
Policy Statement

Open Letter on Mandatory Age Assurance

11 May 2026

DOI: 10.5281/zenodo.20117733

Informatics Europe represents about 200 institutes and more than 50,000 researchers in Informatics in Europe and neighbouring countries. We express serious concerns regarding current proposals to introduce **mandatory age assurance requirements for individuals accessing online services**.

We fully share the goal of protecting children from harmful online content. Well-being and safety of minors in the digital environment are priorities for families, educators, researchers, industry, and policymakers alike. However, the current proposals to mandate large-scale age assurance systems – whether through identity verification, biometric estimation, or behavioural inference – raise significant **technical, legal, psychological, and societal challenges**.

Based on existing research, technical analysis, and international experience, we believe that **mandatory age assurance applied broadly across internet services risks undermining privacy, security, equality, and digital inclusion while offering uncertain benefits for child protection**. We therefore urge policymakers to proceed cautiously and adopt an evidence-based approach before imposing such systems at an internet scale.

Technical Feasibility and Circumvention

Age assurance systems typically rely on one or more of three approaches: age verification (using identity credentials), age estimation (using biometric analysis such as facial recognition), or age inference (using behavioural signals and online activity). Each approach presents significant technical limitations.

First, these systems are **easily circumvented**. Experience from existing deployments shows that users can bypass age checks through VPNs, borrowed credentials, purchased accounts, or alternative services that do not enforce verification. As verification becomes more widespread, new markets for circumventing these mechanisms quickly emerge. The resulting dynamic creates a technological “arms race” between regulators and users that is unlikely to produce reliable outcomes.

Second, biometric and algorithmic age estimation methods remain **technically unreliable**. AI-based age prediction systems can exhibit high error rates and documented bias across demographic groups.

Environmental factors such as lighting, facial appearance, or camera quality further affect accuracy. As a result, legitimate users may be incorrectly blocked while determined users continue to bypass controls.

Third, effective age verification would require a **global trust infrastructure capable of verifying age credentials across platforms, jurisdictions, and devices**. Building such infrastructure securely is an enormous technical undertaking. Comparable global systems for internet security have taken decades to deploy and remain imperfect today. It is unclear whether a reliable and interoperable age verification infrastructure can realistically be implemented in the near future.

Without resolving these technical challenges, mandatory age assurance risks becoming a mere symbolic intervention that provides limited real protection.

Privacy and Security Risks

Large-scale age assurance systems introduce significant privacy and security concerns.

Unlike offline age checks – where an ID may simply be visually inspected – many proposed online systems require the **collection, processing, or storage of sensitive personal information**, including biometric images, government identification documents, or behavioural data. These processes create new concentrations of sensitive data that may become targets for cyberattacks, misuse, or surveillance.

Mandatory age verification also threatens **online anonymity**, which plays an essential role in democratic societies. Journalists, activists, whistleblowers, and vulnerable individuals often rely on anonymity to seek information, share experiences, or participate safely in public debate. Systems that require identity disclosure for ordinary online activity risk weakening these protections.

Furthermore, enforcement mechanisms may indirectly restrict the use of privacy-enhancing technologies such as VPNs. These tools are widely used to protect communications, secure business infrastructure, and safeguard individual privacy. Policies that discourage or restrict such technologies may weaken cybersecurity and undermine trust in the digital ecosystem.

Inequality and Digital Exclusion

Mandatory age assurance may unintentionally exclude many individuals from participating in digital society.

Verification systems often assume that users possess government-issued identity documents, compatible digital devices, and the skills required to use verification tools. However, not all users meet these conditions. Some individuals may lack suitable identification credentials, may rely on shared devices, or may not have access to the digital infrastructure required by certain verification systems. Others – including visitors from outside the EU or people with limited digital literacy – may encounter additional barriers when interacting with such systems.

Even within the EU, not all citizens possess smartphones or digital identity credentials required for certain verification models. If access to online communication platforms, information resources, or digital communities becomes conditional on such credentials, the result will be new forms of digital exclusion.

Policies that inadvertently limit access to essential online services risk contradicting the EU's objectives of digital inclusion, equal access to information, and social participation.

Psychological and Societal Implications

Beyond technical and legal considerations, mandatory age assurance may also produce broader societal effects.

Age restrictions can create a **false sense of security** if they are easily bypassed. Parents and policymakers may assume that children are protected, while minors may continue to access harmful content through alternative services. At the same time, users may migrate towards less-regulated platforms, where safety protections and moderation are weaker.

Young people also rely on online services for education, information, mental health support, and community engagement. Overly restrictive access controls risk limiting beneficial uses of the internet and reducing opportunities for learning and participation.

In addition, large-scale age-assurance infrastructures may centralise control over **who can access which information or services online**. Systems originally designed to enforce age restrictions could potentially be expanded to regulate access based on other attributes. Such infrastructures raise legitimate concerns about long-term implications for digital freedom and democratic participation.

Lessons from International Experience

Countries around the world are experimenting with age assurance policies. The United Kingdom, Australia, France, Denmark, and several other jurisdictions are exploring or implementing various forms of age verification for online services. Early experience demonstrates that such measures are complex to implement and often face significant challenges in circumvention, enforcement, and privacy.

These international developments show that **no jurisdiction has yet demonstrated a large-scale age assurance system that is both effective and compatible with fundamental rights and digital inclusion**.

Europe should therefore carefully evaluate the outcomes of existing initiatives before mandating similar interventions across the digital ecosystem.

A More Effective Path Forward

Protecting children online requires addressing the structural causes of harm rather than relying solely on identity-based access controls.

Policymakers may achieve greater impact by focusing on measures such as:

- **Safer platform design** – addressing addictive algorithms, harmful recommendation systems, and manipulative design practices.
- **Strong enforcement of existing EU regulations** – including the Digital Services Act and other frameworks that require platforms to mitigate risks to minors.
- **Support for parents and educators** – improving parental tools, digital literacy programs, and guidance for families.
- **Independent research and evaluation** – supporting evidence-based policymaking on children’s digital wellbeing.
- **Privacy-preserving innovation** – encouraging research into technical approaches that minimise data collection while supporting legitimate protections for minors.

These strategies focus on the **sources of harm rather than the identity of users**, and therefore offer a more sustainable path toward safer online environments.

Conclusion

The protection of children online is a legitimate and urgent priority. However, **mandatory age assurance applied broadly to internet users risks introducing a far-reaching technological infrastructure without sufficient evidence that it will effectively achieve its intended goals.**

Before implementing such systems at an internet scale, policymakers should ensure that any intervention is:

- technically feasible
- demonstrably effective
- compatible with fundamental rights
- inclusive and accessible to all members of society

Europe has long been a global leader in developing digital policies that balance innovation, safety, and fundamental rights. We encourage policymakers to continue this tradition by pursuing child protection strategies that are **evidence-based, proportionate, and respectful of privacy, security, and democratic values.**

About Informatics Europe

Informatics Europe represents the academic and research informatics community in Europe and neighbouring countries by uniting close to 200 member institutions and connecting over 50,000 researchers in informatics and related disciplines from more than 30 countries. Its mission is to empower and unite the European informatics community, establish common positions, take action on shared priorities, and support policy-making in informatics education, research, and its social impact across Europe. Informatics Europe has previously responded to European Union public consultations on European digital principles, artificial intelligence and the European strategy for data. Informatics Europe is a non-profit organisation.