Digital Age Assurance Act (DAAA): Frequently Asked Questions

Last Updated: October 25, 2024

Table of Contents:

1. **What is device-based age verification?**
    a. Device-based age verification is an age verification method in which a user verifies their age once through their device's operating system. The user's age is then securely stored on the user's device within the operating system.
    a. A user would verify their age at the time of device activation, or through Operating System (OS) updates for devices sold prior to the effective date.
    b. When a user attempts to access a website, application, application store, or online service that requires age verification, the user's operating system would share a user's verification status with the applicable website, application, application store, or online service through a secure application programming interface (API). The API would then provide the website, application, application store, or online service with a response on whether the user meets the defined age requirement thresholds to access the platform.

2. **Who is required to comply under the Digital Age Assurance Act?**
    a. Under the proposed Digital Age Assurance Act, Covered Manufacturers, websites, applications, and online services are required to comply.
        i. Covered Manufacturers are defined as the manufacturer of a device, an operating system for a device, or an application store, and are required to take commercially reasonable and technically feasible steps to determine or estimate the age of the device's primary user. Covered Manufacturers are also required to provide websites, applications, application stores, and online services with a digital signal regarding the device user's age threshold via a real-time application programming interface ("API").
            1. If the Covered Manufacturer is an application store, the application store must obtain parental or guardian consent prior to permitting an individual under sixteen years of age to download an application from the application store.
            2. The application store must also provide the parent or guardian with the option to connect with the developer of an application for the purpose of facilitating parental supervision tools.
        ii. Websites, applications, or online services that make available mature content are required to recognize and allow for the receipt of digital age signals.
            1. Websites, applications, or online services that make available a substantial portion of mature content are required to block access to individuals indicated as under eighteen years of age.
            2. Websites, applications, or online services that knowingly make available less than a substantial portion of mature content are required to block access to known mature content to individuals indicated as under eighteen years of age.
        iii. Application stores are required to recognize and allow for the receipt of digital age signals to determine whether an individual is under sixteen years of age, and obtain parental or guardian consent as described in the above Covered Manufacturer requirements.

3. **What are the proposed enforcement mechanisms?**
    a. It's important to understand that the proposed Digital Age Assurance Act language may differ state-by-state, and as such, enforcement actions should be determined within each jurisdiction. The enforcement mechanisms outlined within the Digital Age Assurance Act include the following:

i. If the state believes an entity is in violation of the age verification requirements, including Covered Manufacturers, websites, applications, and online services, the state may provide an entity with written notice of specific violations. If the entity does not respond to the state or continues to violate the act in breach of an express written statement, the state may bring an action and seek damages against the entity.
    1. Within the action, the state may collect a civil penalty of up to $10,000 per violation.
    2. The state may alternatively seek damages for up to $2,500 per each minor actually harmed in violation of the act.

ii. Covered Manufacturers that have taken commercially reasonable and technically feasible steps to determine or estimate the age of the device's user, are not subject to liability.

4. Why is U.S.C. 2256(2)(A) referenced?

a. Within the Digital Age Assurance Act, "mature content" is defined as U.S. Code 2256(2)(A), which is the federal code definition for "sexually explicit conduct" and is defined as:

i. Except as provided in subparagraph (B), "sexually explicit conduct" means actual or simulated -
    1. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
    2. Bestiality;
    3. Masturbation;
    4. Sadistic or masochistic abuse; or
    5. Lascivious exhibition of the anus, genitals, or pubic area of any person.

ii. This code was specifically included within this legislation to provide a standard definition that can be consistently referenced across various states. Additionally, U.S.C. 2256(2)(A) is inclusive and is non-descriptive towards an individual or group's sexual orientation or identity.

5. Is device-based age verification considered Constitutional?

a. Unlike alternative age verification methods, device-based age verification is considered Constitutional because it neither burdens users nor requires the disclosure of identity or other personal information in order to access mature content, and no Constitutionally protected speech is impeded.

b. For a full analysis on the Constitutionality of device-based age verification, please refer to the 'Digital Age Assurance Act Constitutional Analysis.'

6. **There are age verification bills already, why aren't we just relying on those?**
    a. In the United States, there are currently 19 bills that have been passed requiring age verification for mature content. States with laws currently in effect include: Arkansas, Idaho, Indiana, Kansas, Kentucky, Louisiana, Montana, Mississippi, Nebraska, North Carolina, Texas, Utah, Virginia, and Alabama.
    b. The existing age verification laws pose significant concerns to user data privacy and security, present Constitutional challenges to First Amendment free speech rights, dissuade proper platform compliance and enforcement, and can lead to negative outcomes from unintended user behavior.
    c. Age verification solutions must be properly implemented to achieve the primary goal of protecting children while simultaneously preserving the privacy and Constitutional rights of adult consumers.
    d. As such, there is a significant need for legislation that places the age assurance mandate at the source, on the device, to resolve these challenges. Device-based technology as a method of age verification is technically feasible to implement and relies on elements that are already common practice across industries. Device-based age assurance verifies a user's age through their device's operating system and shares the user's verified age or age range with the application, service, or website the user is attempting to reach.
    e. By standardizing age verification on the device-level, users would no longer be required to provide personal information or PII numerous times across multiple platforms, significantly reducing the risk of misuse, data breaches, and overall concerns for data privacy. In turn, device-based age verification encourages compliance across websites, applications, and online services and significantly reduces opportunities for bypass, eliminating circumstances in which a minor circumvents the anticipated protections by finding ways to access adult content through simple actions like using a basic VPN service, or by accessing non-compliant sites. This creates a safer, privacy preserving approach to age verification that achieves its central goal in protecting children, while also addressing the various Constitutional and compliance challenges posed by existing iterations of current legislation.

7. **How does device-based age verification impact current social media bills?**
    a. Existing social media bills are separate from existing age verification bills for adult content; however, both contain a requirement for entities to verify the age of the user attempting to access their website or service.

b. The verification mechanism proposed by device-based age verification can be leveraged by both social media companies and adult content websites in order to fulfill applicable age verification requirements. Rather than requiring a user to verify their age on a per-platform basis, device-based age verification centralizes the user's point of verification. This allows users to reduce the amount of personal information provided across platforms, including both social media and adult content websites.

8. **What types of devices does the Digital Age Assurance Act apply to, and how would this work for laptops?**
    a. The Digital Age Assurance Act would apply to all devices that are designed for and capable of communicating across a computer network for the purpose of transmitting, receiving, or storing data, including, but not limited to, a desktop, laptop, cellular telephone, tablet, or other device designed for such purpose.
    b. Desktop computers and laptops run on an operating system, such as Google (Android), Apple (macOS/iOS), or Microsoft (Windows), and device-based age verification can be implemented through the operating system at the profile level set-up. This allows for device-based age verification to work with the integrated security processes in place for accessing desktop and laptop computers, including shared devices with multiple accounts or profiles.

9. **Does the Digital Age Assurance Act offer protections on the app store level?**
    a. The Digital Age Assurance Act requires application stores to receive the digital age signal regarding whether an individual is under the age of thirteen, at least thirteen years of age and under sixteen years of age, at least sixteen years of age and under eighteen years of age, or at least eighteen years of age. The application store would receive the digital age signal from the device's operating via the same real-time API integration required for websites, applications or online services.
    b. If the device's user is under sixteen years of age, application stores would be required to obtain parental or guardian consent prior to permitting an individual to download an application from the application store. Additionally, application stores would be required to provide the parent or guardian with the option to connect to the developer of the downloaded application for the purpose of facilitating parental supervision tools.

10. Why is a "commercially reasonable" method of age verification so broad?

a. Covered manufacturers are required to take commercially reasonable and technically feasible steps to determine or estimate the age of the device's user upon device activation.

b. Given the ever-evolving state of technology, providing the option for a "commercially reasonable method" of age verification allows Covered Manufacturers to deploy verification methods in line with their existing processes and technology. Many major device manufacturers, such as Google and Apple, have already integrated age verification processes in their standard device setup practices. Rather than outlining stringent, narrowly defined requirements for age verification, "commercially reasonable" methods allow the trusted handful of Covered Manufacturers to implement processes conducive to their existing system, and therefore allows for the seamless implementation of device-based age verification.

11. What would be the fiscal impact of a proposed bill?

a. The Digital Age Assurance Act would allow the enforcing body to seek civil damages and issue fines for Covered Manufacturers or websites, applications, application stores, or online services found in violation. These fines may total up to $10,000 per entity found in violation of this act, or up to $2,500 per each minor harmed in violation of the act.

b. Enforcement costs are anticipated to be very low as investigation could be conducted through API implementation check, which would include scanning websites, applications, application stores, or online services on a mass scale for the appropriate API integration. Violations identified during the investigations would largely fund any associated costs of enforcement. Note the fiscal impact of a proposed device-based age assurance bill may vary across states, depending on how the enforcing agency implements the existing violations.

12. What if an individual does not have the proper documentation to verify their age?

a. As with all legislation, accommodations are made for exceptions (limitations for the undocumented also exist with platform-level age verification). The commercially reasonable method of age verification should allow Covered Manufacturers to determine different methods of verification, from government-issued identification cards to age estimation technology. At present, these are potential options for age verification:

   i. Documentation: If the Covered Manufacturer allows for government-issued documentation, it can be any government document, including a foreign ID.

ii. Technology: If the individual attempting to verify does not have any government-issued identification, a Covered Manufacturer could employ existing technologies, such as age estimation technology..

b. It's important to note that age verification is not identity verification, and with existing technology capabilities it is possible for Covered Manufacturers to tie an age to an individual's account without knowing the identity of an individual.

13. What happens if a user does not want to verify their age upon device activation?

a. The Digital Age Assurance Act would require all users to verify their age upon device activation, or during OS updates for devices sold prior to the effective date. If a user's age is verified as under eighteen or another applicable age threshold, the user would not be permitted to access websites, applications, or online services that require age verification.

14. If the device is indicated as a child device, how is an application store expected to receive verifiable parental consent?

a. Application stores would be required to implement a reasonably designed, technically feasible method for receiving verifiable parental consent, similar to how manufacturers of devices or operating systems are required to take commercially reasonable and technically feasible steps to verify a user's age.

b. The Digital Age Assurance Act does not prescribe a specific method for receiving parental consent so that application stores may design and deploy a mechanism that is best suited to their existing technology. Note that Covered Manufacturers or websites, applications, or online services will still be required to comply with separate, federal regulations regarding parental consent not associated with the Digital Age Assurance Act.

c. Several existing U.S. federal privacy laws suggest acceptable methods to obtain verifiable parental consent, including:

i. Having the parent provide a copy of a government-issued ID that can be checked against a database.

ii. Having the parent use a credit or debit card to make a transaction, which notifies the account holder.

iii. Having the parent answer a series of knowledge-based questions.

iv. Having the parent call a toll-free number staffed by trained personnel.

////