LIBERTY

**Liberty's submission to the Public Bill Committee on the Online Safety Bill: Private messaging**
June 2022

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, we are extremely concerned by the potential risks it poses to users' rights to privacy and free expression. The focus of this submission is on the provisions in the OSB relating to private messaging, and the potential negative impacts on human rights. For Liberty's wider concerns about this legislation, please refer to our second reading briefing on the OSB.[1]

End-to-end encryption

1. We are concerned that the imposition of duties on **private messaging services** to monitor and ensure that users are not exposed to illegal content and 'legal but harmful' content, as well as the introduction of technology notices and use of "accredited technologies" to detect child sexual exploitation and abuse (CSEA) and terrorism content, may **erode users' rights to privacy and freedom of expression by undermining end-to-end encryption.**

2. It is important to establish first and foremost that the OSB does not distinguish between public social media and private messaging services. **What is posted on a public social media platform is different to private messages sent between individual online users; however, the OSB appears to propose to treat these services in the same way.** This contradicts the Government's 2019 Online Harms White Paper, in which the Government expressed clearly that it understood the difference between public and private communications,[2] and its acknowledgement in its summary of responses to the Paper that "overall respondents opposed the inclusion of private communication services in scope of regulation."[3]

3. What this means in practice is that private messaging services such as WhatsApp could be subject to the same duties and obligations of 'Category 1' services, such as Facebook and Twitter, with which failure to comply can result in significant financial penalties. These include the duties to have systems and processes in place to prevent individuals from encountering 'priority illegal content' by minimising its presence or taking it down; and duties to deal with 'legal but harmful' content (to be specified in regulations by the Secretary of State) including restricting users' access to it, limiting its recommendation, and taking it down. Further, the

[1] Liberty's briefing on the Online Safety Bill for second reading in the House of Commons, April 2022, available at: 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] DCMS, *Online Harms White Paper*, April 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf DCMS, *Online Harms White Paper: Full government response to the consultation*, 15 December 2020, available at: https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response#annex-a
[3] DCMS, *Online Harms White Paper - Initial consultation response,* 15 December 2020, available at: https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

OSB gives OFCOM the ability to issue social media sites *and* private messaging services with a notice to deal with terrorism content or 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 terrorism and CSEA content respectively. "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.

4. As it stands, private messaging services such as WhatsApp are end-to-end encrypted, which means that third parties (such as the social media companies who offer the service, and state governments) cannot access users' direct messages to one another. **The duties imposed on private messaging services by the OSB would require private companies to monitor 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.**[4]

5. Experts such as the Internet Society, a global nonprofit advocating for an open and trusted Internet, have argued 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 (what is referred to as 'client-side scanning', and which has been embraced by Home Secretary Priti Patel[5] alongside the Five Eyes[6]); or after it is sent, when it is still on the platform's server, before it is received by the intended user. **Either way, this circumvents encryption, so that the content of individuals' private messages to one another are no longer private.**[7]

6. We acknowledge the laudable aims of the OSB to tackle the serious human rights issues of child sexual exploitation and abuse (CSEA) and terrorism, 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.

7. **We are concerned that in requiring private companies to monitor users' private online messages - including through the use of 'accredited technologies' - in order to comply with their various duties, the OSB risks undermining users' rights to privacy and freedom of expression.** All around the world, end-to-end encryption has enabled everyone from political dissidents to people in marginalised communities (such as LGBTQ+ people) to be

[4] Voge, C., and Wilton, R., *Internet impact brief: End-to-encryption under the UK's Draft Online Safety Bill,* 5 January 2022, available at: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/
[5] Warwick, S., *Priti Patel says Apple should see through CSAM photo scanning measures,* 9 September 2021, available at: https://www.imore.com/priti-patel-says-apple-should-see-through-csam-photo-scanning-measures
[6] International Statement: End-To-End Encryption and Public Safety, 11 October 2020, available at: https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety
[7] 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

able to communicate and express themselves without fear, safe in the knowledge that only the sender and their intended recipients will be able to know the content of their messages.[8] Under the OSB, private messaging companies would be required to scrutinise individuals' every message to one another and deal with any 'harmful' message in the way that the relevant duty requires. The introduction of client-side scanning in particular would mark an unprecedented expansion of mass surveillance on people's devices by enabling the monitoring of messages before they are even sent, effectively "replicat[ing] the behaviour of a law-enforcement wiretap" without a warrant.[9]

8. The risk of significant financial penalties for failing to comply with the duties under the OSB may cause companies to pre-emptively remove content – including that which is sent privately between users – to avoid breaching their duties, **constituting a significant threat to freedom of expression.** The risk of this being done mistakenly is significant: most internet service providers rely on automated content detection software which is prone to mistakenly flag art, health information, educational resources, advocacy messages, and other imagery, which exacerbates the risk of inaccurate takedowns at scale, especially given the vague definitions of illegal content and legal but harmful content in the OSB.[10] In addition, content removal may result in self-censorship and/or, in a counterproductive fashion, stop particular harmful expression from being challenged.

9. **Introducing scanning technologies of this kind 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 foreign governments, who could hijack and manipulate it in malicious ways.[11] This will not only jeopardise device security but place the rights of all users, including children, at grave risk.[12] 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 people such as dissidents or journalists abroad.[13]

[8] Written evidence submitted by Tech against Terrorism to the Joint Committee on the Draft Online Safety Bill, 14 December, available at: https://committees.parliament.uk/publications/8206/documents/84092/default/
[9] 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
[10] 90+ digital rights organisations ask Apple to drop image surveillance plans, Digital Rights Watch, 26 August 2021, available at: https://digitalrightswatch.org.au/2021/08/26/90-digital-rights-organisations-ask-apple-to-drop-imagesurveillance-plans/
[11] Global Encryption Coalition, *45 organizations and cybersecurity experts sign open letter expressing concerns with UK's Online Safety Bill*, 14 April 2022, available at: 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, available at: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf
[12] https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/
[13] 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

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.[14] Eventually, Apple scrapped its proposal in response to these concerns.

11. **In the longer term, the OSB may result in a reduction in end-to-end encrypted services.** One of the consequences of this Bill is that private messaging companies may be incentivised to get rid of such services altogether, given the potential liabilities arising under the OSB. This will have a detrimental impact on individuals' ability to communicate securely online. [15] The model set by the OSB may also set a negative precedent globally, with other state governments seeking to clamp down on end-to-end encryption in order to stifle dissent and free expression.[16]

12. **For the above reasons, we urge parliamentarians to oppose the inclusion of private messaging services within the scope of the OSB and to support an amendment to the Bill leaving out "or privately" from Clause 103, Page 87, line 14.**

Jun Pang, Policy and Campaigns Officer, Liberty

junp@libertyhumanrights.org.uk

[14] 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, available at: 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
[15] Internet Society, https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/
[16] "Bugs in their Pockets," available: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf