Joint Statement: UK policymakers must prioritise addressing the roots of online harm, not undermining the open web

The open Internet is a global public resource that has long since become foundational to the flourishing of individuals, businesses, and societies. Digital technologies and the open web allow us to foster connections, access educational resources, express ourselves, and work together to build a better society. The open web is also an engine for economic growth, innovation and creativity: anyone can build successful services and products, and reach people across the globe. At the core of this openness lie open standards, shared protocols, and interoperability across borders as the default.

This openness and the opportunities it affords are coming under threat in the UK. In attempting to respond to tough questions around online harms, UK policymakers are currently pursuing blunt policy interventions like access bans that will do little to improve young people's experiences online, and instead undermine the web and infringe on human rights.

Now that the Children's Wellbeing and Schools Bill has passed, ministers are consulting on which platforms and specific features should be placed behind age gates as part of a national consultation on online harms. This approach focuses on restricting young people's access, rather than ensuring services are designed to uphold their rights and interests by default. Crucially, even targeted age restrictions of specific features could mean that all users are required to complete intrusive age assurance processes to retain full access. Restrictions under consultation include curfews for young users and wider restrictions on children's access to online services, with implications across internet services from video games, VPNs to even static websites. Implementing such access restrictions hinges on all users having to verify their ages, not just young people, and places the burden on providers to comply in ways they consider appropriate.

As the UK's experiences with age assurance under the Online Safety Act have shown, deploying age assurance technologies at scale comes with significant trade-offs: Existing age assurance technologies are either insufficiently accurate, undermine privacy and data security, or are not widely available across populations. Beyond concerns related to age assurance technologies themselves, mandating their implementation across an ever-expanding list of core internet services undermines the decentralised nature of the web, its accessibility and creates serious new security threats. Specifically, age assurance mandates risk cementing the dominance of gatekeeper app stores, operating systems, and platforms' walled gardens. They also risk turning the web into a patchwork of age-gated jurisdictions, undermining free expression and access to information, rather than a global resource accessible by all. Finally, age assurance technologies create massive data risks for all users, as demonstrated by serious breaches of UK users' government ID data.

The internet is an essential resource that enables young people to engage with the world in a way that transcends their immediate environment, as well as find information they may not feel safe to access offline, such as about family abuse, politics, or their sexuality. At the same time, however, digital spaces can carry risks for different populations, including young people. These risks are real and require

thoughtful policy interventions that address the root of the issue, not just simplistic policies like access bans. Of particular importance is the way that most online spaces are not built with users' rights or choices in mind, but optimised for extracting value for online platforms. Underlying this is often the massive collection of user data used to target, lock-in and surveil users—feeding platforms ads-based business models.

Addressing these harmful practices and holding tech companies accountable for providing safe online spaces that strengthen, not undermine users' choices and agency, must be the priority of UK policymakers. Now is the time to hold tech to account, not undermine the open internet.

Signatories of this letter remain ready to provide expertise, working with policymakers to ensure that measures that aim to keep children safe online are effective, proportional and enable them to exercise all their human rights.

Signatories

- Big Brother Watch
- Defend Digital Me
- Electronic Frontier Foundation
- ExpressVPN
- Gamers Voice
- Global Partners Digital
- Index on Censorship
- Internet Society
- IPVanish
- Mozilla
- Mullvad VPN
- NO2ID
- Open Rights Group
- Privacymatters
- Proton
- Stop Killing Games
- Tor Project
- Tuta
- VPN Trust Initiative