# ONLINE SAFETY BILL

**Briefing to inform the Third Reading debate in the House of Commons on 17 January 2023**

## Unintended consequences of the Online Safety Bill mean a trio of surveillance, prior restraint of speech, and restriction on access to online content and services.

The Bill seeks to protect children online, but its measures' effect extends far beyond the policy aim, with unintended consequences for the whole of society. Government focuses on the content it wants to ban, with little attention paid to the impact on freedom of expression or privacy.

This Bill vastly increases online surveillance of British people without any judicial or administrative oversight. It will institute a de facto "general monitoring" and proactive scanning. This means all users' posts, public and private, every day, all the time. It will force aggressive age-gating via the implementation of AI-driven systems to collect biometric data.

### Flexibility for the government means legal uncertainty for providers and users.

The text's lack of definition or precision leaves wide open loopholes for over-removals of content and the possibility of government-imposed privatised surveillance. Providers and users simply don't know what is intended and are put in a position of legal uncertainty. Given the enormous implications for freedom of expression and privacy rights, this is a deep flaw. It should specify precisely what the government intends, and if the government does not plan any interference with these rights, it should say so on the face of the Bill.

### Trio of Surveillance, not triple-shield

The government's "triple-shield" combines a requirement for online platforms to enforce their terms and conditions ( S.64-67), combined with the safety duty to remove all illegal content ( S.9) , and a new filter button for adult users to block content they don't want to see in their feeds (S.12). The government claims this will protect users from the range of harms set out in the Bill. It also claims the move will protect free

speech. This claim does not stack up, as the underlying censorship framework remains in place.

Providers will determine what is in the filters, giving them enormous control over what people read or view. They will be incentivised to conduct general monitoring and use upload filters in order to "prevent users encountering" illegal content (S..9). The government claims this is not the case but refuses to say so explicitly. Upload filters introduce a form of prior restraint that effectively ban content before publication.

**The strengthened .requirement for age assurance ( S.11 (4))** will make age-gating compulsory with the effect of restricting not only children's access to content but potentially also adults. It will mean providers estimate age, which incentivises a granular collection of highly intrusive data. People will be subject to ever more algorithmic decision-making. Providers may alternatively decide to sanitise content to be suitable for children. This could restrict access to knowledge for all users.

**Chat monitoring Ofcom will be granted unprecedented power (S.110)** to require providers of private chat services, to proactively scan messages. It includes encrypted messaging, and in doing so it will introduce security risks that will affect the whole system. It will impose a form of mass surveillance on more than 40 million people in Britain who use "chat" services. Please see our briefing 'Who's checking on your chats in private online spaces'.

**Furthermore:**

**The scope of the Bill extends to thousands of websites by reaching mandating search companies to reach deep into their listings** ( S.20 - 25).

**Private actors will be asked to judge criminality including the mental element when restricting illegal content. The bar "reasonable grounds to infer" is low** (S.170).

Ministerial interference The Secretary of State's powers have been a concern throughout the process of this Bill. They have the power to set strategic direction and give guidance to Ofcom and other powers detailed throughout the Bill in individual provisions (S.153-157). For example, the power to set the categorisation of services will impact the duties required of individual services. There is currently considerable uncertainty as to how this categorisation will be handled (S.86-88).

**Criminal liability for tech company directors ( amendment NC2 to S.11)** is likely to embed upload filters and a hard form of age verification under threat of jail. Please see our additional briefing on this amendment.

---

**Open Rights Group (ORG)** is the leading UK-based digital campaigning organisation. We work to protect fundamental rights to privacy and free speech online, including data protection, the impacts of the use of data on vulnerable groups, and online surveillance. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK. We have worked in this policy field throughout the 'online harms' processes and consultations, and both Digital Economy Acts (2010 and 2017), accurately highlighting which parts of both DEAs would prove extraordinarily difficult to implement practically or fairly.