Where Enforcement Happens

Julia Hanson

October 2025

Four related questions

- What entity is responsible for whether age restricted content is shown to an end user?
- What entity is responsible for determining whether content is age restricted?
- What entity is responsible for performing the age verification step?
- What entity is responsible for determining what jurisdiction an end user is in?

Definition of Roles

- Verifier: determines whether a user is above the relevant age threshold
- Enforcer: responsible for technical restriction of access to age-restricted content
- Jurisdiction detector: determines whether a user belongs to a legally relevant audience
- Content rater: determines whether content on a website requires age restriction

Possible Components

- Device / OS
- Browser App
- Website/Service
- 3p Verification Service

Service vs. Device enforcement

- **Service-enforced:** services responsible for not delivering age-restricted content to users unless they verify their age
  - Example: User provides age verification inputs directly to website
- **Device-enforced**: devices responsible for not displaying age-restricted content to users unless they verify their age
  - Example: OS-provided age/content preference setting

https://www.ietf.org/slides/slides-agews-paper-who-bears-the-burden-technical-architectures-for-age-based-content-restriction-00.pdf

Dimensions of Evaluation

- Usability (by end users)
- Privacy
- Ease of adoption (by services)
- Effectiveness
- Centralization risk
- Modifiability

Advantages of device-enforced scheme

Possible arguments

- Usability: one-time age verification; no additional friction per-website
- Ease of adoption: cheaper and easier than website based scheme; websites do not need to individually support age verification techniques or handle age threshold data
- Privacy: websites not exposed to age verification inputs; limits user tracking and fingerprinting risk
- Effectiveness: Users can switch devices less easily they can swith websites to access content
- Modifiability: can suit a diversity of age restriction policies

Advantages of website-enforced scheme

Possible arguments

- Centralization:
  - Users remain in control of their owned device’s behavior
  - Users not required to share age (and potentially identity) information with high-impact device account
- Usability and access: withstands complexities of shared device setups
- Effectiveness: no coordination needed between content distributors and device vendors; same entity responsible for publishing and access control

Some Example Architectures

1. User directly verifies age with each website they visit that contains restricted content
2. User verifies age with a 3p identity provider using a ZKP that then issues them tokens that are then presented to websites as age assurance for subsequent site visits
3. User verifies their age at the device-level with their device provider; device age settings are then propagated to the browser; browser only displays age restricted content to verified users: content rating responsibility could fall to either client or website
4. User verifies their age at the device level with their device provider; browser vends answers to age threshold queries via API

Questions for Discussion

- Do device-enforcement solutions require to service-side content labeling, e.g., <meta name= “rating”>? Or are they compatible with other content rating mechanisms, e.g., on-device detection?
- Do enforcement responsibilities also encompass location/jurisdiction detection?
- Which goals/values may be in tension with the end-to-end principle?
- How would a device-enforcement solution facilitate multi user configurations (e.g., household computer), or public/shared device configurations (e.g., library computer)?
- How could device-enforcement solutions preserve users agency and ownership of their own devices?