Julia Hanson (Apple), George Tankersley (Apple), Theresa O'Connor (Apple)
July 2025

Age verification laws that require websites to verify users' ages can threaten online privacy, especially if technical solutions to satisfy legal requirements are not implemented thoughtfully. In this paper, we outline several privacy risks posed by solutions to age verification requirements on the web and propose privacy principles to guide the development of privacy-preserving alternatives.

Consider a naive approach for a website seeking to restrict access to certain content: when a user attempts to access age-restricted content, the site asks the user to upload some kind of formal identity document, such as a government-issued photo ID. In some cases, the site may also ask the user to upload a selfie or video of themselves as additional verification. A user may have to repeat this process several times with different websites as they try to access various content on the web.

This approach would have significant negative privacy impacts:

- *Oversharing of personal data*. Users are forced to share the information contained in their identity document with the website that they may have otherwise been browsing anonymously, or tied to a pseudonymous identity. Users will have to make a difficult choice between accessing content and sharing sensitive data.
- *Secondary data use*. If a user provides their identity document for age verification purposes, secondary uses of identity data by the website, such as for advertising or tracking, would be unexpected.
- *Cross-site tracking.* Identity information makes it easier for websites to link a user's activity across other websites, or to data from data brokers.
- *Threat of data breach*. Collection of identity documents and photos will create a database of users identity information and photos alongside account activity. This sensitive identity data can be very desirable to breach. Even websites or entities with sophisticated security practices have seen large-scale data breaches. Many smaller websites lack the resources to build sophisticated security practices and are even more at risk.

Privacy Principles

To mitigate these privacy risks, alternative approaches should consider the following:

i. Data minimization. The first aspect of data minimization is that websites without age-based restricted content should not request proof of the user's age. This is discussed further in (iv).

Second, if a website does contain age-based restricted content, the website only needs to learn whether or not a user is at or above the relevant age threshold of the restriction, not *who* the user is, or even when specifically they were born. Thus, a true/false value should be the extent of what a user needs to share with a website to access age-restricted content. Users should also be able to decline to provide any age information; websites should be prepared to offer an age-agnostic experience to those users who chose not to verify their age.

Zero Knowledge Proofs (ZKPs)[1] are a compelling technical solution for this aspect of data minimization in age verification. ZKPs output a forgery-resistant way for a user to prove that their age verification data exists without providing the input data directly to the consuming party— the ZKP can simply output a true/false value as to whether a user's age is above a threshold. Still, when receiving age threshold values, websites may be able to recover a user's exact birth date by observing the true/false value change over time over subsequent site visits. Rate limiting websites' requests for age information would be one mitigating approach. Another mitigation would be to use alternative dates as the reference point for a user's age (such as first visit to that particular site) and report whether a user satisfies the age requirement relative to that reference point. Users would still need a mechanism to provide a site with their age if this strategy denied them rightful access to certain content, but this strategy would help minimize birth date inferences from the majority of websites.

ii. Separation of verification. If sensitive information such as birth date and other identity information is needed to meet age verification requirements, users should be able to minimize the total number of parties with whom that sensitive information is shared. Thus, it may be beneficial for some party other than the direct website the user is attempting to access to preform the data collection step for verification. Centralized verification providers can introduce their own risks of involving a potentially unrelated entity for users to trust with their personal data and posing additional tracking risks, as discussed in (iii).

iii. Unlinkability for tracking prevention. To avoid directly sharing data to verify age with websites, centralized age verification providers are an alternative. However, if centralized age verification providers learn which website is requesting verification of an individual, or learn which website consumes a verification token they issue, verification providers can create a log of websites accessed by an individual. To avoid this risk of cross-site tracking, centralized providers must be prevented from learning what websites or content users accessed (or attempted to access). If websites receive unique age verification tokens, they could still report back to the issuing provider that a particular token was used on their site. It is therefore necessary that whatever a user presents to a website to verify their age be unlinkable from anything they have received from

[1] https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html

a centralized verification provider. This can be achieved in a number of ways. A user might generate a single-use zero-knowledge proof for each verification request, either directly from a backing identity document or by proving possession of an issued age verification token. Because a centralized provider never sees this proof, it cannot be used to track the user's activity. Alternatively, verification providers could be required to implement a blinded token scheme[2], where the user can mathematically randomize the tokens they were issued before presenting them to a website. Since the resulting token is unrecognizable to the verification provider, it also cannot be used for tracking.

iv. Anti-abuse safeguards. There needs to be some mechanism that prevents websites from making users report whether they meet an age verification threshold when it is not required. If browsers were to automatically respond to a website's request for a user's age threshold, it would serve as an additional user fingerprinting vector for websites to track users. Browsers should also refrain from indicating to websites the types of or presence of digital verification mechanisms available on a user's device, which could also be abused by websites for fingerprinting.

v. Control and transparency. Users must be able to control whether they share age-related data with websites and which data they share. Users should also have transparency about what specific data is shared. If an underage user is connected to a parent account, the parent account should be able to elect whether the user's age range is shared with websites.

vi. Low-impact solutions when possible. Designs for age verification on the web must consider that resourced, motivated individuals will be able to circumvent age-based restrictions. Thus, for the many cases in which preventing inadvertent, unwanted exposure to sensitive content is a primary goal, lightweight solutions that do not require providing sensitive identity documents should be favored.

Conclusion

Protecting user privacy while satisfying age verification requirements necessitates thoughtful design to avoid risks of cross-site tracking, re-identification, opportunistic data use, and data breaches. Slightly different solutions may be viable in different regulatory landscapes. Minimizing data that is collected, exposed, and linkable at each layer of a supporting architecture remains a guiding principle, and lightweight solutions that may be as effective as more privacy-invasive approaches should not be overlooked.

---

[2] https://datatracker.ietf.org/doc/html/rfc9576