# Summary of 2023 State Online Age Verification Laws

The 2023 state legislative sessions ushered in the passage of several proposals that seek to implement broad sweeping age verification requirements for certain online services. On March 23, 2023, Utah Governor Spencer Cox (R) signed SB 152 into law, which goes into effect on December 31, 2023. Subsequently, on April 11, 2023, Arkansas Governor Sarah Huckabee Sanders (R) signed similar legislation, SB 396, which was set to become effective on September 1, 2023. However, a federal judge from the U.S. District Court for the Western District of Arkansas recently blocked the law from going into effect while the *NetChoice v. Griffin* case progresses through the legal system. Lastly, on June 28, 2023, Louisiana Governor John Bel Edwards signed SB 162, which goes into effect July 1, 2024. Below, we provide a summary of the overarching trends and associated impacts encompassed by these laws.

## Covered Entities: To Whom Do These Laws Primarily Apply and Which Users Would Be Impacted?

- **"Minor":** an individual under 18 (Note: for Utah, this does not include a minor who has been emancipated or married). This definition is a departure from the federal Children's Online Privacy Protection Act (COPPA) which provides that a minor is a child under 13 years of age.
- **"Social Media Company":** a person or entity that provides a social media platform that has at least 5,000,000 account holders worldwide and is an interactive computer service. (Note: the Arkansas law includes several exemptions to this definition, making it difficult to understand to whom the bill applies).
- **"Social Media Platform":** an online forum that a social media company makes available for an account holder to create a profile, upload posts, view posts of other account holders, and interact with other account holders or users.
    - ***Note:*** None of these Acts provide the definition of a parent or legal guardian.

## Requirements and How Impacts Affect Users: Verification, Consent, and Access

| Requirement | Impact |
|---|---|
| **Age Verification:**<br>Prohibits a social media company from allowing a minor to be an account holder without the express consent of a parent or guardian. Additionally, social media companies must verify the age of an existing or new account holder. | None of these Acts provide a specific definition of age verification but provide broad examples of what could suffice (i.e., "commercially reasonable efforts"), including through the use of a driver's license, parental consent, credit cards, etc. Some third-party vendors offer age verification services, though it remains unclear if any can satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population, and; 3) respecting the protection of individuals' data, privacy, and security. Verifying a user's age would inevitably require the collection of additional sensitive data which creates data privacy concerns and security risks. |
| **Parental Consent/Parental Access:**<br>Requires a social media company to provide a parent or guardian who has provided consent for a minor account holder with access to the account to view all posts made by the minor account holder, and all responses and messages sent to or by the minor account holder. | A parent or guardian must give express consent for their child to have an account on a social media platform. However, there is no explanation of how a company can verify the relationship between a young user and the consenting adult, especially if the consenting parent or guardian does not have an account. |

| | |
|---|---|
| **Limited Hours of Access for Minors/"Curfew":** Requires a social media company to prohibit a minor account holder from accessing the account between 10:30 PM and 6:30 AM. Requires a social media company to provide a parent or guardian with options to access the account and change or eliminate the time restrictions and set a daily time limit for account use by the minor account holder. Note: this is a Utah-only provision. | Such restrictions on access to information online could serve as an impediment to users seeking communities of support and raise concerns about vulnerable users (i.e., children in abusive households or those without access to supportive communities in their physical location). Relatedly, such provisions raise First Amendment concerns by limiting access to lawful speech. |

## Pending Litigation

- ***NetChoice v. Bonta:*** In 2022, California enacted AB 2273, the Age-Appropriate Design Code Act (AADC), a sweeping restriction that requires websites to try to determine their users' ages. NetChoice filed a complaint against California Attorney General Rob Bonta (D) on December 14, 2022. The Northern District of California issued its decision on September 18, 2023, granting NetChoice's request for a preliminary injunction.
- ***NetChoice v. Griffin:*** In 2023, Arkansas enacted SB 396 which mandates that leading websites verify the identity and age of users. NetChoice filed a complaint against Arkansas Attorney General Tim Griffin (R) on June 29, 2023. The Western District of Arkansas issued its decision on August 31, 2023, granting NetChoice's request for a preliminary injunction.

## Trade-Offs, Guiding Principles, and Best Practices

While various age assurance methods, such as age verification and parental consent, are available, each approach comes with its own set of challenges and trade-offs. For instance, more accurate methods often require the collection of additional personal data, potentially conflicting with a service's privacy commitments to users and legal obligations. Mandates to collect and retain additional sensitive information about users creates serious and unnecessary cybersecurity risks for organizations and users. These methods can also lead to disparities among users, particularly for those lacking eligible government-issued IDs or access to financial institutions necessary for verification, potentially discriminating against specific demographic groups. Further, smaller companies may lack the financial resources to implement such verification frameworks. Enhancing confidence in the knowledge of a specific user's age causes implications for safeguarding their privacy rights, ensuring their access to information, and preserving their freedom to engage in digital experiences without constraints.

The Digital Trust & Safety Partnership (DTSP), a group of leading technology companies committed to developing industry best practices verified through internal and independent third-party assessments, recently released a first-of-its-kind initiative aimed at promoting a safer and more trustworthy internet which includes guiding principles and best practices for age assurance online. DTSP identified overarching age assurance principles and practices that may be deployed as part of the overall DTSP Best Practices Framework. The recommended five guiding principles are:

1. Identify, evaluate, and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

2. Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches.

3. Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.

4. Conduct layered enforcement operations to implement age assurance approaches.

5. Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.