Age-Based Content Restrictions and the Operational Dependency on Viable Filtering Infrastructure

A Position Paper from SWGfL

Date: 07/07/2025

Prepared for

Internet Architecture Board, IETF

Written By

Will Earp, David Wright

SWGfL

SWGfL

Safe, Secure, Online

Abstract

This paper sets out the practical considerations for deploying age-based content restrictions in real-world contexts, particularly those affecting children in education and home environments.

Drawing on operational experience across thousands of UK schools and homes, we explore how viable age-based restrictions are fundamentally predicated on the availability of effective, layered content filtering systems.

We also highlight how recent changes to internet protocols (e.g., ECH and DNS-over-HTTPS) are eroding the transparency and enforceability of these systems, raising critical questions about how age assurance can be technically maintained without resorting to device prohibition or invasive surveillance.

1. Introduction

The deployment of age-based content restrictions is increasingly framed as a policy and child protection imperative. However, these expectations must be underpinned by feasible and technically enforceable mechanisms. In schools and homes, content filtering solutions rather than age assurance tokens or verification systems, are the primary tools by which harmful or inappropriate material is restricted according to a user's age. Yet these tools are increasingly undermined by developments in internet protocol design.

This position paper argues that filtering systems remain the de facto infrastructure for age-based restrictions. Without deliberate architectural accommodation for filtering capabilities, standards development risks unintentionally impairing the very protections policymakers and educators rely on.

2. Current Filtering Techniques and Their Constraints

Filtering solutions in schools, homes, and child-facing networks typically deploy a combination of methods, each with distinct dependencies and limitations:

- DNS Filtering: Applies at the domain level but lacks visibility into specific content paths. Easily bypassed via custom or encrypted DNS unless network-level control is maintained
- SNI Filtering: Presents the domain name the user wishes to access in plain text through Server Name Indication (SNI), enabling filtering middleware to filter

requests. Rendered ineffective by ECH, which encrypts the SNI header and undermines domain-based inspection

- Browser Filtering: Achieved via browser extensions, often reliant on device lockdown to ensure users cannot disable or bypass protections. Cannot control content viewed in other applications
- Root Certificate Filtering (TLS Interception): Enables deep packet inspection through man-in-the-middle (MITM) decryption. Only feasible with full device management; fails where applications implement certificate pinning or where CAA DNS records indicate authorised certificate authorities. Hampered by limitations on platform specific API's
- IP Filtering: Crude but sometimes necessary. Applies to IP addresses but is prone to over-blocking due to shared hosting environments and ineffective against CDNs or services with dynamic IP pools

These layered approaches attempt to deliver meaningful protection within a constantly shifting technical landscape. However, each technique is being constrained by emerging protocols and privacy-enhancing standards that deprioritise intermediary visibility.

3. Protocol Evolution and the Challenge to Filtering Viability

Our previous IETF draft (draft-campling-ech-deployment-considerations[1]) illustrated the real-world implications of ECH on school and parental filtering infrastructure. These challenges are not theoretical - they are already affecting safeguarding systems in educational settings where filtering is often a statutory requirement.

The rapid deployment of encrypted DNS (DoH/DoT/DoQ), ECH, and TLS 1.3 makes it technically impossible to distinguish or intercept traffic without full device control, undermining the fundamental assumptions on which age-based content restriction relies.

If network intermediaries (e.g. schools, parents, child-safe ISPs) are no longer able to meaningfully filter, then the remaining options, such as: device bans for under-16s or widespread biometric verification, raise serious feasibility, privacy, and equity concerns.

[1] draft-campling-ech-deployment-considerations-10 - Encrypted Client Hello Deployment Considerations

4. Age-Based Restriction Without Filtering: An Unviable Alternative

If content filtering becomes ineffectual, the alternatives include:

- Device bans for children under a certain age – Already advocated by some groups, this risks social exclusion and increases digital inequality.
- Mandated age verification at the application or content level – These may be invasive and difficult to scale across the global internet. They also often require national infrastructure that does not exist or lacks interoperability.
- Client-based enforcement via secure enclaves or parental controls – These rely heavily on ecosystem cooperation (e.g. OS vendors, browser developers), which remains inconsistent and unregulated.

5. Recommendations and Considerations for IETF

To ensure that age-based content restrictions remain viable, we recommend that the IETF and related working groups:

- Recognise content filtering infrastructure as a legitimate user or network function that should be accommodated in protocol design
- Consider the development of signalling mechanisms that allow clients or intermediaries to declare child-safety policies or network constraints in ways that are privacy-respecting yet enforceable
- Promote greater transparency from client applications (e.g., browsers, operating systems) regarding how they handle content classification, filtering, and parental controls.
- Define age-appropriate meta tags for content to specify the target age range, and minimum age, with guidelines on what types of content is appropriate for each age range.
- Encourage further dialogue with implementers of child-protection systems, particularly those operating in educational or public sector environments.

6. Conclusion

Age-based restrictions cannot be discussed in isolation from the technical means by which they are implemented. Filtering systems are currently the only scalable, moderately privacy-preserving solution in widespread use. Yet these systems are being steadily undermined by changes to protocol architecture that favour end-to-end encryption above all else.

We urge the IETF to consider these real-world implications and to explore protocol enhancements that support, not obstruct, user agency, child safety, and responsible network administration.