JOINT SECOND READING BRIEFING ON THE ONLINE SAFETY BILL FOR THE HOUSE OF LORDS: PRIVATE MESSAGING

JANUARY 2023

The internet is a primary frontier for free expression and the exchange of ideas, and a crucial site of public participation and democratic engagement. At the same time, it has also facilitated the proliferation of hate and oppressive speech, spread of viral propaganda intended to manipulate or undermine democratic institutions, and ubiquitous collection of data and mass surveillance.

Notwithstanding the laudable aim of the Online Safety Bill (OSB) to protect online users from harm, human rights and privacy groups have raised concerns about the potential risks it poses to users' rights to private and family life and freedom of expression.

We are particularly concerned by the OSB's introduction of a duty on private messaging services to monitor and ensure that users are not exposed to harmful content.[1] In spite of some changes being made to the Bill during its Commons Committee stage, these provisions have remained untouched, and as a result of the breadth of the Bill have failed to be robustly scrutinised. Throughout the Bill's passage in the Commons, multiple amendments were also tabled to safeguard end-to-end encryption, although they have not been accepted.

We urge Peers to oppose the undermining of private messaging and end-to-end encryption in the Online Safety Bill at Second Reading in the House of Lords.

MONITORING PRIVATE MESSAGES

1. Clause 110 of the Online Safety Bill gives OFCOM the ability to issue internet services (e.g. social media sites) with a notice to deal with child sexual exploitation and abuse (CSEA) content "whether communicated publicly **or privately** by means of the service (emphasis added)". Such a notice will require providers to use "accredited technology" to identify and swiftly take down CSEA content and to prevent individuals from encountering such content.[2] "Accredited technology" is technology which OFCOM or another person appointed by OFCOM has designated as "meeting minimum standards of accuracy", standards which must be approved and published by the Secretary of State.[3] Providers may also be given a requirement to "use best endeavours" to develop or source their own technology to achieve the same purposes as "accredited technology." In deciding whether it is necessary and proportionate to make such a notice, Ofcom must consider a number of factors, including the kind of service, its functionalities, its user base, the prevalence and dissemination of the content, the risk and severity of harm, the systems and processes used by the service to identify and remove the content, and the risks to users' freedom of expression and privacy.

2. The key issue here is the inclusion of "private messaging" within this clause. As it stands, private messaging services such as WhatsApp are end-to-end encrypted, which means that

[1] For Liberty's wider concerns about this legislation, please refer to our second reading briefing on the OSB: Liberty's briefing on the Online Safety Bill for second reading in the House of Commons, April 2022: https://www.libertyhumanrights.org.uk/wp-content/uploads/2022/04/Libertys-second-reading-briefing-on-the-Online-Safety-Bill-for-the-House-of-Commons-April-2022.pdf
[2] Clause 110(2)(iii) and Clause 110(2)(iv), Online Safety Bill.
[3] These notices could impose requirements on a private messaging service for up to 3 years. A failure to comply with a notice could result in regulatory action including the imposition of substantial fines and the blocking of services.

third parties (such as the social media companies who offer the service, and state governments) cannot access users' direct messages to one another. **While this is not stipulated on the face of the Bill,[4] the duties imposed on private messaging services by the OSB would appear to require private companies to monitor all individuals' private messages in order to comply with their duties; otherwise, it is unclear how they would be able to take action in relation to particular kinds of harmful content.[5]**

3. Cybersecurity experts such as the Internet Society, a global non-profit advocating for an open and trusted Internet, have demonstrated that the only way for service providers that offer end-to-end encryption to comply with the duties imposed by the OSB would be **to remove or weaken the encryption they offer by introducing scanning technology onto their platforms.** Such scanning technology works by comparing individuals' messages to a database of content (e.g. CSEA images), against which it is compared to see if there is a match either *before* it is sent, when it is still on the user's phone or after it is sent, when it is still on the platform's server, before it is received by the intended user. These practices are broadly referred to as 'client-side scanning'. The effect of client-side scanning is to circumvent end-to-end encryption, so the content of individuals' private messages to one another are no longer private.[6]

THREAT TO RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION

4. We acknowledge the laudable aims of the OSB to tackle the serious human rights issues of child sexual exploitation and abuse (CSEA), and the advocacy of civil society groups that has compelled the Government to prioritise eliminating CSEA. We also acknowledge that the internet, as well as being a vital space for debate, has enabled the proliferation of harmful content. These are complex issues which require proportionate and rights-respecting responses. **Nonetheless, we are concerned that in effectively requiring private companies to monitor all users' private online messages in order to comply with their various duties, the OSB risks undermining users' rights to privacy and freedom of expression.**

5. It is important to note that law enforcement agencies in the UK already possess a wide range of powers to seize devices, compel passwords and even covertly monitor and hack accounts to overcome security measures and identify criminals.

6. **A general monitoring obligation on private messages is disproportionate and likely to be harmful to those for whom protections for the ability to communicate privately is most important.** International human rights bodies have recognised the importance of end-to-end encryption to protect the right to privacy and to promote the exercise of other rights. This is because being able to communicate safely and securely can be a precondition to being able to being able to communicate and express one's views – whether that is LGBTQ+ people

[4] It is worth noting that in summer 2022, two senior GCHQ officials published an article (in their personal capacities) in which they endorsed CSS as a potential solution to the problem of CSEA content being transmitted on encrypted platforms, in the context of wider debates on end to end encryption.
[5] Voge, C., and Wilton, R., *Internet impact brief: End-to-encryption under the UK's Draft Online Safety Bill,* 5 January 2022: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/
[6] Abelson et al, *Bugs in our pockets: The risks of client-side scanning,* 15 October 2021: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

seeking community in countries where homosexuality is illegal or journalists seeking to report on human rights abuses in places where there is limited press freedom.[7] The case law of the European Court of Human Rights (ECtHR) recognises the importance of anonymity in "promoting the free flow of ideas and information in an important manner" including by protecting people from reprisals for their exercise of freedom of expression.[8]

7. The United Nations High Commissioner for Human Rights has also voiced concerns about the drastic effect that client-side scanning might have on privacy and free expression:

> "Imposing general client-side scanning would constitute a paradigm shift that raises a host of serious problems with potentially dire consequences for the enjoyment of the right to privacy and other rights. Unlike other interventions, mandating general client-side scanning would inevitably affect everyone using modern means of communication, not only people involved in crime and serious security threats.
>
> Given the possibility of such impacts, indiscriminate surveillance is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship."[9]

8. Much of the focus of the debate on end-to-end encryption in the Online Safety Bill has been on the negative impacts of encrypted messaging on children, particularly in facilitating online child sexual abuse and exploitation. As demonstrated in a recent report by Child Rights International Network and Defenddigtalme, however, the children's rights implications of encryption are nuanced, and there are vital ways that encryption can act to protect children's rights, including children who are marginalised and vulnerable.[10] The UN Committee on the Rights of the Child has also noted that measures designed to detect and tackle CSEA content must be "strictly limited according to the principles of legality, necessity and proportionality" and suggested that routine and indiscriminate measures may not be necessary and proportionate.[11]

UNDERMINING USER SAFETY

9. **Introducing scanning technologies will undermine user safety.** As more than 45 human rights organisations and cybersecurity experts warned, the introduction of 'scanning' technology may introduce new vulnerabilities to the design of platforms: once technology is built to circumvent encryption, it is not only the social media companies themselves tasked with complying with their duties under the OSB, but also hostile actors such as hackers and

[7] Written evidence submitted by Tech against Terrorism to the Joint Committee on the Draft Online Safety Bill, 14 December: https://committees.parliament.uk/publications/8206/documents/84092/default/
[8] Delfi AS v Estonia [2015] EMLR 26, [147] and [149] quoted in legal opinion by Matthew Ryder KC and Aidan Wills on the human rights implications of client-side scanning, November 2022: https://www.indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf
[9] UN High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/51/17, 4 August 2022, para. 28, https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age
[10] Child Rights International Network and Defenddigitalme, Privacy and Protection: A children's rights approach to encryption, 2023: https://home.crin.org/readlistenwatch/stories/privacy-and-protection
[11] UN Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021, para. 75.

foreign governments, who could hijack and manipulate it in malicious ways.[12] This will not only jeopardise device security but place the rights of all users, including children, at grave risk.[13] Companies may also come under pressure from state governments to expand the use of such technologies to monitor wider categories of content, or to share information about users between jurisdictions in ways that endanger dissidents or journalists abroad.[14]

10. In August 2021, Apple proposed the introduction of client-side scanning in order to scan for images of child abuse in text messages. This move was met with opposition from over 90 civil society organisations, who criticised Apple for introducing surveillance capabilities onto its devices and highlighted the potential for the technology to actually put young people at risk by eroding their rights to privacy – for example, LGBTQ+ young people or children subject to abuse on family accounts, who may no longer be able to communicate safely and securely. Experts also warned that once scanning technology is introduced to people's devices, the scope of the targeted content could be easily broadened – including if companies like Apple are pressured into doing so by state governments – thus enabling greater surveillance and erosions of individuals' privacy and free expression rights.[15] Eventually, Apple scrapped its proposal in response to these concerns.

11. Seventy civil society organisations, companies, elected officials, and cybersecurity experts including members of the Global Encryption Coalition (GEC) have further warned that eroding end to end to encryption will make UK businesses less safe online, by leaving them more susceptible to cyber-attacks and intellectual property theft.[16] The GEC noted one study which found that when Australia passed a similar law undermining end-to-end encryption in 2018, the Australian digital industry lost an estimated $AUS 1 billion in current and forecast sales and further losses in foreign investment as a result of decreased trust in their products.[17]

MASS SURVEILLANCE BY THE BACKDOOR

12. Should the Online Safety Bill's requirement on private messaging services to monitor the private messages of user amount in practice to requirements to impose client-side scanning, we echo the concerns raised by legal and cybersecurity experts that this would equate to "generalised, state-mandated mass surveillance of communications by the private sector."[18]

---

[12] Global Encryption Coalition, *45 organizations and cybersecurity experts sign open letter expressing concerns with UK's Online Safety Bill*, 14 April 2022: https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill ; and Abelson et al, *Bugs in our pockets: The risks of client-side scanning,* 15 October 2021: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

[13] https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/

[14] Abelson et al, *Bugs in our pockets: The risks of client-side scanning,* 15 October 2021: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

[15] Franklin, S.B. and Nojeim, G., *International Coalition Calls on Apple to Abandon Plan to Build Surveillance Capabilities into iPhones, iPads, and other Products,* 19 August 2021: https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-and-other-products/#:~:text=An%20international%20coalition%20of%2090,iPads%20and%20other%20Apple%20products

[16] Global Encryption Coalition, *70 organizations, cyber security experts, and elected officials sign open letter expressing dangers of the UK's Online Safety Bill,* 24 November 2022: https://www.globalencryption.org/2022/11/70-organizations-cyber-security-experts-and-elected-officials-sign-open-letter-expressing-dangers-of-the-uks-online-safety-bill/

[17] New Study Finds Australia's TOLA Law Poses Long-Term Risks to Australian Economy, Internet Society, 2 June 2021: https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

[18] Legal opinion by Matthew Ryder KC and Aidan Wills on the human rights implications of client-side scanning, November 2022: https://www.indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf

The lack of safeguards for these extraordinary powers would effectively "replicate the behaviour of a law-enforcement wiretap" without a warrant.[19]

13. It is useful to refer by analogy to the UK's existing framework for regulating mass surveillance - the Investigatory Powers Act 2016 (IPA). The IPA contains a range of powers enabling the intelligence services and law enforcement bodies to obtain the content of communications, including targeted interception and equipment interference warrants, albeit under specific defined criteria. Of particular relevance is the IPA's provisions regarding "bulk" interception which can authorise the interception of overseas-related communications that are being transmitted and the subsequent automated analysis and human examination of the content of those communications. The IPA also provides for "bulk" equipment interference, including interference with communications equipment for the purposes of, among other things, obtaining overseas-related communications, equipment data or any other information.

14. Both the IPA and OSB enable the interception of the content of private messages of large numbers of people[20] in circumstances where there is no suspicion of wrongdoing. However, the OSB goes further in a number of ways. Importantly, there are almost no safeguards in the OSB as compared to even the minimal – and even so, highly contested – safeguards in the IPA[21] or those that have been established as essential to assessing the necessity and proportionality of measures being taken in the process of "bulk" surveillance, for example independent prior authorisation (i.e. before a notice is issued) and ex post facto independent oversight. Expert legal counsel have warned that the lack of safeguards risks in itself constituting a disproportionate interference with articles 8 and 10 of the ECHR.[22]

15. **For the above reasons, we urge parliamentarians to oppose the Online Safety Bill's intrusion into private messaging at Second Reading.**

For more information, please contact Jun Pang, Policy and Campaigns Officer, Liberty (junp@libertyhumanrights.org.uk).

[19] Abelson et al, Bugs in our pockets: The risks of client-side scanning, 15 October 2021, available at: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

[20] In the case of client-side scanning, everyone using a particular communications service; and in the case of bulk interception, everyone whose communication passes along a particular bearer.

[21] Government agrees bulk surveillance powers fail to protect journalists and sources, *ComputerWeekly.com*, 14 April 2022: https://www.computerweekly.com/news/252515935/Government-agrees-bulk-surveillance-powers-fail-to-protect-journalists-and-sources.

[22] Legal opinion by Matthew Ryder KC and Aidan Wills on the human rights implications of client-side scanning, November 2022: https://www.indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf