Written evidence submitted by Open Rights Group

Response to the DCMS Subcommittee inquiry into Online Safety and Online Harms

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 are also preparing our response to the Joint Pre-Legislative Scrutiny Committee.

Q. How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

Despite two and a half years of debate and discussion, the concept of "online harms" remains vague, malleable, and undefined. The intended scope of the legislation still encompasses any content, conduct, or content which could be potentially subjectively harmful to anyone, based on subjective judgements and tastes, as defined by government ministers. The draft Bill further distinguishes between "primary priority content" and "priority content", which no definition of what these terms mean.

In attempt to gain clearer definitions of harms, primary priority content, and priority content, we have sought written confirmation, in collaboration with several other human and digital rights organisations[5], from the Minister of State for Digital, Media, Culture, and Sport on the following questions. We would encourage the Committee to press the Government for clarity on these matters as well:

1. Does the legislation impose any limitations on what the Secretary of State is able to designate as "priority content that is harmful" to adults or children?
2. Clause 11(2) requires services within scope to specify in their terms of service how priority content that is harmful to adults and other content that is harmful to adults "is to be dealt with" by the service. Can the department confirm whether or not a service could specify in its terms of service that it takes no action with respect to such forms of content and still meet its duty under that section? Or

[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] Joint letter to Oliver Dowden and Caroline Dinenage sent by ORG, Global Partners Digital, the Adam Smith Institute, Index on Censorship, DefendDigitalMe, Article19, and English PEN, 12 August 2021

does the term “how … is to be dealt with” require action of some sort to be taken?

3. Does the department envisage requirements in clause 11 ever to require or encourage services to *proactively* monitor and detect priority content that is “harmful” to adults or other content that is harmful to adults?
4. At this stage, can the department provide an indication of the types of “content that is harmful” to adults and children which it envisages the Secretary of State will instruct Ofcom to require companies to take action on?
5. Can the department (a) define “physical or psychological impact” as used in clauses 45 ad 46, and (b) indicate what it considers would constitute an “indirect” physical or psychological impact”?
6. Clause 46(4) refers to “certain characteristics” in relation to content that is harmful to adults. What “characteristics” does the department envisage this as including, and will there be any clinical reference?

We have been disturbed to note the shift in tone and terminology from “online harms” to “online safety”. This has clearly been done to support the economic interests of the safety tech market, which DCMS has enthusiastically endorsed as a growth area for the UK tech sector in the aftermath of the UK’s departure from the European Union.[6] This seemingly innocuous semantic shift poses two risks.

The first risk is the obvious move towards regulatory capture, where businesses offering products which can be highly privacy-invasive, and can also restrict the right to freedom of expression, are being permitted - and indeed, encouraged - to redraft the law and its framing around their commercial ambitions. The second threat is the risk of the perception, among both the public and government, that online harms (whatever that might mean) can and should be solved by market-ready technical solutions. This flawed perception moves us further away from a good-faith discussion of the societal and systematic causes of behaviours which can manifest as online harms, and pushes us closer towards digital solutionism and electronic surveillance.

Q. Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

If some form of action, such as moderation or takedown, must follow after some form of content, conduct, or contact has been deemed “harmful”, then a defined process is clearly necessary in order to provide rationality, predictability, and legal certainty. However, as discussed in the previous question, the difficulties in trying to define what ‘harm’ and ‘risk’ might constitute, and who has the authority to define those terms, have yet to be resolved. It therefore falls to online services to define the harms, the actions, *and* the processes. All this serves to achieve is to prove how the Online Safety Bill’s underlying concept - that the “health and safety” model for physical premises can be transferred to speech in the online world - remains implausible.

As those definitions, actions, and processes are established and defined, it is imperative that they must to be linked to existing global human rights standards, existing

[6] https://www.gov.uk/government/publications/directory-of-uk-safety-tech-providers

regulations and judicial safeguards on privacy and freedom of expression, and for harms which cross a threshold, existing laws on civil and criminal liability. The UK cannot achieve its goal of creating "world leading" internet regulation by falling completely out of line with international norms and the rule of law.

Q. Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

As it has been drafted, the Online Safety Bill regulates user-generated content rather than system design, algorithmic amplification, and surveillance-driven business models. It targets speech rather than reach, including speech which is completely legal and subjective, in effect, punishing the public rather than the platforms.

The risks to freedom of expression presented by such a model are exacerbated by the draft Bill's clauses on senior management liability[7], which will create a chilling effect on freedom of expression, as tech sector workers will feel they have no choice but to take down legal and permissible content lest they face personal sanctions or criminal arrests. As we have previously noted, tackling online harms will require the best and the brightest minds the tech sector has to offer, and these people cannot work to protect public safety if they are constantly living in fear of their own.

The issues the Online Safety Bill seeks to address are proof of an underlying market failure: power is concentrated in too few companies. These companies, and the competitor entrants which may seek to upstart them, must be incentivised to nurture trust and value their relationships with their customers, rather than nurturing attention and valuing data. As it has been drafted, the Bill does nothing to shift that dynamic, and arguably makes it worse, by cementing dominant players in place, who will continue to maximise attention without effective competitors and a competitive market.

To address these converging issues at their source, we would recommend that the Bill shifts from the regulation (meaning the censorship) of content to the empower users to control the way they receive content, such whether they use prioritisation engines, or other forms of targeting, and the factors that go into such prioritisation and personalisation. They should be empowered to use competing platforms to receive content from users at other platforms, so they can choose the kind of user experience they want, through "interoperability" requirements. After all, we can use a TT phone to communicate with a BT customer. In the same way we should be able to choose a 'friendly' platform to receive content from a Twitter customer.

The existential threat of senior management liability should also be removed entirely. Subjectively harmful speech would be removed from the scope of the Bill altogether.

[7] https://www.openrightsgroup.org/blog/online-abuse-why-management-liability-isnt-the-answer/

Q. What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

As discussed in previous answers, the lack of clarity on what the Bill means by "freedom of expression" is the fault line which leads to the rest of the Bill's weaknesses and omissions. Our joint letter to the Minister for Digital (see question 1) seeks clarity on these questions, and we would encourage the Committee to seek the same:

1. Clause 12(2) places a duty on services within scope to "have regard to the importance of (a) protecting users' right to freedom of expression within the law, and (b) protecting users from unwarranted infringements of privacy, when deciding on, and implementing, safety policies and procedures". This language is weaker than that for other duties under the Draft Bill and the duties on public authorities when it comes to human rights (e.g. section 6 of the Human Rights Act which simply prohibits authorities from acting in a way which is incompatible with human rights). Can the department give examples of how it considers this wording will make a difference in practice and what content will be protected as a consequence?
2. Clause 36(5) states that a service will be considered to have complied with the duty to protect freedom of expression if a provider takes steps described in a code of practice to protect safety. Does this mean codes of practice on safety overwrite any duty to protect freedom of expression?
3. Other than the requirement in clause 31(6), what duties will there be on Ofcom not to infringe on the rights to freedom of expression or privacy?
4. If clause 12 is considered by the department to be sufficient to protect the right to freedom of expression, could the department explain why it is also necessary to include separate provisions which protect journalistic content and content of democratic importance, and why clause 12 alone would not provide sufficient protection?

Q. Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

There are two unaddressed areas of tension within the draft Bill which deeply concern us as risks to freedom of expression.

The first area is the broad powers granted to the Secretary of State, under the draft Bill, to define and alter the boundaries of free speech as well as the privatised enforcement of those rules. This is exemplified, for example, in Part 2, Chapter 5, Section 33, which grants the Secretary of State with the power to "direct Ofcom to modify a code of practice...to ensure that the code of practice reflects government policy." This could be used as a means of chilling debate about topics that the government of the day does not find favourable, for example, legal migration[8], and sanctioning companies which permit discourse on the topic.

[8] https://www.openrightsgroup.org/blog/is-government-preparing-to-censor-discussions-about-migration/

The second area is the requirement, as set forth under Part 2, Chapter 4, for 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.[9] This is a means of using a tick-box compliance obligation as not just a trade barrier, but as a means of shutting out foreign companies, and the user-generated content on them, from being accessible in the UK, using child safety as the justification, on the open presumption that all service providers are complicit in child exploitation. This is not a healthy message to send about the attractiveness of Global Britain as a place to do business.

This clause furthermore compels foreign companies to collect personally identifiable data about all its UK visitors (*nb 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, and even if they are based in countries which have scant regard for the data privacy of those users.

Q. What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

In August, Iran announced an internet regulation bill which is so closely patterned on the UK's Online Safety Bill that even the name - the "Protection Bill" - mirrors our own.[10] Its provisions are directly inspired by the UK's aspirations. Government has said that it seeks to create a "world leading" internet regulation regime. In that light, it has succeeded, although perhaps not in the way it intended. This would not have been possible if the Online Safety Bill had a more thorough grounding in international human rights and freedom of expression standards. Our recommendation would therefore be that the government stops trying to collect international plaudits for its "world leading" legislation until it has a package worthy of that name, and that it centres the needs of the British public, rather than the needs of its public relations strategy.

We would also stress the need for government, and the Committee, to contrast the UK's Online Safety Bill approach, which regulates content but not design, with the emerging EU approach, as defined in the Digital Services Act. The latter regulation aspires to set constraints on platform design, process, and algorithmic reach, but *not* freedom of expression. Unlike the UK's aspirations, subjective and "legal but harmful" content remains explicitly out of scope, leaving the dissemination and amplification of explicitly illegal content the Act's focus. User rights and due process are also central to the regulation's aims, whereas its UK counterpart aims to centralise adversarial authority in government and the regulator.

From a commercial perspective, the DSA is establishing legal certainty and cooperative consistency for a global trading bloc of half a billion, whereas the UK's Online Safety Bill is creating ambiguity and an adversarial environment for a single nation of seventy

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

[10] https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/

million. Both service providers and end users will decide where to do business accordingly.