Age Verification Harms Users of All Ages

Online child safety is a complex issue. Many recent proposals have tried to require platforms to verify users' ages in order to see various types of content or access critical services. But without fail, these "age assurance," "age verification," or "age estimation" systems hurt user privacy and increase the risks of identity theft.

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."

Solutions often involve offering a variety of age determination options, but this only glosses over the fact that every solution has serious privacy, accuracy, or security problems. This puts the burden on the 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.

Age Verification Systems are Surveillance Systems

This applies to all users: Age verification laws don't just impact young people. It's necessary to confirm the age of *all* website visitors in order to exclude one select age group.

The most common method of age verification, collecting ID online, is fundamentally different—and more dangerous—than in-person ID checks in the physical world. Online ID checks are not just a momentary display: They require adults to upload data-rich, government-issued identifying documents to either the website or a third-party verifier, and so create a potentially lasting record of their visit to the establishment.

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.

Age Verification and Data Theft

The more information a website collects about visitors, the more chances there are for such data to get into the hands of a criminal or other bad actor, a marketing company, or someone who has filed a subpoena for it. So-called "anonymized" data can be reassembled to identify individuals, especially when it consists of data-rich government ID together with browsing data like IP addresses.

Data breaches are a fact of life. Once governments insist on creating these ID logs for visiting websites with certain types of content, those data breaches will become more dangerous for users, leaving them vulnerable to phishing, blackmail, or identity theft, in addition to the loss of anonymity and privacy. Requiring users to upload government documents—some of the most sensitive user data—will hurt all users.

Want more information? Please contact Director of Federal Affairs India McKinney at **india@eff.org**.