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

Summer 2023

Private online messaging matters to everyone. None of us want to feel as though someone is looking over our shoulder when we are communicating with our loved ones. End-to-end encryption ensures that private communications remain private. It ensures that our messages cannot readily be viewed, compromised, or altered by anyone else – not even the provider of the chat service. End-to-end encryption is a particularly vital protection for human rights defenders and journalists who rely on private messaging to do their jobs in hostile environments; and for those who depend on privacy to be able to express themselves freely, like LGBTQ+ people.

The government claims that the Online Safety Bill does not undermine end-to-end encryption, but clause 111 of the Bill could expressly mandate the use of technological tools to proactively prevent content from appearing on encrypted private messaging services, while also requiring platforms to invest in technology to remove content from such services. These tools are driven by artificial intelligence – intercepting people's private messages and running algorithms over their images in search of prohibited content. Crucially, these tools don't just flag bad content – they check every message and every image from everyone on the system.

The potential for Ofcom to require social media companies to scan people's private messages en masse poses significant human rights implications for the more than 40 million people in the UK who use private messaging services every day. Well-intentioned efforts to protect people from prohibited content could open the door to wider harms, including making UK businesses and individuals less safe online, with criminals, domestic abusers, and hostile foreign states just some of the bad actors that could exploit backdoors into our private communications. **For these reasons we urge parliamentarians to support amendment 255, laid by Lord Moylan, to protect end-to-end encryption from surveillance powers in the Bill set out in clause 111.**

AMENDMENTS TO PROTECT PRIVATE MESSAGING

Clause 111, amendment 255 in the name of Lord Moylan:

"(5A) A notice under subsection (1) may not impose a requirement relating to a

service if the effect of that requirement would be to require the provider of the service to weaken or remove end-to-end encryption applied in relation to the service or part of the service."

BRIEFING ON CLAUSE 111

1. Clause 111 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. "Accredited technology" is defined in the Bill at clause 206(11) as "content identification technology" that will seek out and identify the prohibited content, intercept it on upload and remove it from the platform. Ofcom or another person appointed by Ofcom may designate technology as "accredited" where it meets "minimum standards of accuracy", standards which must be approved and published by the Secretary of State. 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 several 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.[1]

2. Many private messaging services including Apple iMessage, WhatsApp and Signal are end-to-end encrypted, which means that third parties (including the companies who operate the services and governments) cannot readily access users' direct messages to one another. **The duties imposed on private messaging services by the OSB would appear to require private companies to monitor the private messages of <u>all</u> individuals 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.**

1For "accredited technology" and content identification systems see Clause 111(2)(iii) and Clause 111(2)(iv), and see also Clause 206(2), Clause 206(10) and Clause 206(11)Online Safety Bill. OFCOM 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.

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 introduce scanning technology onto their platforms.**[2] Such scanning technology works by comparing individuals' messages to a database of content (e.g. CSEA images), to see if there is a match (known as "perceptual hashing"). An image may be compared either *before* it is sent, when it is still on the user's phone (known as client-side scanning),[3] or after it is sent, when it is still on the platform's server, before it is received by the intended user. The effect is either to circumvent end-to-end encryption, so the content of individuals' private messages to one another are no longer private; or to remove it, creating a back-door that leaves the system open to security vulnerabilities.[4]

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 sharing of illegal content. These are complex issues which require proportionate and rights-respecting responses. **We are concerned that in effectively requiring private companies to monitor <u>all</u> users' private online messages in order to comply with new 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.

UNDERMINING USER SAFETY

6. **Scanning technologies undermine user safety.** Cybersecurity experts have warned that the introduction of 'scanning' technology may introduce new

2Voge, 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/
3It is worth noting that in summer 2022, two senior GCHQ officials published an article (in their personal capacities) in which they endorsed client-side scanning 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. Ian Levy and Crispin Robinson: Thoughts on child safety on commodity platforms https://arxiv.org/abs/2207.09506
4Abelson et al, *Bugs in our pockets: The risks of client-side scanning,* 15 October 2021: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf; See also Wikipedia on perceptual hashing: https://en.wikipedia.org/wiki/Perceptual_hashing

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.[5] This will not only jeopardise device security but place the rights of all users, including children, at grave risk.[6] 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.[7]

7. The impact on business was highlighted by seventy civil society organisations, companies, elected officials, and cybersecurity experts including members of the Global Encryption Coalition (GEC). In an open letter to Rishi Sunak, they warned that eroding end-to-end encryption will make UK businesses less safe online by leaving them more susceptible to cyber-attacks and intellectual property theft.[8] 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.[9]

8. On a practical level, it is not clear that all devices would be compatible with these systems. For example, many mobile phones may not have the processing power required to maintain such a system of scanning. The power required on an individual device to carry out these functions would also have a major and debilitating impact on a device's battery life. In other cases, older devices, particularly those out of circulation, may not be capable of undertaking system updates, leaving discovered vulnerabilities exposed and

---

5 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

6 Electronic Frontier Foundation, *Why Adding Client-Side Scanning Breaks End-To-End Encryption*, 1 November 2019: https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

7 Committeee to Protect Journalists, *What the UK's Online Safety Bill could mean for press freedom*, 30 January 2023: https://ifex.org/what-the-uks-online-safety-bill-could-mean-for-press-freedom/

8 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

9 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/

open to exploitation by bad actors.[10] The Government are yet to set out how any of these practical challenges would be addressed.

MASS SURVEILLANCE BY THE BACKDOOR: A LEGAL QUAGMIRE

9. Should the Online Safety Bill's requirement on private messaging services to monitor the private messages of users 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."[11] The lack of safeguards for these extraordinary powers would effectively "replicate the behaviour of a law-enforcement wiretap" without a warrant.[12] This was a view expressed by a leading human rights and technology barrister, Matthew Ryder KC, in a legal opinion commissioned by Index on Censorship. In the opinion, Ryder also set out his view that measures in the Bill would grant Ofcom a wider remit on mass surveillance powers of UK citizens than bodies such as GCHQ.[13]

10. 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 that can circumvent end-to-end encryption under specific defined criteria. Of 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.

---

10 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; See also Wikipedia on perceptual hashing: https://en.wikipedia.org/wiki/Perceptual_hashing

11 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

12 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

13 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

11. Both the IPA and OSB enable the interception of the content of private messages of large numbers of people[14] in circumstances where there is no suspicion of wrongdoing. However, the OSB goes further in several 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[15] 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.[16]

12. For years, civil society groups have argued that mass surveillance powers are incompatible with human rights. In a recent landmark victory for Liberty and Privacy International, the Investigatory Powers Tribunal (IPT) found that MI5 had committed serious wrongdoing in failing to comply with its statutory obligations in relation to the handling of the public's personal data under the IPA and previously the Regulation of Investigatory Powers Act (RIPA). The Tribunal also found that the Home Office had breached its duties to oversee MI5 by failing to enquire into MI5's non-compliance and granting MI5 unlawful surveillance warrants as a result.[17] This judgment shows that even minimal statutory safeguards can be ignored in practice, undermining further the little protection they offer, and that oversight bodies cannot be relied on to spot and prevent lawbreaking.

13. The OSB provides far fewer safeguards than the IPA, and yet gives Ofcom unprecedented powers to issue technology notices potentially mandating client-side scanning. Client-side scanning entails the mass surveillance of users' private communications. Mass surveillance of this sort is incompatible with users' rights to privacy.

For the above reasons, we urge parliamentarians to support amendment 255, laid by Lord Moylan, to protect end-to-end encryption from surveillance

---

14In 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.

15 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.

16Legal opinion by Matthew Ryder KC and Aidan Wills.

17Liberty and Privacy International v Security Service and Secretary of State for the Home Department, [2023] UKIPTrib1

powers in the Bill set out in clause 111. For more information, please contact: mark.johnson@bigbrotherwatch.org.uk