Joint statement of security and privacy scientists and researchers on Age Assurance

ISOC LIVE -- March 2, 2026

Signatories: ~390 security and privacy scientists and researchers from approximately 30 countries

Source: *https://www.patreon.com/posts/joint-statement-152079448*

Overview

A coalition of nearly 400 security and privacy researchers released a joint public statement addressing the rapid global push toward mandatory online age-assurance systems. The letter responds to legislative and regulatory initiatives in multiple jurisdictions that would require users to verify or estimate their age before accessing social media platforms, online services, websites, or AI tools.

While affirming the importance of protecting children from online harms, the signatories argue that current age-assurance proposals are technically immature, insufficiently studied, and likely to introduce serious privacy, security, and equity risks. They call for a moratorium on broad deployment until stronger scientific evidence and safeguards are established.

What Is Being Proposed Globally

Governments are increasingly considering or adopting systems that require:

- Age verification (proving age via official documents or digital identity systems)
- Age estimation (using biometrics such as facial analysis)
- Age inference (analyzing behavior or other data to infer age)

These systems would often apply universally — meaning all users, not only minors, would need to prove or estimate their age to access ordinary online services.

The researchers emphasize that such measures would represent a structural transformation of the Internet's access model, moving from largely open access to identity-conditioned participation.

Core Concerns Raised by the Signatories

1. Lack of Scientific Consensus on Effectiveness

The letter states that there is no clear scientific consensus that age-assurance technologies will significantly reduce harms to minors.

Researchers caution that harms such as exposure to inappropriate content, harassment, or exploitation are complex social problems unlikely to be solved through identity gating alone. The authors argue that policymakers are advancing sweeping mandates without robust empirical evidence demonstrating net benefit.

2. Technical and Practical Limitations

The signatories highlight that age-assurance systems are vulnerable to circumvention through:

- VPNs
- Borrowed credentials

- AI-generated images or spoofing tools
- Cross-border service access

They warn that building interoperable, global digital age-verification infrastructures would be highly complex and unevenly implemented across jurisdictions. Such systems could create fragmented or inconsistent enforcement regimes.

3. Privacy and Security Risks

Age-assurance mechanisms may require the collection and storage of sensitive data, including:

- Government IDs
- Biometric information (facial scans, behavioral signals)
- Device or behavioral profiling data

The researchers argue that mandating such systems expands the surface area for data breaches, surveillance, and misuse.

They also note that weakening anonymity and restricting privacy tools could chill free expression and increase vulnerability for journalists, activists, and marginalized communities.

4. Discrimination, Bias, and Exclusion

AI-based age-estimation systems may exhibit demographic bias, leading to disproportionate error rates across race, gender, disability, or other characteristics.

Additionally, requiring formal identification may exclude or burden:

- Migrants or undocumented individuals
- Elderly users
- People without access to smartphones or digital IDs
- Individuals in lower-income or rural communities

The letter warns that age-assurance mandates could deepen digital inequality.

5. Broader Structural Impacts on the Internet

The signatories caution that universal age gating may normalize identity-linked access to online participation. Over time, this could:

- Reduce anonymous speech
- Expand surveillance capabilities
- Shift the Internet toward credential-based participation
- Create long-term governance precedents affecting civil liberties

They stress that these structural effects require careful democratic debate before implementation.

Call for a Moratorium

The researchers urge policymakers to pause broad deployment of age-assurance mandates until:

- Independent research demonstrates clear net benefits
- Technical safeguards are validated at scale
- Privacy-preserving designs are proven effective

- Trade-offs are openly debated

They frame this not as opposition to child protection, but as a call for evidence-based policymaking grounded in security, privacy, and human rights principles.

Conclusion

The joint statement presents a unified message from the security and privacy research community: large-scale age-assurance systems represent a fundamental redesign of Internet access, and current proposals risk unintended consequences that may outweigh their intended protections.

The signatories advocate for caution, further study, and public deliberation before embedding mandatory age-verification infrastructures into the core architecture of the digital ecosystem.