

BIG BROTHER WATCH

**Big Brother Watch
submission – Draft Online
Safety Bill Joint Committee
call for evidence**

September 2021

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Email: silkie.carlo@bigbrotherwatch.org.uk

Mark Johnson

Legal & Policy Officer

Email: mark.johnson@bigbrotherwatch.org.uk

INTRODUCTION

1. The Online Safety Bill, published in May of this year by the Department for Digital, Culture Media and Sport (DCMS) is a fundamentally flawed piece of legislation, destined to negatively impact the fundamental rights to privacy and freedom of expression in the UK. The proposed model, centred on imposing “duties of care” on all companies that enable people to interact with others online, to protect users from “harm”, will force these companies to act as privatised online police. Under the threat of penalties, this will compel online intermediaries to over-remove content.
2. We believe the Online Safety Bill in its current form is not fit to become law in a liberal democracy like the UK. In order to protect citizens’ free expression and the free flow of information, the Bill must be materially altered.
3. The legislation engages the fundamental rights to freedom of speech and privacy, protected by Article 10 and Article 8 of the European Convention on Human Rights (ECHR) respectively. The European Convention on Human Rights is clear that interference with these rights will only be lawful where they are provided by law, necessary and proportionate.¹ The presumption must rest in favour of protecting these rights and interference with them should come as a last resort.
4. The Bill has been widely criticised across the human rights sector. The international freedom of expression organisation, Article 19, has stated that if passed, the Bill would be “a chokehold on freedom of expression” and that it is “wary of legal frameworks that would give either private companies or regulators broad powers to control or censor what people get to see or say online”.² Gavin Millar QC, of Matrix Chambers, has also been highly critical of the legislation. Talking about the impact the Bill could have on rights around the world he said,

“As someone who has undertaken many free speech missions for international organisations to countries with repressive free speech regimes such as China, Turkey, Azerbaijan there is a real risk that this legislation, if passed, will be used to justify repressive measures aimed at closing down free speech on the internet in these countries.”³

5. As well as our profound concerns regarding the proposed duty of care, we believe that the Government’s approach to this legislation will effectively mean that the legal standard for permissible speech online will be set by platforms’ terms of use rather

¹The Human Rights Act, EHRC, <https://www.equalityhumanrights.com/en/human-rights/human-rights-act>

²UK: Draft Online Safety Bill poses serious risk to free expression, Article 19, 26 July 2021, <https://www.article19.org/resources/uk-draft-online-safety-bill-poses-serious-risk-to-free-expression/>

³Government’s Online Safety Bill will be “catastrophic for ordinary people’s freedom of speech” says David Davis MP, Index on Censorship, 23 June 2021, <https://www.indexoncensorship.org/2021/06/governments-online-safety-bill-will-be-catastrophic-for-ordinary-peoples-freedom-of-speech-says-david-davis-mp/>

than being clearly set out in statute. It is also our view that the broad definition of harm given in the legislation will result in a malleable, censorious online environment. Additionally, we believe that the regulatory model will give legal backing to a system often described as “surveillance capitalism”, demanding that online intermediaries monitor millions of users in order to enforce increasingly fortified terms of service.

6. We believe that as a minimum, provisions relating to so-called “legal but harmful” content should be removed from the face of the Bill (clause 11), that the scope of the legislation should not include private messaging services (clause 39) and that the legislation should not attempt to introduce age-verification via the back door.
7. In responding to this call for evidence, we have examined the Bill, section by section, looking in particular at the impact that legislation would have on fundamental rights. In doing so we will respond to the following questions:

Does the proposed legislation represent a threat to freedom of expression, or are the protections for freedom of expression provided in the draft Bill sufficient?

The draft Bill specifically places a duty on providers to protect democratic content, and content of journalistic importance. What is your view of these measures and their likely effectiveness?

Earlier proposals included content such as misinformation/disinformation that could lead to societal harm in scope of the Bill. These types of content have since been removed. What do you think of this decision?

What would be a suitable threshold for significant physical or psychological harm, and what would be a suitable way for service providers to determine whether this threshold had been met?

Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

How much influence will a) Parliament and b) The Secretary of State have on Ofcom, and is this appropriate?

Does the draft Bill make appropriate provisions for the relationship between Ofcom and Parliament? Is the status given to the Codes of Practice and minimum standards required under the draft Bill and are the provisions for scrutiny of these appropriate?

PART 1 – DEFINITIONS

Clause 3 – Meaning of “regulated service”

8. Part 1, clause 3 sets out the scope of the legislation and describes what constitutes a “regulated service” for the purposes of the regulatory framework. This includes “user to user” and “search” services that have “links to the United Kingdom”. Excluded from the scope of the legislation are emails, SMS messages, MMS messages, comments and reviews on provider content, one-to-one live aural communications, paid-for advertisements and news publisher content. However, under clause 3(9) the Government has also reserved the right to extend the duty of care to comments and reviews on provider content as well as one-to-one live aural communications if it is deemed “appropriate” based on the “risk of harm”⁴. This could mean, for example, that Zoom could have a duty to surveil calls to impose anti-harm rules.
9. Additionally, clause 3 (8) of the legislation awards the Secretary of State the power, through regulations, to exempt services of a particular description if he deems that the threat of “harm” on such services is low. As is the case throughout the Online Safety Bill, this provision gives the Secretary of State undue power to influence the regulatory framework and if exercised, this power could have serious implications from a markets and competition perspective.
10. The way in which the Bill covers any services with “links to the UK” also brings into question the extent to which the legislation could apply to communications that are sent from overseas but encountered by users in the UK. This has the potential to bring provisions within the regulatory framework into direct conflict with the laws of those states from which communications (viewed by users in the UK) are sent. For example, the Polish Government have proposed a “social media free speech” law. The proposed law would prevent online intermediaries from removing content or banning users who do not break Polish laws⁵. In the event that this legislation and the Online Safety Bill were passed, the ability of social media users in Poland and the UK to communicate directly would be severely hampered by contradictory laws. In such a case, should a user in Poland issue a post on a large social media platform which, although lawful in Poland, could be viewed by users in the UK and deemed as “harmful” under the online safety framework, the intermediary in question would be posed with a complex legal

⁴ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

⁵ Poland proposes social media ‘free speech’ law, BBC News, 15 January 2021, <https://www.bbc.co.uk/news/technology-55678502>

dilemma. This could move us towards national digital silos and directly threaten the transnational interconnectedness of the internet as a whole.

11. The scope of the legislation has also been criticised by Article 19, who have raised concerns about the breadth of the regulatory framework. In particular, the group have raised concerns about the extension of the regulatory framework to private messaging services, where it is likely to undermine the privacy guaranteed by end-to-end encryption.⁶

PART 2 – PROVIDERS OF REGULATED SERVICES: DUTIES OF CARE

12. At the heart of the Online Safety Bill is a shift towards increased liability on social media companies, who, under obligations placed on them through the legislation, must take responsibility for the speech and even private messages of members of the public on their sites. Such a move would have serious ramifications for freedom of expression and privacy online. Part 2 of the Bill sets out the new “duties of care” that the legislation places on all in-scope services.

Clause 5 - Providers of user-to-user services: duties of care

13. Chapter 2 of Part 2 places duties of care on providers of regulated user-to-user services. According to the legislation, all regulated user-to-user services will be obliged to fulfil “illegal content risk assessment” duties, “illegal content” duties, duties regarding freedom of expression and privacy, duties regarding reporting and redress and record keeping and review duties.⁷ The legislation also places additional duties on services which “are likely to be accessed by children” and Category 1 (larger services) including a duty “to protect adults’ safety” even where the content is not illegal.⁸
14. The notion of duties of care was borne out of a proposal, put together by Professor Lorna Woods and Will Perrin of the Carnegie Trust in 2018/19, on tackling “internet harm”. The model proposed a singular duty of care placed upon online intermediaries who would thus be liable for the welfare of online users in a similar vein to workplace health and safety regulations and the obligations an employer has to maintain the safety of employees. In doing so, the proposal cited the 1974 Health and Safety at Work

⁶ UK: Draft Online Safety Bill poses serious risk to free expression, Article 19, 26 July 2021, <https://www.article19.org/resources/uk-draft-online-safety-bill-poses-serious-risk-to-free-expression/>

⁷ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

⁸ Ibid.

Act.⁹ The paper indicated that such a regime should be overseen by an independent regulator and proposed that Ofcom undertake this task.

15. This approach was criticised by civil society groups and members of the legal profession. Internet lawyer Graham Smith warned about the dangers of employing such an approach as a blanket measure for all internet regulation, pointing out that duties of care when it comes to risk of physical injury in public or semi-public spaces are often sector specific. He also warned of the unsuitability of this approach where a platform has to take responsibility for and govern the interactions of users.¹⁰
16. The freedom of expression NGO, Index on Censorship, has also been highly critical of the duty of care model. Arguing that it will put freedom of expression in “peril”, the organisation set out its concerns in paper on the duty of care, asserting that it “will reverse the famous maxim, ‘published and be damned’, to become, ‘consider the consequences of all speech, or be damned’. It marks a reversal of the burden of proof for free speech that has been a concept in the common law of our country for centuries.”¹¹ In a report published by the House of Lords Communications and Digital Committee, which was largely critical of the Government’s Online Safety Bill, the Committee documented many of the problems with the duty of care model and acknowledged that there are many “legitimate concerns” regarding such an approach.¹²
17. The deployment of a liability model developed in tort law, to regulate and likely curtail free speech, is highly inappropriate. We are deeply concerned by this model which would mark a significant step-change in how free expression is protected in the UK. A duty of care on the part of online intermediaries, which makes platforms liable for the interactions of individuals on the internet, is gravely threatening to free expression. This approach, which is preventative in its outlook, will prove to be excessively censorious as companies will over-zealously remove content in adherence with their obligations.

Clauses 7 and 8 – Risk assessment duties and timing of risk assessment under section 7

⁹ Lorna Woods and William Perrin, “Internet Harm Reduction: a proposal”, Carnegie UK Trust Blog, 30 January 2019, <https://www.carnegieuktrust.org.uk/blog/internet-harm-reduction-a-proposal/>

¹⁰ Smith, G. Graham Smith, “Take care with that social media duty of care”, Cyberlegal, 19 October 2018, <https://www.cyberleagle.com/2018/10/take-care-with-that-social-media-duty.html>

¹¹ *Right to type: How the “duty of care” model lacks evidence and will damage free speech*, Index on Censorship, June 2021, <https://www.indexoncensorship.org/wp-content/uploads/2021/06/Index-on-Censorship-The-Problems-With-The-Duty-of-Care.pdf>

¹² *Free for all? Freedom of expression in the digital age*, House of Lords Communications and Digital Committee, July 2021, <https://committees.parliament.uk/publications/6878/documents/72529/default/>

18. Clauses 7 and 8 set out the first of the duties that the legislation would mandate online intermediaries to comply with - namely, risk assessment duties. These provisions compel companies to undertake risk assessments relating to (i) illegal content, (ii) harm to children from content that is not illegal, and (iii) harm to adults from content that is not illegal.¹³
19. While a greater level of transparency from online intermediaries is in and of itself a good thing, these provisions are not without problems and may themselves impact upon the extent to which individuals in the UK can access a free flow of information unimpeded. For example, under clause 8, the legislation sets out that an online service that is not currently operating in the UK must undertake the relevant risk assessments before the service can be accessed by users in the UK. Under such a regulatory burden, it may be the case that online intermediaries based overseas instead opt for UK users not to be able to access their services.
20. As with other sections of the Bill, we also reject the nebulous concept of "content which is harmful to adults", which is inherent to the referenced risk assessment duties for adults. We discuss this in greater detail later in this document, with regard to operational safety duties.

Clause 9 - Safety duties about illegal content

21. Clause 9 sets out a key operational user safety duty, which applies to all regulated services in scope and is central to the legislation. It reads as follows:

9 (3) A duty to operate a service using proportionate systems and processes designed to—

(a) minimise the presence of priority illegal content;

(b) minimise the length of time for which priority illegal content is present;

(c) minimise the dissemination of priority illegal content;

(d) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.¹⁴

22. Introducing obligations of this nature marks a stark departure from a traditional regulatory approach towards online platforms, held in both the EU and US, which gives intermediaries immunity from liability for the user-generated content on their sites.

¹³ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf

¹⁴ Ibid.

This principle has been applied in regulatory frameworks with the specific intention of protecting the free expression and privacy of users online. A standard that directly applies is Article 15 of the EU's E-Commerce Directive (this technically still applies to the UK as "EU retained law"), which prohibits member states from imposing general monitoring obligations on social media companies operating within their jurisdictions.¹⁵

23. The duties set out in clause 9 require social media platforms to make judgements on the legality of content and effectively deputise these companies to act as online police. While clause 9 (3) refers to priority illegal content (that which is specified by the Secretary of State in subsequent regulations), platforms will also be under an obligation to set out in their terms of service how they will "protect users" from all illegal content and to uphold these terms of service consistently.¹⁶ This is particularly problematic when it comes to judgements on the legality of controversial expression.

24. To take one example of this, the Communications Act 2003 criminalises communications that are deemed to be "grossly offensive".¹⁷ This legislation has proved to be deeply controversial since it was passed and has resulted in the criminalisation of speech that merely causes offence. In the case of one prominent example, *Chambers v Director of Public Prosecutions (2012)*, the High Court overruled the verdict of a magistrate's court which had found the defendant guilty of sending a "menacing electronic communication" under the Act (in this case for an offensive tweet).¹⁸ This demonstrates the complexity of the law in this area and the care that is required when considering the permissibility of speech.

25. Under their obligations in the Online Safety Bill, social media companies would be obliged to set out in their terms of use how they would tackle illegal content such as "grossly offensive" material made illegal by the Communications Act 2003, and uphold these terms "consistently". Under the threat of penalties for non-compliance, this could result in social media companies being overly censorious in their removal of any content that remotely risks crossing this threshold.

26. The courts, Crown Prosecution Service and the police are all bound by a duty under the Human Rights Act 1998 to act in accordance with the European Convention on

¹⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>

¹⁶ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

¹⁷ Communications Act, 2003, <https://www.legislation.gov.uk/ukpga/2003/21/section/127>

¹⁸ *Robin Hood Airport tweet bomb joke man wins case*, BBC News, 2012, <https://www.bbc.co.uk/news/uk-england-19009344>

Human Rights, including protecting the right to freedom of expression. In practice this often means that no action is taken against speech which does cross the threshold of "grossly offensive" if this would violate the right to free expression. However, no equivalent duty falls upon the platforms in the course of the Online Safety Bill.

27. The rule of law must be upheld online, but if speech is alleged to cross the threshold into illegality, it should be a matter for the police to investigate and the courts to adjudge.
28. A swift social media takedown procedure, obligated under the threat of penalties for non-compliance, could inadvertently make users less safe if they are not made aware of potential threats or if potential evidence is speedily removed.

Clause 10 - Safety duties for services likely to be accessed by children

29. Clause 10 sets out safety duties that intermediaries must undertake with a focus on users who are children. The provisions within the clause effectively demand that regulated services take responsibility for the safety of children who may access their site. Clause 10 (3) states:

(3) A duty to operate a service using proportionate systems and processes designed to—

(a) prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children;

(b) protect children in age groups judged to be at risk of harm from other content that is harmful to children (or from a particular kind of such content) from encountering it by means of the service.¹⁹

30. In this instance (and as it is referred to throughout the legislation), priority content includes designated categories set out by the Secretary of State. "Other content that is harmful to children" is later defined as content that is not necessarily illegal but may pose a "risk of the content having, or indirectly having, a significant adverse physical or psychological impact on a child of ordinary sensibilities".²⁰

31. It is vital that children are protected online but this legislation would result in internet-wide censorship at intolerably strict levels. There are many forms of content that could

¹⁹ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

²⁰ Ibid.

be considered “harmful” for children to view but should not be censored from user-to-user platforms - for example, adult humour or the documentation of crime or violence.

32. The Online Safety Bill suffers throughout from being overly broad in its aims. Rather than focus on upholding the rule of law and ensuring platforms take steps to work with law enforcement to protect children from genuinely illegal content online, this Bill seeks to eradicate nebulous concepts of harm, which would result in a more restricted online experience for everyone.

33. The legislation states that the obligations set out in Clause 10 must be integrated into services’ terms of use and applied consistently.²¹

34. Clause 10 (9) also states:

“The duties in this section extend only to such parts of a service as it is possible for children to access.”²²

35. Given the huge popularity of social media and the vast number of users on each of the major platforms, the likelihood that a social media site may be accessed by children is high in any case. This means that unless a platform undertakes invasive age verification checks and then age-gates user-generated content at a granular level, content moderation on the site in question must be tailored for children.

36. This directly threatens both free expression and privacy rights online. The measures will force platforms to comply with higher thresholds for the acceptability of content unless they verify users’ age using ID. This means mandating age verification and would be hugely damaging to privacy rights online. Online anonymity is crucially important to journalists, human rights activists and whistleblowers all over the world. Even tacit attempts to undermine online anonymity here in the UK would set a terrible precedent for authoritarian regimes to follow and would be damaging to human rights globally.

37. Such a measure would also mean that internet users would have to volunteer even more personal information to the platforms themselves, which would likely be stored in large centralised databases. Further, many people across the UK do not own a form of ID and would directly suffer from digital exclusion.

²¹ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

²² Ibid.

The Bill should not force online platforms to introduce mandatory age verification via the back door.

Clause 11 - Safety duties protecting adults: Category 1 services

38. In addition to their duties relating to potentially illegal content and content that may be “harmful to children”, “Category 1 services” (large social media companies) are obliged to fulfil additional duties “to protect adult online safety” including a duty to address “content that is harmful to adults”. This is set out in the legislation as follows:

11 (2) A duty to specify in the terms of service—

(a) how priority content that is harmful to adults is to be dealt with by the service (with each such kind of priority content separately covered), and

(b) how other content that is harmful to adults, of a kind that has been identified in the most recent adults’ risk assessment (if any kind of such content has been identified), is to be dealt with by the service.

(3) A duty to ensure that—

(a) the terms of service referred to in subsection (2) are clear and accessible, and

(b) those terms of service are applied consistently²³

39. As with clause 10, “priority content” means categories of content specifically identified by the Secretary of State, whereas “other content which is harmful to adults” is later defined in clause 46 as where there is a “risk of the content having, or indirectly having, a significant adverse physical or psychological impact on an adult of ordinary sensibilities”.²⁴

40. The provisions above are the most egregious threat to freedom of expression posed by any legislation in the UK in recent times. The notion of a state-backed censorship of lawful expression contravenes long-held human rights standards on protecting freedom of expression. The state should not curtail or endorse the censorship of expression which is lawful. Limitations on free speech should be exercised only where necessary, where they are proportionate and where they are clearly prescribed in law.

²³ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

²⁴ Ibid.

41. Once again, the threshold of “harm” that online platforms would be obliged to prevent on their sites is intolerably low. The legislation sets out a definition of harmful content (and therefore harm) which category 1 platforms must endeavour to tackle through their terms of use. The definitions set out in Cl. 46 are:

(3) Content is within this subsection if the provider of the service has reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on an adult of ordinary sensibilities

Or

(5) Content is within this subsection if the provider of the service has reasonable grounds to believe that there is a material risk of the fact of the content’s dissemination having a significant adverse physical or psychological impact on an adult of ordinary sensibilities, taking into account (in particular) —

(a) how many users may be assumed to encounter the content by means of the service, and

(b) how easily, quickly and widely content may be disseminated by means of the service.²⁵

42. In order to protect freedom of expression and limit the possibility of overzealous or censorious enforcement, restrictions on permissible speech should always be clearly defined in law. However, a “risk of... having a significant adverse physical or psychological impact”, even “indirectly”,²⁶ is an overly broad definition and threatens application that would be damaging to free speech. An adverse psychological impact could, for example, refer to an offensive joke or footage of an emergency situation. It could even constitute the documentation of social injustice, such as the video of George Floyd’s murder which changed debates internationally about race, justice and authority. Such content might cause distress but is important to see and share for the benefit of society.

43. The Bill also gives power to the Secretary of State to designate, through secondary legislation, specified categories of “harmful content” which Ofcom must incorporate into its codes of practice. While the Government have set out a definition of “harm” in the Bill, what specific “harms” will be set out in secondary legislation remain opaque, and subject to change.

²⁵Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

²⁶Ibid.

44. This level of influence over the regulatory regime (alongside a number of other provisions throughout the legislation), will give the government of the day a huge amount of executive power to ultimately influence the permissibility of speech online. It is also unclear whether these specific “harms” will even have to meet the aforementioned standard of posing a risk of having an “adverse physical or psychological impact”. The Bill defines “priority content that is harmful to adults”, which the Secretary of State sets via secondary legislation, as “content of a description designated as such in [those] regulations” (cl. 46(9)) – that is, harmful content is whatever the Secretary of State says it is.

45. Unsurprisingly, clause 11 has been roundly criticised by freedom of expression groups in the strongest of terms; a warning which must not go unheeded by policymakers. Index on Censorship criticised this provision in a paper, which stated:

“‘Legal but harmful’ has been defined in the draft Bill as causing ‘physical or psychological harm’, but how can this be proved? This definition opens up significant problems of subjectivity. The reason, in law, we do not use this definition for public order offenses is that it is hard for citizens to understand how their words (written or spoken) could cause psychological harm in advance, especially on the internet where we do not know our audience in advance.”²⁷

46. Concerns around the breadth of the definition of harm have also been expressed by internet lawyer, Graham Smith:

“What is an adverse psychological impact? Does it have to be a medically recognised condition? If not, how wide is it meant to be? Is distress sufficient? The broader the meaning, the closer we come to a limitation that could mean little or nothing more than being upset or unhappy. The less clear the meaning, the more discretion would be vested in Ofcom to decide what counts as harm, and the more likely that providers would err on the side of caution in determining what kinds of content or activity are in scope of their duty of care.”²⁸

47. In a blog on the Government’s Online Harms agenda, the lawyer Ashley Hurst previously wrote that the Government should “focus on what is illegal and defined, not legal and vague.”²⁹ An article by digital rights organisation, Matrix, also referred to

²⁷ Right to type: How the “duty of care” model lacks evidence and will damage free speech, Index on Censorship, June 2021, <https://www.indexoncensorship.org/wp-content/uploads/2021/06/Index-on-Censorship-The-Problems-With-The-Duty-of-Care.pdf>

²⁸ Smith G. *The Online Harms edifice takes shape*, Cyberleagle, December 2020, <https://www.cyberleagle.com/2020/12/the-online-harms-edifice-takes-shape.html>

²⁹ Hurst, A. Tackling misinformation and disinformation online, Informm, <https://inform.org/2019/05/16/tackling-misinformation-and-disinformation-online-ashley-hurst/>

these provisions within the legislation as an attempt at “centralising and regulating relative morals”³⁰.

- 48.** However, most recently and most prominently, the House of Lords Communications and Digital Committee recommended that clause 11 be removed from the Bill entirely. In the Committee’s report, which followed a Parliamentary inquiry into freedom of expression online, the Committee stated:

“We do not support the Government’s proposed duties on platforms in clause 11 of the draft Online Safety Bill relating to content which is legal but may be harmful to adults. We are not convinced that they are workable or could be implemented without unjustifiable and unprecedented interference in freedom of expression. If a type of content is seriously harmful, it should be defined and criminalised through primary legislation. It would be more effective — and more consistent with the value which has historically been attached to freedom of expression in the UK — to address content which is legal but some may find distressing through strong regulation of the design of platforms, digital citizenship education, and competition regulation.”³¹

- 49.** Whilst we believe that the model upon which the Online Safety Bill, clause 11 is arguably the single most damaging provision for freedom of expression. The idea that social media platforms could be compelled to remove broad categories of so called “harmful” content would lead to two distinctive tiers of permissible speech in the UK in the online and offline worlds. Not only would our online public squares be restricted and censored but free speech more broadly would be chilled as a result.

If we are to avert the Online Safety Bill doing permanent damage to the right to free speech in the UK, as a minimum, clause 11 should be removed from the Bill.

Clause 12 - Duties about rights to freedom of expression and privacy

- 50.** In addition to the risk assessment duties and operational safety duties, the Bill sets out a number of additional duties relating to freedom of expression and privacy, protecting “journalistic content” and content which is of “democratic importance”. However, far from creating effective protections in these areas, the provisions create points of conflict within the legislation and are, nevertheless, largely outweighed by safety duties that will encourage platforms to over-remove content.

³⁰Almeida, D. How the UK's Online Safety Bill threatens, Matrix, 19 May 2021, <https://matrix.org/blog/2021/05/19/how-the-u-ks-online-safety-bill-threatens-matrix>

³¹Free for all? Freedom of expression in the digital age, House of Lords Communications and Digital Committee, 22 July 2021, <https://committees.parliament.uk/publications/6878/documents/72529/default/>

51. The duties relating to freedom of expression and privacy, which engage all regulated services, are particularly weak and read as follows:

12 (2) A duty 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.³²

52. Unlike the previously considered operational safety duties, which compel companies to “minimise” illegal or so-called harmful content on their sites, this duty only instructs tech companies to “have regard to the importance” of free expression and privacy.

53. The very nature of the legislation, which compels social media companies to take liability for content on their sites, means that platforms of this kind will be forced to monitor and surveil users more than ever before. This approach is a serious threat to online privacy and cannot be remedied by asking platforms to simply give “regard” to this fundamental right.

54. In fact, by mandating so called “technology notices” (see clause 64)³³ the Bill will compel social media companies to read the messages of their users to scan for potential “harm”. Far from “reining in” big tech companies, this legislation gives foreign companies license to spy on the communications of British citizens, supporting an exploitative business model that erodes privacy rights.

55. The duties specifically imposed upon category 1 services are no more conducive to effectively protecting freedom of expression on large social media platforms than the aforementioned requirements. They compel platforms to undertake impact assessments on the way in which their systems and processes affect freedom of expression and privacy on the platform and set out how they might remedy any threats to these rights on their platform. Once again, this duty is significantly weaker than the operational safety duties and will do little to materially protect free expression online. It also fails to acknowledge that most of the major companies already do limit free expression far beyond that which is prescribed in domestic law, and fails to offer policies to materially remedy this.

56. The weakness of these provisions was fairly characterised by internet Lawyer Graham Smith when he said:

³²Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

³³ Ibid.

*“No obligation to conduct a freedom of expression risk assessment could remove the risk of collateral damage by over-removal. That smacks of faith in the existence of a tech magic wand. Moreover, it does not reflect the uncertainty and subjective judgement inherent in evaluating user content, however great the resources thrown at it.”*³⁴

57. Under the weight of pressure from civil society groups and following recent high-profile cases of “big-tech” censorship, the Government have embarked upon attempts to rebrand the Bill as legislation which could in fact protect freedom of expression. This is doublespeak and is patently not true given the way in which the legislation will force the regulation and removal of lawful content.

58. The legislation addresses the point of conflict between the operational safety duties and duties to protect free expression and privacy in clause 36 (5):

36 (5) A provider of a regulated user-to-user service is to be treated as complying with the duty set out in section 12(2) (duty about freedom of expression and privacy) if the provider takes such of the steps described in a code of practice which are recommended for the purposes of compliance with a Chapter 2 safety duty (so far as the steps are relevant to the provider and the service in question) as incorporate safeguards for—

(b) the protection of users’ right to freedom of expression within the law,

or

*(b) the protection of users from unwarranted infringements of privacy.*³⁵

59. This suggests that so long as platforms follow the code of practice on operational safety duties, this will be sufficient to comply with their free expression and privacy duties. This demonstrates the inherent weakness of the duties to have regard to freedom of expression and privacy, which pay lip service to these fundamental rights in a Bill which otherwise damages them.

Clause 13 - Duties to protect content of democratic importance: Category 1 services

60. In addition to the aforementioned duties, the Online Safety Bill also places an obligation upon category 1 regulated services to protect content of “democratic importance” and “journalistic content”. The Government claim that this legislation will

³⁴Smith, G. *Harm Version 3.0: the draft Online Safety Bill*, Cyberleagle Blog, May 2021, <https://www.cyberleagle.com/2021/05/harm-version-30-draft-online-safety-bill.html>

³⁵Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

not threaten free expression online - however, if this is the case it begs the question of why these carve-outs are necessary.

61. These provisions, clearly borne out of concern that platforms could reprimand politicians in a similar way to former President Trump, include an obligation on platforms to apply the safety duties in a politically neutral manner:

13 (3) A duty to ensure that the systems and processes mentioned in subsection (2) apply in the same way to a diversity of political opinion.³⁶

62. This demonstrates a recognition on the part of the Government that the fortification of and mandated adherence to platforms' terms of use will create a more politicised, censorious environment online. However, these provisions effectively exempt politicians themselves from this new system of regulation.

63. In describing what content of "democratic importance" would constitute, the Bill states:

6 (b) the content is or appears to be specifically intended to contribute to democratic political debate in the United Kingdom or a part or area of the United Kingdom.³⁷

64. The vague nature of this categorisation will only create additional complications for the platforms as they are simultaneously told to deal with content which could subjectively be considered "harmful", but not that which is considered a part of "democratic political debate". Given the sweeping nature of this description and the regulatory burden dealt to them, it is likely that intermediaries will take a narrow interpretation of this provision and give additional protection to the expression of elected officials. As a result, these exemptions present as one rule for politicians, who will have greater privileges to speak freely online, and another rule for the population at large.

Clause 14 - Duties to protect journalistic content: Category 1 services

65. The carve-out in clause 14 requires online platforms to consider whether content is "journalistic" when enforcing their terms of use, and to create an expedited appeals process for the reinstatement of removed journalistic content. When setting out a duty upon category 1 services to protect "journalistic content", the Bill states that platforms have:

³⁶Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

³⁷Ibid.

14 (4) A duty ... to make a dedicated and expedited complaints procedure available to a person who considers the content to be journalistic content³⁸ (Where the complainant is the person who shared or created the content in question.)

66. Services are also obligated to create such a dedicated and expedited complaints process for *all* users where action has been taken by the platform on “journalistic content”.³⁹ However, the legislation provides only a loose definition of what “journalistic content” should constitute and states that platforms are to set out a means of identifying journalistic content. The definition given in the Bill is as follows:

14 8 (a) the content is—

(b) news publisher content in relation to that service, or

(ii) regulated content in relation to that service;

(b) the content is generated for the purposes of journalism; and

(c) the content is UK-linked.

67. It is unclear how freelance or citizen journalism would fit within this description. A democratising effect of the internet has been the opening of spaces for marginalised voices, blogs, campaign journalism and more disintermediated news sharing. Citizen journalism online has made a significant contribution to media as a whole, offering new and diverse perspectives, rapid story-telling, inclusive media and audience participation. Citizen journalism has played a major role in 21st Century political events,⁴⁰ including the Occupy movement and the Arab Spring, and this has relied on the more equal playing field online for individuals to gain exposure and generate revenue. If carve-outs are only afforded to the journalists and media operators that the social media companies choose, this unhealthy monopolisation will only be exacerbated.

Clause 15 - Reporting and redress duties

68. Clause 15 sets out the obligations placed upon platforms to ensure that sufficient reporting and complaints systems are integrated into their systems and processes in order that they fulfil the aforementioned duties. This includes the mandating of complaints procedures for users who have had their content removed because the service provider in question believed that it may be illegal, harmful to children or harmful to adults.

³⁸Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

³⁹Ibid.

⁴⁰Citizen Journalism, Encyclopaedia Britannica, <https://www.britannica.com/topic/citizen-journalism>

69. Whilst the integration of effective and thorough appeals processes is a progressive step when it comes to protecting freedom of expression online, this measure will make little difference if the bar for what is considered acceptable online is considerably lowered.

Clause 16 - Record-keeping and review duties

70. Clause 16 obliges platforms to keep a record of all risk assessments conducted under clause 7 and to keep a record of steps taken to comply with duties that are not described in the codes of practice. Greater levels of accountability and transparency from online intermediaries is welcomed.

Chapter 3 - Providers of search services: duties of care

Clauses 17-25

71. Through clauses 17-25, Chapter 3 replicates those provisions set out in Chapter 2 but for search services as opposed to user-to-user services.

72. The right to freedom of expression in an online setting not only concerns the ability of individuals to impart information but also to receive it. In this regard, a free flow of information and the right to freedom of expression go hand in hand.

73. Clauses 17-25 transpose many of the duties set out in Part 2, Chapter 2 (for user-to-user services) and apply them to search services. This includes illegal content risk assessment duties, risk assessment duties specifically for services “likely to be accessed by children”, safety duties relating to potentially illegal content and safety duties where the service is “likely to be accessed by children”. Unlike with user-to-user services, there is no stipulation of obligations based on the size of the service in question and as such, no additional duties for larger services.

74. As with user-to-user services, the legislation imposes further duties upon search services to “have regard to” freedom of expression and privacy but these are weak checks on an otherwise deeply restrictive model. Reporting, redress and record-keeping duties also apply.

75. As with user-to-user services, we are deeply concerned that the broad definitions and the weight of the obligations placed upon these intermediaries will mean that search services feel obliged to censor heavily. As such, this runs the risk of stifling the free flow of information online. This is a retrograde step given the otherwise democratising power of the internet.

76. Of all of the major digital markets, the field of search engines is among the most monopolised, with Google overwhelmingly acting as the major market player. Given

the expensive regulatory costs of the proposed online safety regime, far from taking power from online platforms like Google, this legislation will obstruct market entry to potential new services and entrench powerful actors such as Google.

Chapter 4 – Assessment about access by children

Clauses 26 and 27 - Assessment about access by children and timing of assessment under clause 26

77. Clause 26 sets out obligations platforms must undertake to establish how likely it is that their service is used by children. Clause 26 (4) states:

(4) The “child user condition” is met in relation to a service, or a part of a service, if—

(a) there are a significant number of children who are users of the service or of that part of it, or

(b) the service, or that part of it, is of a kind likely to attract a significant number of users who are children

78. Clause 26 (5) states:

(5) For the purposes of this Part, a service is to be treated as “likely to be accessed by children” if the provider’s assessment of the service concludes that—

(a) it is possible for children to access the service or any part of it, and

(b) the child user condition is met in relation to—

(i) the service, or

(ii) a part of the service that it is possible for children to access.⁴¹

Clause 27 - Timing of assessment under section 26

79. Clause 27 states that an online service that is not currently operating in the UK must undertake the assessments set out in clause 26 before the service can be accessed by users in the UK. As with clause 8, this regulatory burden may lead online intermediaries based overseas to restrict UK users from accessing their services. This poses a direct threat to the free flow of information to the UK.

⁴¹ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Chapter 5 – Codes of practice

Clause 29 - Codes of practice about duties

- 80.** Building on the duties of care, clause 29 instructs the newly appointed regulator, Ofcom, to draft codes of practice setting out how social media companies can fulfil their obligations when it comes to regulating content that is deemed to be illegal or “legal but harmful”. Compliance with the relevant duties is met if a platform takes the steps set out in the codes of practice, which they will have to integrate into their company’s “systems and processes”.⁴²
- 81.** The effect of this step is to fortify social media companies’ terms of use, ensuring that they are upheld, and to clearly identify companies that fail to comply, who risk sanction. Whilst companies consistently upholding their terms and conditions might be seen by some as a good in and of itself, it is widely recognised that the online data trade means many online companies’ terms and conditions are primarily designed for their own economic benefit and legal protection rather than to protect the interests of their users. The terms of service model regulating the relationship between platform and user effectively gives many platforms absolute power and complete discretion as to their application of it.⁴³ As such, it would seem a controversial position for a Government-appointed regulator to oversee private companies in effectively upholding those terms and conditions – sets of rules that are not neutral, and which have complex implications.
- 82.** Ensuring companies comply with their terms and conditions raises particularly significant issues where those terms apply to speech issues. Platforms’ rules (if not always their enforcement) typically go much further than domestic laws in limiting speech. For example, Facebook’s community standards include policies on ‘objectionable content’ that go far beyond the limits set in domestic law. It would be distinctly wrong for a regulator to oversee the fulfilment of terms and conditions that facilitate the censorship of lawful speech. For the regulator to adhere to and endorse speech standards set in private ‘community standards’ would show a worrying lack of commitment to the laws and case law on free speech that have evolved in this country over many years. Such proposals would make the Government-appointed regulator complicit in limitations on free speech.

Clause 30-31

⁴²Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

⁴³ For further analysis, see *Digital Constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms* – N. Suzor, July 2018, in *Social Media + Society*

83. Clause 30 states that in designing the codes of practice, Ofcom must ensure that they are in line with a set of “Online Safety Objectives” which may be amended by the Secretary of State. As discussed in succeeding paragraphs, this, alongside other measures, would allow the Government of the day undue influence over this regulatory framework and as such control over online discourse.

Clauses 32-35 - Approval of codes of practice, Secretary of State’s power of direction, Publication and review of codes of practice, Minor amendments of codes of practice

84. A running theme throughout the entirety of the Online Safety Bill is the way in which the Government awards itself a huge amount of executive power to shape this proposed system of online speech moderation and as a result, to influence discourse.

85. Clauses 32-35 set out the processes by which Ofcom’s codes of practice may be approved. This includes initial sight of the proposed codes by the Secretary of State who can effectively veto and give “direction” to the codes:

33 (1) (a) to ensure that the code of practice reflects government policy, or

(b) in the case of a code of practice under section 29(1) or (2), for reasons of national security or public safety.⁴⁴

86. Ofcom is obliged to comply with the direction.

87. This is incredibly dangerous and opens the entirety of this flawed system up to politicisation. The Secretary of State’s power of direction would allow the Government to pressure Ofcom into writing codes of practice that would shape the permissibility of categories of online content based on the political mood.

88. As set out in clause 32, approval of the codes of practice is done by statutory instrument, via a negative procedure. This is entirely inadequate for the purposes of shaping the permissibility of speech online as MPs would have no automatic vote on the codes. If MPs force a vote, the debate would last for no more than 90 minutes before a yes or no vote, with parliamentarians denied the opportunity to mend the substance of the code.

89. It is wholly inappropriate for our right to free expression to be curtailed by secondary legislation which is unamendable and allows for little parliamentary oversight. In these circumstances, the power exercised by the online regulator and Secretary of State would bypass the full democratic process, creating a two-tier speech system whereby

⁴⁴Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

the increasingly ubiquitous online tier would be, for all intents and purposes, untethered from decades of existing law and highly susceptible to political swings of the day. This situation is precisely what Government should be seeking to prevent – not endorse.

90. According to clause 34 (6), the influence that the Secretary of State has over the codes of practice is constant:

34 (6) The Secretary of State may at any time require OFCOM to review a code of practice prepared under section 29(1) or (2).⁴⁵

91. Similarly, Ofcom must notify and seek approval from the Secretary of State for any of their own amendments to the codes of practice.⁴⁶

92. The architects of the Online Safety Bill’s framework, Professor Lorna Woods and Will Perrin of the Carnegie Trust, raised concerns about the undue executive power over the framework that is granted by the legislation. In a response to the publication of the legislation, the Trust argued:

“To meet the UK’s international commitments on free speech, there should be a separation of powers between the Executive and a communications regulator. The draft Bill takes too many powers for the Secretary of State. These should be reduced, removing in particular the Secretary of State’s power to direct OFCOM to modify its codes of practice to bring them in line with government policy.”⁴⁷

Clause 36 - Relationship between duties and codes of practice

93. Clause 36 establishes the relationship between codes of practice and intermediaries’ respective duties. Adherence to the codes in most cases will result in fulfilment of the operational safety duties. The notion that online expression should ultimately be governed by codes of practice set by a regulator and led solely by the executive are deeply concerning.

Chapter 6 – Interpretation of Part 2

Clauses – 41-47

⁴⁵ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

⁴⁶ Ibid.

⁴⁷ The Draft Online Safety Bill: Carnegie UK Trust initial analysis, Carnegie Trust, June 2021, https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2021/06/16171457/draft-OSB-CUKT-response-FINAL-1.pdf

- 94.** Clauses 41-47 establish the meanings of “illegal content”, “content which is harmful to children” and “content which is harmful to adults”.
- 95.** In doing so, the legislation identifies “illegal content”, “priority illegal content”, “primary priority content that is harmful to children”, “priority content that is harmful to children”, “non-designated content that is harmful to children”, “priority content that is harmful to adults” and “content that is harmful to adults”.
- 96.** These broad definitions of harm will result in overzealous application, the quashing of free expression, and undue influence of the government of the day in defining “priority” categories of content. Furthermore, the Bill has also been criticised for being excessively complicated.
- 97.** Article 19 has publicly criticised the Bill in this regard, saying “It is obvious that this kind of scheme will benefit lawyers, not freedom of expression or privacy.”⁴⁸
- 98.** Further, where discussing the nebulous concept of content which is “harmful to adults”, the Government have attempted to create an objective test to determine, in particular, whether “there is a material risk of the content having, or indirectly having, a significant adverse psychological impact”.⁴⁹
- 99.** However, harmful speech is highly subjective, as internet lawyer Graham Smith stated:
- “The problem with trying to define harmful content is that speech is subjectively perceived and experienced. Different people respond to reading, hearing or viewing the same content in different ways.”⁵⁰*
- 100.** In attempting to assert objectivity to assess the impact of online expression, a relatively subjective process, the definition of “content that is harmful to adults” set out in clause 46 requires that the content in question must risk such an outcome to an “an adult of ordinary sensibilities”.
- 101.** The appropriateness of such a definition was brought into question by Graham Smith, who argued that such a term does not nullify subjectivity from the measure of harm.⁵¹ He also noted that such a test ordinarily refers to a “reasonable person of ordinary sensibilities” and thus the objective nature of this term has been further

⁴⁸ UK: Draft Online Safety Bill poses serious risk to free expression, Article 19, 26 July 2021, <https://www.article19.org/resources/uk-draft-online-safety-bill-poses-serious-risk-to-free-expression/>

⁴⁹ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

⁵⁰ On the trail of the Person of Ordinary Sensibilities, Cyberleagle, 28 June 2021, <https://www.cyberleagle.com/>

⁵¹ Smith G. On the trail of the Person of Ordinary Sensibilities, Cyberleagle, 28 June 2021 <https://www.cyberleagle.com/2021/06/on-trail-of-person-of-ordinary.html>

eroded.⁵²

102. Furthermore, where content “may reasonably be assumed to particularly affect people with a certain characteristic” or of a “certain group”, the platform must apply that characteristic or group to the “adult of ordinary sensibilities” (cl. 46(4)). These “characteristics” or “groups” can be any at all and are not restricted to protected characteristics, leaving an absurdly broad and subjective framework for “harm” that is skewed towards censorship and open to abuse.

103. The legislation goes even further in clause 46 (7), where it defines content which could have an “indirect” impact and could risk an adult acting in a way which may cause “harm” to another person.⁵³ Obligations on platforms to tackle “harmful content” of this kind are deeply problematic and would pave the way for sweeping online censorship. These measures play on the idea that adults do not have individual agency and exposure to others’ speech, even where lawful and not incitement, could cause others to perpetuate “harm”. This could make online spaces sanitised spaces where it would be impossible to document violence or other societal ills.

References to “indirect harm” should be removed from the Bill.

PART 3 – OTHER DUTIES OF SERVICE PROVIDERS

104. Part 3 sets out obligations on platforms in regard to publishing transparency reports and provisions relating to fees for regulated services.

105. As with other elements of the Bill, provisions within this part give the Secretary of State an undue degree of influence over the regulatory framework.

PART 4 – OFCOM'S POWERS AND DUTIES IN RELATION TO REGULATED SERVICES

Chapter 1 – General Duties

Clause 57 - Duties of OFCOM in relation to strategic priorities

106. Clause 57 states that Ofcom must have regard for, and thus act on, a statement from the Secretary of State setting out their “strategic priorities” in relation to the

⁵²Smith G. On the trail of the Person of Ordinary Sensibilities, Cyberleagle, 28 June 2021
<https://www.cyberleagle.com/2021/06/on-trail-of-person-of-ordinary.html>

⁵³Draft Online Safety Bill, 2021,
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

regulatory regime. Once again, this demonstrates an undue level of executive influence over the legislation and subsequent processes.

Chapter 4 – Use of technology in relation to terrorism content and child exploitation and abuse content

Clauses 63-69 – “Technology notices”

107. Provisions set out later in the Bill put private messaging services within scope and oblige platforms to uphold duties of care in these channels. This is a dangerous direction and will result in growing surveillance online, even in spaces intended for users to hold a private conversation. The legislation states that:

*137 (1) “content” means anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description;*⁵⁴

108. “Safety duties about illegal content” and other obligations to deal with content which is harmful to adults, will therefore extend to private messaging services.

109. There are important technical issues to consider when imposing the “duty of care” on companies’ private messaging channels. Some companies offer structural privacy to their services – for example, the end-to-end encryption offered by instant messaging/VoIP apps WhatsApp and Signal. It is concerning that the Government’s intentions appear to deliberately make privately designed channels of this kind incompatible with platforms’ obligations set out in the Bill.

110. Clauses 63-69 give Ofcom the power to mandate the use of technology to identify and remove certain types of illegal content. Clause 64 states:

64 (4) A use of technology notice under this section is a notice relating to a regulated user-to-user service requiring the provider of the service to do either or both of the following—

(a) use accredited technology to identify public terrorism content present on the service and to swiftly take down that content (either by means of the technology alone or by means of the technology together with the use of human moderators to review terrorism content identified by the technology);

⁵⁴ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

*(b) use accredited technology to identify CSEA content present on any part of the service (public or private), and to swiftly take down that content (either by means of the technology alone or by means of the technology together with the use of human moderators to review CSEA content identified by the technology).*⁵⁵

111. Regulated services can appeal such a notice under provisions set out in clause 105.

112. It is vital that terrorism and CSEA content are removed from the internet. However, the risk of such content being stored or shared does not justify breaking encrypted channels, sacrificing the security, safety and privacy of millions of users. Given that private messaging services are within the scope of the legislation, the provision above does imply that certain types of technology could be used to break, erode or undermine the privacy and security provided to messaging services by end-to-end encryption. This could involve the use of a technique known as client-side scanning, which would create vulnerabilities within messaging services for criminals to exploit or could open the door to a greater level of surveillance through use of this technology.⁵⁶

113. It is not unreasonable to think that such technology would be escalated in time, put to use in other areas and result in increased surveillance of individuals' private messages.

114. As with other areas of the Bill, one of the real risks when it comes to legitimising new surveillance technology is that it will be emulated and indeed, will embolden, authoritarian regimes around the world to undertake similar practices but for even more undemocratic means.

115. Private communications are fundamental for our safety and privacy – and are critical for protecting journalists, human rights activists and whistleblowers all around the world. If the Government use this Bill to attack private communications, this will impact upon safety online for all and will set an example for more authoritarian regimes to follow.

In order to protect the right to privacy, clauses 63-69 should be removed from the Bill. Further, the scope of the Bill (clause 137) should be refined and private messaging services should be excluded from the Bill entirely.

⁵⁵ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

⁵⁶ Fact Sheet: Client-Side Scanning, The Internet Society, March 2021, <https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/>

Chapter 5 – Information

Clause 73 - Senior managers' liability: information offences

116. As part of wider “information notice” provisions, clauses 71-73 require regulated services to name a designated “senior manager” upon request. Such an individual is then bound by reporting obligations to the regulator and takes on a degree of personal liability for the conduct of the organisation in dispatching its relevant duties.

117. Clause 73 states that senior managers would commit an offence if they fail to comply with an information notice, provide false information in complying or if the information provided is encrypted. The maximum penalty is a 2-year custodial sentence.

118. While clauses 72 and 73 are deferred, these are deeply concerning provisions. At a risk of serious punishment from individual criminal liability, platforms will endeavour to unscrupulously remove content on their sites. Coupled with broad definitions and a low threshold of acceptable expression, these measures would guarantee widespread censorship online.

119. Article 19 raised concerns regarding this provision:

“the Draft Bill creates criminal liability for senior managers who fail to comply with demands for information from Ofcom (clause 73). Again, we are concerned that this would encourage managers to be overzealous in their compliance with their duties, especially the quick removal of content.”⁵⁷

120. Once again, these measures create a devastating example and will embolden authoritarian actors around the world to impose criminal liability on companies' senior management. These powers could be read to justify the imprisonment of social media executives overseas.

121. In setting out these provisions, clauses 72 and 73 also feature a disturbing inclusion. They state that following the issue of an information notice, a senior manager may commit an offence if:

72 (5)... in response to an information notice, the person—

⁵⁷ UK: Draft Online Safety Bill poses serious risk to free expression, Article 19, 26 July 2021, <https://www.article19.org/resources/uk-draft-online-safety-bill-poses-serious-risk-to-free-expression/>

(a) *provides or publishes information or produces a document which is encrypted such that it is not possible for OFCOM to understand it*⁵⁸

122. This is a deeply problematic sub-clause and will have the effect of dissuading online intermediaries from encrypting services (particularly messaging services), which keep users' conversations private and secure. As previously discussed, this is deeply damaging to journalists, human rights defenders and whistleblowers, who require structural privacy to undertake their work. This move would likely be welcomed by malign actors around the world.

Clause 77 - Powers of entry and inspection

123. As part of their powers of inspection, clause 77 gives Ofcom powers of entry.

124. This may be with a warrant, as set out in Schedule 5, where:

*3 (1) (b) (i) the provider is failing to comply, or has failed to comply, with an enforceable requirement in respect of that service,*⁵⁹

125. Or without a warrant where access has been denied, notice given and other sufficient criteria met.

126. We believe that this is overbearing and heavy handed as a provision. Threatening companies with prospective actions of this nature, for non-compliance with the regulatory regime, will add to an environment which encourages censorship and overzealous content removal.

Chapter 6 - Enforcement Powers

Clauses 85 and 86 – Amount of penalties

127. Clauses 85 and 86 mean that a failure on the part of a platform to fulfil their relevant duties of care could result in a fine of up to £18m or 10 per cent of annual global turnover, depending on which is higher.

128. It is unprecedented for the Government to seek to punish technology companies for essentially failing to act as effective law enforcement auxiliaries and even for failing to censor or demote lawful content. Given the financial and reputational costs that could be incurred if these proposals go ahead, there will be a chilling effect that will motivate companies to monitor, demote and censor expression overzealously.

⁵⁸ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

⁵⁹ Ibid.

Clause 90 - Penalty notice for failure to comply with use of technology notice

129. Clause 90 establishes that Ofcom may impose financial penalties upon intermediaries for failing to comply with a technology notice. Once again, we are deeply concerned about this provision, not least as it will likely result in the regulator forcing tech companies to use surveillance technology that could undermine the privacy afforded by encrypted channels. Not only is this a violation of the right to privacy but it would also have wider ramifications for human rights in general.

Clauses 91-95 – Service restriction orders & Access restriction orders

130. In terms of penalties, the Bill also goes much further and clauses 91-94 give Ofcom license to seek service restriction orders (e.g. forced removal from the app store) or Access Restriction Orders (ISP blocking), either of which must be approved in court. The proposal for search engine, intermediary and ISP blocking is severe and is a fundamental threat to free expression.

131. Clause 91 gives Ofcom the power to apply to a court for a service restriction order. Such a measure may be sought if a service fails to comply with a technology notice, fails to pay a fine, there is a substantial “risk of harm” on the service or other failures with regard to obligations placed on services in the course of the legislation.

132. Such measures would target ancillary services which support the platform in question and could include hosting providers or ad servers. Clause 92 allows Ofcom to apply for such an order on an interim basis.

133. Clause 93 gives Ofcom the power to seek, from a court, permission to impose an access restriction order, where a service restriction order “was not sufficient to prevent significant harm arising to individuals in the United Kingdom” or if a service restriction order was deemed insufficient to prevent “harm”.

134. This involves the full blocking of a service so that it may not be accessed by users in the UK. Clause 94 gives Ofcom the power to seek such a measure on an interim basis.

135. These are extremely serious sanctions with wide-ranging effects, including on third parties such as search engines and ISPs, and the public more widely. The idea of the British Government appointing a regulator to enforce Chinese-style ISP blocks and search-engine controls over information is extraordinary. Such severe sanctions are

chilling and reflect the extreme nature of this proposed legislation, which is at odds with liberal democratic values.

136. As with other aspects of the Bill, there remains a risk that measures included in the legislation could be opened up to politicisation. As Open Rights Group (ORG) has pointed out, this is particularly the case for interim service restriction orders and access restriction orders, where the Secretary of State could pressure Ofcom to apply these totalitarian sanctions on a service of their own choosing. In a blog post on this topic, ORG wrote:

“it is not a stretch to imagine the temporary orders being used to block public access to popular services, such as social media sites, if public opinion turns too rapidly against the government tide.”⁶⁰

137. Concerns about service restriction orders and access restriction orders were also raised by Article 19 in its response to the Bill. Addressing what the group described as “disproportionate sanctions”, it stated:

“Website (or service) blocking is almost always disproportionate under international human rights law because in most cases, websites would contain legitimate content. In practice, blocking is a sanction that would penalise users who would no longer be able to access the services that they like because a provider hasn’t removed enough content to the liking of Ofcom or the Minister. It is also the kind of measures that have been adopted in places such as Turkey. It is therefore regrettable that the UK is signalling that these types of draconian measures are acceptable.”⁶¹

138. The wide range of punishments set out in this section, are excessively severe and are designed to pressure intermediaries to implement their operational safety duties in an overbearing manner. In the event that the measures set out in clauses 91-95 should ever be drawn upon, they would be a direct violation of the right to freedom of expression. Blocking access to a major intermediary in the UK would prevent many citizens from freely expressing themselves and would inhibit the free flow of information in this country. Such measures are more commonly associated with authoritarian regimes and have no place in a liberal democracy.

Clauses 91-95 should be removed from the Bill.

⁶⁰ Burns, H. ACCESS DENIED: SERVICE BLOCKING IN THE ONLINE SAFETY BILL, Open Rights Group, 6 July 2021, <https://www.openrightsgroup.org/blog/access-denied-service-blocking-in-the-online-safety-bill/>

⁶¹ UK: Draft Online Safety Bill poses serious risk to free expression, Article 19, 26 July 2021, <https://www.article19.org/resources/uk-draft-online-safety-bill-poses-serious-risk-to-free-expression/>

Chapter 7 – Committees, Research and Reports

Clause 98 - Advisory committee on disinformation and misinformation

- 139.** Clause 98 states that Ofcom must establish a committee to advise the regulatory regime on disinformation and misinformation.
- 140.** Upon the publication of the Bill, the Government’s press release specifically stated that the legislation would mean Category 1 Services would “need to act on content that is lawful but still harmful such as mis/disinformation.”⁶²
- 141.** While their designation as “priority content which is harmful to adults” is not yet confirmed, this statement of political will to do so is very concerning. Terms such as “disinformation” can be subjective and easily politicised.
- 142.** The malleable nature of the concepts of “disinformation” and “misinformation” mean that the threshold for censorship in this area is low. Social media platforms have shown their willingness to make interventions on content that is perceived to be misleading by fact-checking organisations and others. The inclusion of “disinformation” as a specified category of content within the online safety framework could result in social media companies more frequently arbitrating the speech of academics, pundits and users in general. While disinformation generally constitutes information that is deliberately misleading, it should be reiterated that the legislation is also set to cover misinformation, which is content that is unintentionally misleading or merely inaccurate. This could result in members of the public having any content removed simply because it is considered to be “wrong”.
- 143.** It should generally not be the place of a private company to assess and then instruct their users as to the “reliability” of the information and news sources they access. This is a highly subjective task best fulfilled by internet users themselves, who can optionally conduct wider research or access fact-checking websites online. This is much easier online than it is in a library and offline public spaces. The critical faculties of members of the public are not the responsibility of tech companies. Nor are tech companies best placed to judge the “reliability” of information.

Clause 101 - OFCOM’s report about researchers’ access to information

⁶² Landmark laws to keep children safe, stop racial hate and protect democracy online published, UK Government, 14 May 2021, <https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published>

144. The Online Safety Bill approaches problems identified online from the end point of content moderation, rather than looking at companies’ business models and the design of algorithms. Clause 101 is a rare provision within the legislation that seeks to create a greater degree of transparency in the operations of online intermediaries and tackles many of the problems identified from the right angle. It states:

101 (1) OFCOM must prepare a report—

(a) describing how, and to what extent, persons carrying out independent research into online safety matters are currently able to obtain information from providers of regulated services to inform their research,

(b) exploring the legal and other issues which currently constrain the sharing of information for such purposes, and

(c) assessing the extent to which greater access to information for such purposes might be achieved.⁶³

145. Social media companies’ algorithms often promote sensationalism and controversy in an attempt to capture users’ attention and keep them active on their sites. Attempts to audit these systems should be promoted.

PART 5 – APPEALS AND SUPER-COMPLAINTS

Chapter 2 – Super Complaints

Clause 106 – Power to make super-complaints

Clause 106 creates a “super-complaints” system within the regulatory framework. It states:

106 (1) An eligible entity may make a complaint to OFCOM that any feature of one or more regulated services, or any conduct of one or more providers of such services, or any combination of such features and such conduct is, appears to be, or presents a material risk of—

(a) causing significant harm to users of the services or members of the public, or a particular group of such users or members of the public;

⁶³ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

(b) significantly adversely affecting the rights to freedom of expression within the law of users of the services or members of the public, or of a particular group of such users or members of the public;

(c) causing significant unwarranted infringements of privacy, in relation to users of the services or members of the public, or a particular group of such users or members of the public; or

(d) otherwise having a significant adverse impact on users of the services or members of the public, or on a particular group of such users or members of the public.⁶⁴

146. As with many of the provisions within the Bill, this is a well-intended inclusion that has a number of fundamental flaws. The fact that only “eligible entities”, who will meet criteria set out by the Secretary of State, may make super complaints is a major limitation. With a degree of executive discretion, the Secretary of State could refine such a group of potential complainants to those of their own choosing. Moreover, that this function is not open to all members of the public means that certain groups and individuals will have a greater degree of influence over the permissibility of speech than others.

PART 6 - SECRETARY OF STATE'S FUNCTIONS IN RELATION TO REGULATED SERVICES

Clause 109 and 110 – Statement of strategic priorities

147. Clauses 109 and 110 allow the Secretary of State the power to issue a statement of strategic priorities. Ofcom must have regard to this statement and demonstrate its accordance with it.

148. Once again, this measure gives the executive undue influence over the regulatory regime and could allow for the politicisation of its processes in the future.

149. The Secretary of State’s statement is laid before Parliament and can be rejected via a negative procedure. This gives parliamentarians virtually no adequate scrutiny over this executive decree.

Clause 112 - Secretary of State directions in special circumstances

⁶⁴ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

150. Clause 112 gives the Secretary of State the power to give direction to Ofcom if circumstances:

present a threat—

(a) to the health or safety of the public, or

(b) to national security.⁶⁵

151. This can involve compelling a regulated service or all services to set out how they are dealing with the circumstances in question.

152. Emergency situations are often dangerous when it comes to the protection of civil liberties and this measure gives the Government a lever to influence the regulatory regime in such times with limited oversight from the legislature.

Clause 113 - Secretary of State guidance

153. Clause 113 also gives the Secretary of State the power to give guidance to Ofcom about its functions under the legislation. This may not be done more frequently than every three years unless the legislation is amended or the guidance is agreed by both the Secretary of State and Ofcom.

154. The legislation states that this guidance must be laid before Parliament. However, once again, this is an opportunity for the Government to issue this framework in a way that could impact upon fundamental rights, without full parliamentary scrutiny.

PART 7 - GENERAL AND FINAL PROVISIONS

Clause 127 - Extra-territorial application

155. Clause 127 describes the extra-territorial application of the legislation and its application to services which are available in the UK but located out of the country.

156. This could directly inhibit the free flow of information to the UK, which is inherent to the right to free expression. Such a free flow of information could be threatened if a service deems the regulatory framework too complicated or risky to operate to users in the UK or, if the legislation directly conflicts with domestic legislation from the jurisdiction within which it is based.

⁶⁵ Draft Online Safety Bill, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

157. As previously referenced, the Polish Government have proposed a “social media free speech” law. The proposed law would prevent online intermediaries from removing content or banning users who do not break Polish laws⁶⁶. In the event that this legislation and the Online Safety Bill were passed, the ability of social media users in Poland and the UK to communicate directly would be severely hampered by contradictory laws. In such a case, should a user in Poland issue a post on a large social media platform which could be viewed by users in the UK and the material were deemed “harmful” under the online safety framework but was not illegal in Poland, the intermediary in question would be posed with a complex legal dilemma. This could move us towards national digital silos and directly threaten the transnational interconnectedness of internet as a whole.

RECOMMENDATIONS

158. The Online Safety Bill poses a greater threat to freedom of speech in the UK than any other law in living memory. In this submission, we have set out our key concerns regarding the impact that this legislation would have on fundamental rights in the UK, whilst also attempting to answer the Committee’s questions.

159. It is vital that policymakers consider the impact on the right to free speech and privacy in the course of their scrutiny of this legislation. Whilst we believe that the Bill is fundamentally flawed in its approach, the legislation suffers particularly from broad definitions, overbearing provisions and measures which grant the executive excessive power over the process.

160. There are a number of measures that policymakers could take to limit the detrimental impact of this legislation on free speech and privacy. Key amendments that are crucial for the protection of free speech and privacy are set out below.

- **The legislation should not force platforms to take down or suppress speech that is lawful.** In its current form the Online Safety Bill would create a two-tier system for freedom of expression, with extra restrictions for online speech which is considered subjectively harmful. Any further restrictions on our right to free speech must be in line with UK law and decided on in a democratic, parliamentary process.

If we are to avert the Online Safety Bill doing permanent damage to the right to free speech in the UK, as a minimum, clause 11 (relating to “legal but harmful” content) should be removed from the Bill.

⁶⁶ Poland proposes social media 'free speech' law, BBC News, 15 January 2021, <https://www.bbc.co.uk/news/technology-55678502>

- **References to “indirect harm” should be removed.** In setting out definitions of harm, the Bill makes reference to “indirect harm” on a number of occasions. This is an incredibly vague concept which would lead to widespread censorship online. Such a notion erodes individual responsibility and could have a major detrimental impact on free speech.

References to “indirect harm” should be removed from the Bill.

- **Private conversations should not fall within the scope of the Bill.** The legislation extends duties of care to private messaging services and threatens end-to-end encryption. Private communications are vital for our safety and privacy – and are critical to protect journalists, human rights activists and whistleblowers all around the world. Moves to erode privacy online undermine the fundamental right to privacy and would make us all less safe.

In order to protect the right to privacy, clauses 63-69 (technology notices) should be removed from the Bill. Further, the scope of the legislation (clause 137) should be refined and private messaging services should be excluded from the Bill entirely.

- **The Bill should not force online platforms to introduce mandatory age verification.** At present, the legislation requires companies which are “likely to be accessed by children”, to moderate content accordingly unless they can prove otherwise. This will push platforms towards mandatory age verification which is invasive, would cause digital exclusion and sets a poor example for less democratic regimes around the world to follow.
- **The Bill should not give authorities the power to block or prevent UK citizens from accessing online intermediaries.** These measures are incompatible with liberal democratic ideals, could cause wholesale damage to both free expression and the free flow of information, and would be cited and emulated by malign actors all around the world.

Clauses 91-95 should be removed from the Bill.