Written evidence submitted by Open Rights Group (OSB0118)

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK.

We have previously provided evidence on the Online Safety Bill to the Joint Committee on Human Rights[1], the Lords Communications Committee[2], the Law Commission[3], and to Government[4], and to the DCMS Subcommittee enquiry into online safety and online harms[5]. We also wrote detailed reports around the green and white paper stages, including our response to the consultation paper, [6] Internet Regulation, Part I[7] and Part II[8], Blocked: Collateral Damage in the War against Online Harms[9], and DNS Security: Getting It Right[10]. These evidence submissions and publications should be taken into consideration by the Committee in tandem to this submission.

Three years into the online harms debate, we are no closer to finding a meaningful solution to the issues which the framework seeks to resolve, and we are no closer to devising legislative solutions which preserve the rights to freedom of expression and privacy in the quest to "make the UK the safest place in the world to be online." Indeed, as those issues have exacerbated, so has the Government's endorsement of legislative and technical "solutions" which would drastically limit the fundamental rights of everyone, not just those who are culpable of committing harms.

To that end, we reiterate our significant concerns about the unintended consequences of the Online Safety Bill, its regulatory framework, and its enforcement powers. They are as follows:

1. The Bill will politicise free speech, and the boundaries surrounding it, through the powers granted to the Secretary of State over the speech regulator (Ofcom.)

As it has been drafted, the Bill grants sweeping powers to the Secretary of State for Digital, Culture, Media, and Sport, and potentially to the Home Secretary, to make unilateral decisions, at any time they please, as to what forms of subjectively harmful content must be brought into the scope of the bill's content moderation requirements. It also allows them to make those decisions for political reasons. These risks come in Part 2, Chapter 5, Section 33 of the draft, which states (emphasis our own):

---

[1] https://www.openrightsgroup.org/publications/response-to-the-joint-committee-on-human-rights-inquiry-into-freedom-of-expression/

[2] https://www.openrightsgroup.org/publications/response-to-the-lords-communications-committee-enquiry-into-freedom-of-expression-online/

[3] https://www.openrightsgroup.org/publications/open-rights-group-response-to-the-law-commission-reform-of-the-communications-offences/

[4] https://www.openrightsgroup.org/publications/response-to-consultation-on-the-online-harms-white-paper-july-2019/

[5] https://committees.parliament.uk/work/1432/online-safety-and-online-harms/publications/, pending publication

[6] https://www.openrightsgroup.org/app/uploads/2020/03/Online_Harms_Consultation_Response.pdf

[7] https://www.openrightsgroup.org/assets/files/pdfs/reports/Internet_Regulation_Part_I_Internet_Cens%20orship_in_the_UK_today-web.pdf

[8] https://www.openrightsgroup.org/assets/files/pdfs/reports/ORG_Regulation_Report_II.pdf

[9] https://www.openrightsgroup.org/assets/files/reports/report_pdfs/top10vpn-and-org-report-collater%20al-damage-in-the-war-against-online-harms.pdf

[10] https://www.openrightsgroup.org/assets/files/reports/report_pdfs/ORG_DNS_Security_Report_.pdf

(1) The Secretary of State may direct OFCOM to modify a code of practice submitted under section 32(1) where the Secretary of State believes that modifications are required—
(a) ***to ensure that the code of practice reflects government policy [...]****,*

In other words, a government minister will have the authority to order a independent regulator - which, by definition, would no longer be independent - to modify the rules of content moderation on topics which are entirely subjective, entirely legal, and entirely political, and to order that regulator to enforce those new rules.

These illiberal clauses create the legal scaffolding for state control over free speech and a chilling effect on public discourse. They should have no place in this Bill, or in any democratic society.

2. The Bill will result in the end of private personal messaging.

Under the Bill, online service providers will have legal obligations to limit the appearance of *illegal* content, above and beyond the systems they already use to detect and take down the overwhelming majority of this abhorrent material. However, as drafted, the Bill will also oblige service providers to exercise "duty of care" responsibilities over *legal* content, meaning our free and subjective speech. The only way for service providers to meet these compliance requirements, in the context of private messaging, is to scan the contents of our private messages - and yours - for that legal content. And the only way for service providers to read the contents of these private messages, whether that is for illegal or legal content, is to break end-to-end encryption.[11]

Put simply, there will no longer be any such thing as personal communications. Everything we say, no matter how private, will be fair game under the Bill. Only email and SMS services are exempted; and these are typically insecure in any case. This radical curtailment of our rights to privacy and freedom of expression will be done on the assumption that we are all criminals trading in the most abhorrent matter imaginable.

Regulatory limits on end-to-end encryption will apply to companies and service providers regardless of their location if they target or serve UK users. This means that data will become easily accessible and subject to misuse. This places both users and businesses at risk, if data breaches occur.

We have spoken to several service providers, both inside the UK and abroad, who are planning to either block UK customers or leave the UK altogether, rather than be compelled to weaken their data security and act as state content moderators if end-to-end encryption is compromised or banned under the Bill. If the government will not acknowledge the risks to fundamental digital rights inherent in the plans to compromise encryption, they may find the voice of the marketplace to be much more direct.

3. The Bill will result in the blocking of services, sites, and apps, at ISP and app store level, which OFCOM will be permitted to do via court order.

[11] https://www.openrightsgroup.org/blog/encryption-in-the-online-safety-bill/

As it has been drafted, the Bill imposes requirements for a dizzying array of compliance obligations, assessments, and documentation processes onto all services which host user-generated content, whether they are a tiny start-up or the largest social media giant.[12] What is notable is that a failure to achieve any one of these bureaucratic obligations, including still-undefined requirements over legal and subjective content, can be used by the regulator as leverage to impose service restrictions onto a site or service.

In other words, the compliance obligations, as proposed in the draft Bill, bypass any debates about the nature of the content, conduct, or contact on a site or service altogether, in order to arrive directly at the same punitive outcome. The options on the table include technology restriction orders, service restriction orders, and access blocking orders.

It is clear that these compliance requirements can, and will, be used as means of chilling public discourse, censoring uncomfortable discussions, or shutting down the services used for personal communications altogether. It is also clear that these requirements are setting businesses up to fail.

We know that, as with so many aspects of the Bill, these provisions have been drafted to target specific individual services which policymakers, for reasons of their own, would like to block from the UK.[13] Those services have the legal and human resourcing to cope with the compliance requirements. Smaller services do not, nor will they commit scant resources to achieving them, especially in an atmosphere which openly associates compliance failures - even if that is a failure to tick a box on an assessment form - with complicity in child exploitation. There is a marked irony in the UK government embarking on a drive to deregulate the digital economy from what it perceives as European bureaucratic red tape, only to replace it with far more stringent domestic red tape, with far graver consequences.

4. The Bill will impose mandatory age gating, and therefore, personally identifiable internet usage, across all sites and services, regardless of risk.

Perhaps the most sweeping and illiberal consequence of the draft Bill's compliance obligations is the mandating of age verification processes onto all sites, services, or applications offering user-to-user content or communication which can be accessed in the UK, regardless of scope, risk, proportionality, or the possibility of subjective harm to anyone, as has been mandated in Part 2, Chapter 4.[14] To be clear, what is on the table is not age verification as it has been traditionally debated, e.g. blocking access to explicit adult content or a brewpub's draught menu. What is being mandated is age checks on sites and services with user-to-user content or communication across the board, meaning *all content, all sites, all services, and all users, all the time*, excepting sites which are deemed 'child safe'.

Although the Bill's impact assessment notes that "We expect only a small percentage of the highest risk businesses that are likely to be accessed by children to be required to implement age verification systems", the Bill itself has been drafted in a way that means every business in scope will need to implement some form of age verification or assurance. They will need to do

[12] https://www.openrightsgroup.org/blog/access-denied-service-blocking-in-the-online-safety-bill/

[13] https://www.telegraph.co.uk/politics/2020/08/21/duty-care-regulator-should-able-block-whatsapp-says-former-culture/

[14] https://www.openrightsgroup.org/blog/age-verification-in-the-online-safety-bill/

this not to shield children from subjectively harmful content, but to achieve their compliance requirements (see previous question).

There are several risks here. The first and most obvious is consent fatigue, as mandatory age verification popups replace the much-hated cookie popups on every site or service which could be potentially accessed by someone in the UK.

The second is the chilling effect that these blanket age verification processes will have on the rights to privacy and freedom of expression. We will no longer be able to read information, speak our minds, or look up information without proving who we are. That is profoundly illiberal.

The third risk comes from the age verification and assurance processes themselves. These processes will collect many different pieces of personally identifiable information in order to profile us to establish our likely age. In doing so, they will create massive privatised databases of personal Internet browsing – databases which would be very appealing to governments or hackers.

And the fourth risk, as will be obvious, is the risk that this will pose to Internet architecture. Large parts of the UK Internet will, for all intents and purposes, be gated off behind a giant state-mandated identity verification wall. That wall, as a form of content filtering, will act as an additional technical layer within the UK's Internet architecture – a wall not duplicated in any other western country. As the Internet Society has noted[15], this kind of mandated content filtering process risks four out of five of the fundamental networking properties of the Internet.

At the end of the day, children will be no safer, and online harms will continue just as they did before.

5. Those who need online anonymity, for whatever reason, will no longer be able to exercise it.

Parallel to the risks of mandatory age verification requirements is the de facto establishment of an identity verification requirement as a condition for accessing the internet. There is no doubt that anonymity is frequently abused. But the fact remains that people - journalists, victims of domestic abuse, dissidents, young people in crisis, whistleblowers, and countless others - rely on anonymity to play their roles in a free and democratic society.

We are heartened by the government's acknowledgement of the need for anonymity and of the right to it[16], however, the draft Bill still puts it at risk. We want to see a commitment to preserving the right to anonymity established in the Bill. The Committee must also take heed to the ways that anonymity could be at risk through secondary means, such as compliance requirements which effectively ban justifiable and necessary anonymity through the back door, as we have discussed above.

6. Calls for senior management liability will create a chilling effect and will dissuade the talent needed to address online harms.

---

[15] https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-content-filtering/

[16] https://hansard.parliament.uk/Commons/2021-01-13/debates/8FE512AB-7F60-492E-B213-5A521F01C4C6/OnlineAnonymity?highlight=dinenage%20anonymity#contribution-ADACAAE8-909B-4840-A6BB-568936E920E1

We note repeated calls for the Bill to create personal criminal liability for senior managers and company directors. We reiterate, once again[17], why this will do nothing to make the web safer, better, or less harmful:

- It will create a culture of fear which results in a phenomenon known as "collateral censorship", where service providers and companies feel they have no choice but to take down vast swathes of content which may be perfectly legal, perfectly subjective, and perfectly harmless, less they face sanctions, penalties, and even personal arrests for getting it wrong. The content taken down though collateral censorship will include valid and healthy public opinions on politics, public affairs, and the nature of our democratic society.
- It dissuades the very talent and expertise needed to tackle online harms, and improve online safety, from taking on that work, and indeed, from taking those jobs at all. No tech sector professional will offer themselves up for a job where they face the threat of arrest for getting something wrong, or indeed, for the way that a member of the public misused the service they work for. Good people cannot do the work required to improve safety if they are constantly in fear of their own.
- It sets a very poor global example, putting the UK into the company of authoritarian nations which arrest people for legal speech matters, and indeed, arrest people for the legal speech of others. It will also provide inspiration to authoritarian nations who look up to the UK as an example to follow: if the UK arrests company employees for the political speech carried on their platforms, why shouldn't they?

As we have noted from the start, calls for management liability target a small handful of specific and high-profile individuals, all of whom are American. These individuals can more than afford to duck. Any legislation imposing criminal liability will miss these targets and hit British tech talent instead.

7. The Bill acts as a trade barrier to foreign commerce and investment.

Lastly, Part 2, Chapter 4 of the draft Bill requires all non-UK companies to carry out a "child risk assessment", including implementing a form of age verification or age assurance, *before they would be allowed to operate within the UK.*[18] This creates not just a trade barrier, but a means of shutting out foreign companies, and the user-generated content on them, from being accessible in the UK, through a tick-box compliance process which equivocates a failure to carry out the assessment with complicity in child exploitation.

This clause furthermore compels foreign companies to collect personally identifiable data about all its UK visitors - who are *not necessarily customers or users* - as a prerequisite for being able to do business in the UK, with no guarantee they will actually be able to do so. This will apply even if those companies are based in countries, unlike the UK, which offer no legal rights to those individuals over those companies' collection, use, exploitation, and sale of that personally identifiable data.

[17] https://www.openrightsgroup.org/blog/online-abuse-why-management-liability-isnt-the-answer/
[18] https://www.openrightsgroup.org/blog/access-denied-service-blocking-in-the-online-safety-bill/

The draft Bill also fails to explain what sort of technical means the UK, presumably through Ofcom, intends to put in place to block foreign web sites from being accessible in the UK until they have completed a child risk assessment, regardless of whether the regulator considers that service to have passed or failed the assessment. It also fails to explain what sort of human resourcing the regulator intends to put into place to classify virtually every site, service, or application on the global internet as being acceptable for admittance, pending review of a safety assessment, onto British screens.

As with so many other aspects of the draft Bill, the only logical conclusion is that service providers will simply not bother doing business here, or will block UK visitors and users altogether, rather than expend time and resources on a highly adversarial compliance process which has set them up to fail. As grim a prospect as this is, it is an easier one to stomach than the prospect of a technical firewall which blocks out non-British web sites from being accessible on the British internet. This is not the message that Global Britain should be sending out about its attractiveness as a place for trade and inward investment.

We look forward to continuing to liaise with the Committee on these issues.

21 September 2021