

The Future of Privacy Forum (FPF) writes to share our analysis of how proposed legislation on social media regulation in Utah would impact the Utahns' privacy. FPF is a nonprofit organization dedicated to advancing principled data practices in areas such as youth and education privacy, and FPF recognizes that Utah is often a leader in passing privacy legislation.

The federal law that regulates the privacy of children under 13, the Children's Online Privacy Protection Act (COPPA), requires a website or service to obtain verifiable parental consent before collecting personal information from a child when a service is directed to children or the site has actual knowledge that children are accessing a website. Utah's proposed legislation would go beyond the requirements of COPPA to require some companies to affirmatively require parental consent before teens may open an account, as well as require companies to verify the age of all Utah residents.

FPF agrees that kids and teens deserve heightened protections online, but both the parental consent and age verification components raise serious questions about how the proposed rules could create privacy risks for adults, teens, and kids.

While COPPA applies to many websites and services, Utah's proposed legislation applies to social media companies operating social media platforms. As written, it may be difficult for companies to determine whether they meet the definition of social media company or whether the service they offer falls into the definition of social media platform. Uncertainty in the scope of this bill may undercut compliance efforts.

Parental consent under COPPA has longstanding challenges:

FPF published an [analysis](#) and [accompanying infographic](#) regarding verifiable parental consent (VPC) under COPPA, which was informed by research and insights from parents, COPPA experts, industry leaders, and other stakeholders. The white paper and infographic highlight key friction points that emerge in the VPC process, including:

- **Efficacy:** It can be difficult to distinguish between children and adults online, and it is harder still to establish whether a particular child is related to a particular adult. While the approved methods under VPC may confirm someone is an adult, they do not confirm whether that adult is a parent or guardian of a child.
- **Privacy and security:** Parents often do not feel comfortable sharing sensitive information, such as their credit card or ID information, and having that information linked to their child's presence online.

Age verification requires additional data collection:

As written, Utah's proposed legislation requires companies to affirmatively verify the age of all Utah residents. A key pillar of privacy legislation and best practices is the principle of data minimization and not collecting information beyond what is necessary to provide a service. Requiring social media companies, or their agents to collect this data increases the risk of identity theft resulting from a data breach. We also note that since some social media companies are based outside of the United States (with some located in jurisdictions that have few, effective privacy rules), there is an inherent security risk in increased collection of sensitive data for age verification purposes.

Additionally, as written, Utah's proposed legislation specifies that ages must be *verified* without a definition of what "verify" means. Companies would benefit from clarity on whether age verification or age *estimation* is required. An example of age estimation might include capturing a "selfie" of a user to estimate the user's age range. Verifying someone's exact age almost always requires increased data collection compared with estimating an age range or age bracket. Some of the current age estimation technology can accurately distinguish a 12 year old from someone over 25, resulting in a much smaller number of users that would be required to provide sensitive identity documentation. Although methods of verification and forms or methods of identification will be established by further administrative rulemaking, compliance with the proposed legislation as written may still necessitate companies to require government-issued ID to access their services.

Protecting children and teens online should include increasing privacy protections:

FPPF knows that children and teens deserve privacy protections and has highlighted Utah's leadership in this space, [notably in the education context](#). However, a one-size-fits-all approach may not be appropriate given developmental differences between young children and teens. Similarly to how children under 13 can access services with safeguards under COPPA, teens stand to derive benefit from online services such as socializing with peers, distant family, and communities. Utah's legislation proposes to restrict access to services rather than enhancing privacy protections on these services that not only benefit children, but could benefit adult consumers as well. Because many parents may ultimately choose to provide consent, it is important to consider how privacy protections could be implemented on online services.

Last year, Utah passed the Utah Consumer Privacy Act. While the Utah Consumer Privacy Act creates some new rights for Utah residents, it provides fewer protections than other state frameworks. Adding these protections would not just help Utah align with other states but also would address several of the privacy issues the social media bills present. Furthermore, improving upon this law could increase privacy protections for all consumers, regardless of their age. Examples of these provisions include:

- Classifying children's and teens' data as sensitive data, and restricting the sale or use of children and teens' data for targeted advertising by default;

- Adding provisions requiring data minimization, restrictions on secondary uses, or any prohibition against processing personal data in violation of state and federal anti-discrimination laws; and
- Providing all consumers with a right to opt out of profiling.

Please reach out if you would like to discuss FPF's analysis of this legislation. We welcome further opportunities to provide resources or information to assist in this effort. If you are planning meetings to get stakeholder input, we would appreciate an invitation to to discuss further.

Best,
David Sallay
Director, Youth & Education Privacy