
# Online Safety Bill

# House of Lords

# Second Reading Briefing

# January 2023

**For further information contact**

Stephanie Needleman, Legal Director

email: sneedleman@justice.org.uk

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

## Introduction

1. JUSTICE is an all-party law reform and human rights organisation working to strengthen the justice system. It is the UK section of the International Commission of Jurists. Our vision is of fair accessible, and efficient legal processes in which the individual's rights are protected and which reflect the country's international reputation for upholding and promoting the rule of law.

2. This briefing addresses the Online Safety Bill (the "**Bill**") in advance of its 2nd Reading in the House of Lords. JUSTICE recognises the growing concern about online harms, and the need to protect service users, especially children, from harmful and illegal content online.[1] With this in mind, JUSTICE is broadly supportive of the stronger regulation of online service providers, particularly with respect to child sexual exploitation and abuse ("**CSEA**") content. As highlighted in our report, *Prosecuting Sexual Offences* (2019), JUSTICE considers the introduction of appropriate regulation of internet services as an important step in preventing CSEA.[2] We welcome the fact that a number of the report's recommendations are reflected in the Bill. These include:

    a) **Placing a duty on online service providers to act with regard to CSEA content online.[3]** As identified in our report we consider that placing a duty on services to moderate and remove such content is crucial to preventing its proliferation online.[4]

    b) **Promoting greater accountability by requiring service providers to produce transparency reports.** Under the Bill, OFCOM would have a duty to require certain platforms to provide information, including on the incidence of illegal content, the number of users assumed to have encountered that content, and the systems in place to deal with that content.[5]

---

[1] The Internet Watch Foundation, for instance, has noted a year-on-year increase in reports of webpages that were found to contain child sexual abuse imagery between 2017 and 2021. See The Independent Inquiry into Child Sexual Abuse, *The Report of the Independent Inquiry into Child Sexual Abuse* (2022).

[2] JUSTICE, *Prosecuting Sexual Offences* (2019), paras 1.23, 2.28-2.36.

[3] Clause 9 and 23, and 53.

[4] supra n. 2, para 2.33.

[5] Clause 68 and 69 and Schedule 8.

3. Nevertheless, JUSTICE considers that the Bill could go further in tackling the proliferation of CSEA online. We recommend that the Bill:

    a) **Make explicit that once provided to OFCOM transparency reports are to be made publicly available, subject to appropriate redactions.** Making such reports publicly available is crucial for empowering service users and parents to make more informed choices online.

    b) **Impose minimum transparency reporting requirements in relation CSEA content.** The government should extend these requirements to all companies with a footprint in the UK. This would bring the Bill further in line with the approach to reporting CSEA content recommended in our report *Prosecuting Sexual Offences*.[6]

    c) **Enhance OFCOM's duties with regard to improving media literacy.** The Bill should place a responsibility on OFCOM to run national awareness campaigns promoting the importance of safety online. The Bill should also require OFCOM to conduct research into services that help people at risk of offending tackle inappropriate sexual thoughts, and to run national advertising campaigns to raising awareness of such services.[7]

4. At the same time, JUSTICE recognises several areas of deep concern with the Bill with respect to its implications for freedom of expression, as guaranteed by Article 10 of the European Convention on Human Rights ("**ECHR**"). In particular, JUSTICE is concerned that:

    a) **The Bill does not go far enough in protecting users from over moderation by online service providers.** To overcome this, we recommend:
        i) The removal of content that amounts to an offence under section 5 of the Public Order 1986 ("**POA**") from category of priority illegal content to be regulated by the Bill. Section 5 of the POA covers "*threatening or abusive*

[6] JUSTICE, *Prosecuting Sexual Offences* (2019), para 2.33.

[7] *ibid,* paras 2.46-2.47

*words or behaviour, or disorderly behaviour*" that is likely to cause "*harassment, alarm or distress*."

ii) That the duties about freedom of expression and complaints procedures within the Bill are strengthened.

b) **The Bill would give too much power to the Secretary of State in relation to OFCOM's policies and the setting of priority content to be regulated by the Bill.** This could threaten OFCOM's status as an independent regulator and afford the executive unprecedented power to police the boundaries of what constitutes legitimate speech.

## The Duty of Care Model

5. Part 3 of the Bill sets out the duties of care which regulated user-to-user services and regulated search services[8] would have towards their users. This includes duties to conduct risk assessments and duties to protect users against "*illegal content,*"[9] and "*content that is harmful to children*."[10]

6. The Bill imposes different duties on companies in relation to illegal and harmful content depending on the activity on their services. Under the proposed framework:

a) All in-scope services would be required to undertake an illegal content risk assessment[11] and address illegal content on their services.[12]

b) Services that are likely to be accessed by children would be required to undertake a children's risk assessment[13] and address content that is harmful to children.[14]

---

[8] "User-to-user service" and "search service" are defined in Part 2 of the Bill. Schedule 1 of the Bill sets out a limited number of services excluded from the regulatory framework. For instance, email, SMS and MMS services where these services are "*the only user-generated content enabled by that service,*" are expressly excluded. It is worth noting that messenger services on social media platforms such as Instagram, Facebook, WhatsApp, Telegram, and Twitter would not qualify and would be subject to regulation under the Bill.

[9] Clause 53.

[10] Clause 54.

[11] Clause 8 and 23.

[12] Clause 9 and 23.

[13] Clause 10 and 24.

[14] Clause 11 and 25.

c) Companies providing Category 1 services (to be defined in secondary legislation, and expected to cover the largest online platforms, such as Facebook and Twitter[15]) would also have additional duties to provide adults with greater choice over the content they see and engage with. This would include providing users with the choice to filter out content that encourages suicide or self-harm or eating disorders, as well as abusive content that targets or incites hatred against people with protected characteristics.[16]

7. While the Bill's measures would represent a change in the current online regulatory landscape, as highlighted by the House of Lords Select Committee on Communications, the internet is not currently the unregulated 'Wild West' it is sometimes painted to be. [17] Civil and criminal law already apply to activities online as well as offline.[18] Moreover, there are a number of independent regulatory bodies with the power to enforce rules for conducting certain activity relevant to the online sphere.[19] Finally, as of 1 November 2020, OFCOM has been able to take action against UK-established video-sharing platforms ("**VSPs**"), such as TikTok and Snapchat, that do not adopt measures to protect users from harmful content.[20]

8. Nonetheless, despite existing law providing a level of regulation of the online sphere, there are some key differences between the current law and the new proposals contained in the Bill:

[15] Schedule 11. See also HM Government, 'Online Harms White Paper: Full Government response to the consultation', 2020, para. 2.34; Department for Digital, Culture, Media and Sport,'Online Safety Bill: factsheet', January 2023.

[16] Clause 12.

[17] House of Lords Select Committee on Communications, *Regulating in a digital world* (2019), p.9.

[18] For instance, the offence prohibiting sexual communication with a child applies equally in both contexts see Ministry of Justice, 'Sexual Communication with a Child: Implementation of Section 67 of the Serious Crime Act 2015', 2017.

[19] For example, the Advertising Standards Agency, the Information Commissioner's Officer, and indeed OFCOM, which currently has responsibility for regulating 'TV-like' content and telecommunications companies in line with its principles for broadcast media. For a full of existing regulator list see House of Lords Select Committee on Communications, *Regulating in a digital world* (2019), Appendix 4.

[20] Part 4B, Communications Act 2003; Ofcom, 'Regulating video-sharing platforms: what you need to know', 2021. For a list of registered VSPs *see* OFCOM, 'Notified video-sharing platforms', 2022.

a) As opposed to relying on criminal and civil law once an offence has occurred, the Bill would place the onus on companies to proactively prevent the proliferation of illegal content online.[21]

b) While there are various regulators with responsibility for certain online activities,[22] there is currently no unified regulatory framework over seen by a single regulator.[23] By imposing a duty of care on online services, enforced by OFCOM, the Bill would establish this kind of unitary regime.

c) While OFCOM has the power to enforce rules on harmful content with regard to VSPs, this power is limited to the extent that it applies only to UK-based services whose "*principal purpose"* or "*essential functionality*" is to provide videos to the public.[24] This means that OFCOM's powers do not apply to user-generated content services such as Facebook, Instagram or Twitter.[25] By contrast, the Bill's duty of care would apply to a far wider range of services, including those which are not based in the UK, as well as a wider range of content beyond VSPs. Indeed, OFCOM's power to regulate VSPs was introduced as an interim measure until the Bill comes into force.[26]

9. In short, the imposition of a duty of care on online services would signal a significant departure from existing regulation of online content, insofar as it would allow for a more preventative approach to regulating illegal content online and would form part of a unified regulatory framework applying to a wider range of online services. JUSTICE welcomes certain aspects of the duty of care model, especially with respect to preventing the proliferation of CSEA online. However, as outlined in detail below, JUSTICE remains concerned about certain aspects of the illegal content duties.

---

[21] The benefit and necessity of this regarding CSEA was highlighted in JUSTICE's report *Prosecuting Sexual Offences*, see pp. 9, 10, 20-25.

[22] E.g., the Financial Conduct Authority, the Advertising Standards Agency and the Internet Watchdog Foundation. For a full list of existing regulators which have remits for online regulation see House of Lords Select Committee on Communications, *Regulating in a digital world* (2019), Appendix 4.

[23] *Ibid* p.3.

[24] OFCOM, 'Video sharing platforms: who needs to notify Ofcom?', 2021.

[25] For a list of registered VSPs *see* OFCOM, 'Notified video-sharing platforms', 2021.

[26] HM Government, 'Online Harms White Paper: Full Government response to the consultation', 2020 p.55.

Duties regarding illegal content

10. Clauses 8 and 22 would place a duty on all regulated user-to-user services and all regulated search services to undertake an "*illegal content risk assessment*." This assessment should identify, the level of risk of service users encountering:

    a) Priority illegal content: and

    b) Other illegal content.

11. Priority illegal content means "*terrorism content*,"[27] "*CSEA content*"[28] and "*content that amounts to an offence specified in Schedule 7*."[29] Other illegal content refers to content that amounts to a relevant non-priority offence.[30] Clauses 8(5) and 22(5) provide that illegal content risk assessments should take into account a number of factors, including the user base of the service, the level of risk of harm to individuals presented by illegal content, the level of risk the nature and severity of the harm that might be suffered, and how the design and operation of the service may reduce or increase the identified risk.

12. Clauses 9 and 23 would place a duty on all in-scope services to "*effectively mitigate and manage the risks of harm to individuals*" presented by illegal content. Under the Bill, in-scope companies would be required to take measures to prevent users from encountering "*priority illegal content*," and minimise the length of time for which "*priority illegal content*" is present. Regulated user-to-user services would also be required to put in place processes to facilitate the swift removal of illegal content once it became aware of it. The Bill would also impose a duty on companies to specify in clear accessible language in their terms of service how users are to be protected from illegal content, and to apply these provisions consistently.

13. JUSTICE supports placing a duty of care on companies to regulate CSEA content on their services. In our report *Prosecuting Sexual Offences* we highlight the crucial role of

[27] Per clause 53 (8) "terrorism content" means content that amounts to an offence specified in Schedule 5.

[28] Per clause 53 (9) "CSEA content" means content that amounts to an offence specific in Schedule 6.

[29] Clause 53 (10).

[30] Per clause 53(5) an offence is a relevant non-priority offence if the victim or intended victim of the offence is an individual (or individuals).

regulating online platforms in preventing sexual offending in the online sphere.[31] The internet has facilitated a surge in sexual offences and the sheer volume of CSEA content online has placed a significant burden on the criminal justice system;[32] it is clear that "*we cannot arrest our way out of the problem*".[33] Placing an onus on internet companies to prevent certain types of offending from entering the online sphere is essential to addressing the volume of online sexual offences.

14. Moreover, we particularly welcome the requirement that companies make public, in their terms of service, the steps they are taking to ensure individuals are protected from illegal content. This would increase transparency and accountability and would hopefully encourage online platforms to develop robust processes for reducing CSEA content on their services.

15. We are also pleased to see that, in the case of CSEA, the Bill would also support the police in tackling this kind of offending. Clause 59 places a duty on service providers to use systems and processes which "*secure (so far as possible) that the provider reports all detected and unreported UK-linked CSEA content present*" on their services to the National Crime Agency. Requiring providers to have these systems in place ensures that evidence of serious crimes can be handed to the relevant authorities to be investigated and tackled offline.

16. We note that similar reporting requirements do not apply to any of the other illegal content to be regulated by the Bill. Whilst we recognise the practical and resource challenges that reporting all content identified as illegal to law enforcement would pose, we find it surprising that the Bill is silent on what service providers are to do with this content once it is removed from their services. Some of this content is likely to provide evidence of serious, repeated criminality and therefore should be preserved for use in criminal investigation. The Bill should provide more guidance to online service providers regarding

[31] JUSTICE, *Prosecuting Sexual Offences* (2019), paras 2.28-2.36.

[32] For example, the NSPCC has found that there was a record-high 70% increase in offences related to Sexual Communication with a Child recorded during the first year of the pandemic. NSPCC, 'Briefing on the draft Online Safety Bill', 2021, p.1. See also Independent Inquiry into Child Sexual Abuse, *The Report of the Independent Inquiry into Child Sexual Abuse* (October, 2022).

[33] JUSTICE, *Prosecuting Sexual Offences* (2019), para. 2.1; Chief Constable Simon Bailey, Lead for Child Protection, National Police Chiefs' Council, Home Affairs Select Committee, 'Oral Evidence: Policing for the Future', 2018.

the handling of the illegal content they find on their services, to ensure potentially vital evidence is not destroyed.

17. Whilst JUSTICE welcomes the increased regulation of certain types of illegal content online, we also recognise the need, identified in the Government's response to the White Paper, to protect freedom of expression by ensuring that companies avoid taking an "*overly risk-averse approach to the identification and removal of material likely to be illega*l."[34] It is JUSTICE's view that the Bill, in its current form, does not sufficiently safeguard against this risk of over-moderation by online companies.

*Concerns*

18. The Bill does not account for the difficulty that in-scope providers are likely to face in moderating certain content, and moreover doesn't account for the fact that certain forms of illegal content are inherently difficult to moderate. As stated by Richard Wingfield, Head of Legal, at Global Partners Digital, in his evidence before the Select Committee on Communications and Digital:

> "*Making decisions about what is illegal speech is incredibly difficult. It takes time to gather evidence and to talk to witnesses, and it is most likely there will be a trial at the end of it, yet we are asking content moderators to understand our legal system and make decisions in minutes about whether somebody's speech is illegal or not*."[35]

19. JUSTICE is particularly concerned about the inclusion of content that amounts to an offence under section 5 of the Public Order Act ("**POA"**) within the category of priority illegal content to be regulated by the Bill.[36] Section 5 of the POA covers "*threatening or abusive words or behaviour, or disorderly behaviour*" that is likely to cause "*harassment, alarm or distress*." As recognised by the Joint Committee on Human Rights, "*it is hard to*

[34] HM Government, 'Online Harms White Paper: Full Government response to the consultation', 2020, p.31.

[35] House of Lords Select Committee on Communications and Digital, 'Corrected oral evidence: Freedom of expression online', 2020.

[36] Schedule 7.

*see how providers, and particularly automated responses, will be able to determine whether content on their services fall on the legal or illegal side of this definition."*[37]

20. Given the fine line between what constitutes abusive as opposed to merely offensive material, as well as the difficulties involved in determining whether or not content is likely to cause someone sufficient "*alarm or distress*," it is our view that placing a duty on online service providers to prevent users encountering content amounting to a section 5 POA offence will result in the disproportionate removal of legitimate content that does not meet the threshold for the offence. This risk is exacerbated by the fact that when determining whether content is illegal content on not, providers need only have "*reasonable grounds to infer*" that the elements necessary for the commission of the offense in question are satisfied.[38]

21. Moreover, the Bill designates as priority illegal content the inchoate versions of section 5 POA offences.[39]This means that under the Bill content that encourages, for instance, disorderly behaviour likely to cause alarm would also have to be moderated and removed by online companies. It is not difficult to imagine the broad range of content that could meet that definition given that companies only need to have reasonable grounds to think the threshold for the offence is met. For instance, content that portrays protest activity in a positive light, or which shows protest activity which could be viewed as disorderly, without directly condemning that activity.

22. Whilst the Bill does state that in making judgments as to whether content is illegal content or not, providers would have to consider that there are reasonable grounds to think that the mental element[40] of the offence is met,[41] given the low bar set by "*reasonable grounds*," the difficulties in determining the state of mind of any particular poster,

---

[37] Letter from Harriet Harman MP, Chair of the Joint Committee on Human Rights to the Secretary of State for Digital, Culture, Media and Sport, 19 May 2022.

[38] Clause 170.

[39] Schedule 7. Inchoate offences occur where an individual does not commit the substantive offence but instead commits an offence by encouraging, inciting, assisting, or attempting the commission of the substantive offence.

[40] The mental element of an offence is the state of mind an individual must have when carrying out the conduct prohibited by the offence. For instance, in the case of inchoate section 5 POA offences the individual encouraging the commission of the substantive section 5 offence must also intend or believe that the substantive offence would be committed.

[41] Clause 170(6).

particularly where automated technology is being used,[42] and the consequences that attach to failing to fulfil an illegal content duty,[43] online providers will have a strong incentive to infer this once the other elements of the offence are reasonably satisfied.

23. The inclusion of section 5 POA offences in the category of priority illegal content therefore has potentially significant implications for the Article 10 ECHR rights of users. The European Court of Human Rights ("**ECtHR**") has repeatedly warned against the collateral effect of measures designed to prevent the dissemination of illegal content online and has consistently reiterated that to be ECHR compliant domestic law must strictly target the illegal content in question.[44] Provisions which encourage an overly risk-averse approach to content removal, resulting in legitimate content being removed, may therefore fall short of the UK's obligations under the ECHR. **JUSTICE therefore considers that section 5 of the Public Order Act should be removed from the category of priority illegal content, set out in Schedule 7 of the Bill**.

24. JUSTICE also considers that in order to protect users from overcautious content moderation by service providers, the Government should do more to strengthen the safeguards designed to protect freedom of expression within the Bill. The most obvious of these safeguards are the duties about freedom of expression contained in Clause 18 and 28 of the Bill, which would require all services to "*have particular regard to the importance of protecting users' right to freedom of expression within the law*" when deciding on and implementing their safety measures and policies.

25. It is JUSTICE's view that the requirement to "*have regard to the importance of*" protecting freedom of expression, rather to simply protect it, significantly dilutes this duty. Moreover, JUSTICE recognises the concern highlighted by the Joint Committee on Human Rights, that the obligation to have regard to "*freedom of expression within the law*" lacks clarity

[42] See i.e. Microsoft, 'Online Safety Bill – Parliamentary Briefing from Microsoft' 2022; Independent Reviewer of Terrorism Legislation, 'Missing Pieces: A Note on Terrorism Legislation in the Online Safety Bill' 2022.

[43] Under the Bill OFCOM would be able to issue those who fail to comply with a duty of care with a fine of up to £18 million or 10% of annual global turnover, whichever is higher. In cases of continued non-compliance OFCOM would be able to take measures to disrupt a company's business activities in the UK, including blocking access to services. See Chapter 6 (Enforcement Powers).

[44] See e.g., *Engels v Russia* (2020) App. No. 61919/16; *OOO Flavus and Others v Russia* (2020) App. Nos. 12468/15,23489/15 and 19074/16.; *Vladimir Kharitonov v Russia* (2020) App. No. 10795/14; *Cengiz and others v Turkey* (2016) App. Nos. 48226/10 and 14027/11.

given the number of interrelated legal duties that affect freedom of expression.[45] As John Howell MP, noted during October's debate on online harms, the ECHR is a "*key pillar*" for protecting the right to freedom of expression online.[46] With this in mind, **we recommend that the duties about freedom of expression in the Bill be amended to specify that when deciding on, and implementing, safety measures and policies, in-scope services must uphold the right to freedom of expression as protected by Article 10 ECHR.**

26. Under Article 10 ECHR any interferences with freedom of expression must be necessary and proportionate to achieving a legitimate aim.[47] Making explicit reference to Article 10 of the ECHR would impress on service providers the need to ensure that the measures they impose in complying with their duties under the Bill are proportionate and necessary restrictions on the freedom of expression. This would go some way to guarding against overzealous moderation, as it would make clear that the measures imposed by service providers should be no more restrictive than is necessary to, for instance, protect users from a particular kind of illegal content.

27. Another safeguard which JUSTICE considers could be strengthened is the requirement concerning complaints procedures. Under the Bill companies would have a duty to operate complaints procedures to allow, amongst other things, complaints from users whose content is taken down on the basis that it is illegal content or who are suspended from the service as a result of content which the provider considers to be illegal content.[48] However, whilst this requirement is designed to offer users some protection from overzealous content moderation, by enabling users to challenge the removal of their content, the Bill leaves it entirely up to online companies how they chose to operate their complaints procedure and contains no provisions for the kinds of redress that might be available to those whose content is wrongly removed.

---

[45] Letter from Harriet Harman MP, Chair of the Joint Committee on Human Rights, to Nadine Dorries MP, Secretary of State for Digital, Culture, Media and Sport, 19 May 2022.

[46] HC Deb 26 October 2022, vol 721, col 168WH.

[47] Such aims include protecting national security, preventing disorder or crime, and protecting health or morals. See European Court of Human Rights 'Guide on Article 10 of the European Convention on Human Rights,' (2022).

[48] Clause 17 and 27.

28. To ensure that online service providers implement robust complaints processes, the face of **the Bill should contain requirements as to what basic features these processes should have.** At a minimum, this should specify that where content is taken down wrongfully, the company must have a process for reinstating that content (or user) within a particular time-frame.

29. Moreover, the Bill should make explicit that when determining whether content is illegal content in the context of an appeal or complaints process, a service provider should have to have more than "*reasonable grounds to infer*" that the elements of the offence are met. The Bill already suggests that judgements about the status of content are likely to differ based on whether the judgement is made by a human moderator or an automated system, given the information likely to be available in each of those cases.[49] It is consistent with this position that a higher standard should apply in the context of appeals where more time is given over to considering that content and more information is likely to be available. **The Bill should therefore specify that when determining whether content is illegal content for the purpose of an appeal or complaints process, the provider must be satisfied that its more likely than not that the elements of the offence are met.**

30. As well as requiring regulated service users to operate a complaints service, **the Bill should also introduce an independent appeals mechanism, which would allow individuals who have had their content repeatedly taken down to complain to an independent body tasked with considering such complaints.** The right to access this external redress process would be reserved for those who have exhausted the internal complaints process with the service provider against which they are making a complaint. It is our view that the possibility of being subject to an external appeals process, aimed at safeguarding freedom of expression, would discourage service providers from taking an overzealous approach to content moderation and would go some way in addressing the imbalance of power between online service providers and their users.

31. This appeals body should also provide scrutiny at a systematic level and should be empowered to review the effectiveness of the measures platforms are taking to preserve freedom of expression. This would include conducting analysis of the complaints it

[49] Clause 170.

receives, to identify industry wide risks and flaws in service providers complaints processes. Such analysis would be published in a report. This would both promoting greater transparency and encourage service providers to improve their appeals processes – ensuring that users are treated fairly and consistently in instance where their right to freedom of expression has potentially been repeatedly infringed.

## The Role of OFCOM

32. The Bill names OFCOM as the independent regulator of in-scope services, empowering it with a range of additional duties and functions. This would include issuing codes of practice setting out, amongst other things, how services should comply with their duties under the Bill,[50] establishing a transparency, trust and accountability framework[51] and requiring all in-scope companies to have effective and accessible mechanisms for users to report concerns.[52]

33. The Bill would also provide OFCOM with a number of enforcement powers. This would include the power to fine companies failing in a duty of care up to £18 million or 10% of annual global turnover, whichever is higher.[53] OFCOM would also be able, in cases of continued non-compliance, to take measures to disrupt a company's business activities in the UK, including blocking access to services.[54]

34. JUSTICE welcomes making online services providers subject to a UK regulator, who can assess whether companies have complied with their duty of care and take enforcement action should there be a breach. In our report, *Prosecuting Sexual Offences*, we highlighted that such an approach would mirror the approach to corporate responsibility in the Companies Act 2006 and would facilitate the stronger regulation of companies

[50] Part 3, Chapter 6.

[51] Part 4, Chapters 4 (Transparency Reporting) and Part 7, Chapter 4 (Information).

[52] Clause 16 and 26 (Duties about content reporting), and Clauses 17 and 27 (Duties about complaints procedures).

[53] Schedule 13.

[54] Clause 131-134. OFCOM will have the power to require providers to withdraw access to key services. If providers do not comply, OFCOM will be able to enforce this through a court order (a service restriction or interim service restriction order). For serious failures of the duty of care, OFCOM will have the power to block a company's services from being accessible in the UK, by requiring the withdrawal of services by key internet infrastructure providers, for instance browsers and web-hosting companies. In order to impose this sanction often must obtain an access restriction or interim access restriction order through the courts.

providing internet services.[55] However, the extent of executive oversight of OFCOM's duties and powers is cause for concern and calls into question the independence of OFCOM in carrying out its would-be functions under the Bill.

35. The Bill would give the Secretary of State the following significant powers in relation to OFCOM's duties and functions. The following powers are of particular concern:

    a) Clause 39 would give the Secretary of State the power to direct OFCOM to modify a code of practice "*for reasons of public policy*."

    b) Clauses 54 would enable the Secretary of State to set priority content that is harmful to children by way of secondary legislation. While clause 194 allows the Secretary of State to amend priority offences under Schedule 7.

Concerns

36. As recognised by Carnegie UK, the powers set out above are unique insofar as they would give the Secretary of State the ability to shape the role of OFCOM in relation to online regulation.[56] Whilst other pieces of legislation have empowered government to set high-level objectives and provide limited direction to OFCOM,[57] these powers would be far more wide-, allowing the Secretary of State to determine OFCOM's priorities, both strategic and in terms of content. This would go beyond setting overarching objectives and would allow for detailed government influence over how OFCOM policy is implemented, including decisions on what content is subject to regulation.

37. It is our view that, as it stands, the Bill would provide few safeguards, and would actively enable the boundaries of legitimate free speech to be shaped in accordance with the needs of the Government of the day. To avoid the politicisation of online speech, it is crucial that OFCOM can make independent decisions concerning the content of their policies and guidance without unwarranted political inference. Failing that, the Bill would

[55] JUSTICE, *Prosecuting Sexual Offences* (2019) paras 2.29 and 2.33.

[56] William Perrin and Lorna Woods, 'Secretary of State's powers and the draft Online Safety Bill', *Carnegie UK blog*.

[57] See for example, Communications Act 2003; Wireless Telegraphy Act 2006; Digital Economy Act 2017.

open the door to arbitrary exercises of government power in the online sphere, thereby posing a significant risk to freedom of expression.

38. Of particular concern is Clause 39, which would enable the Secretary of State to modify OFCOM's codes of practice to reflect Government policy. OFCOM's codes of practice set out how in-scope companies are to comply with their duties, including their duties concerning illegal content and duties regarding content that is harmful to children. Clause 39 would therefore give the Secretary of State unprecedented power to direct an independent regulator to modify the rules of content moderation of politically contentious topics. This would both undermine the regulator's independence and provide Governments with opportunity to use online regulation to promote their agendas and stifle debate around issues that challenge their policies.

39. Moreover, changes to codes of practice made under clause 39 are subject to very limited scrutiny or consultation. Whilst the Bill would require OFCOM to consult various stakeholders and experts[58] when preparing or amending its codes of practice, there is no similar requirement on the Secretary of State in modifying these codes. Giving the Secretary of State broad powers to modify codes of practice, which includes the power to reject OFCOM proposals over and over again until it is satisfied,[59] therefore risks undermining this consultation process, which the government itself has recognised as vitally important.[60]

40. Whilst modified codes of practice are then laid before parliament[61] where they are subject to the "*negative procedure"*,[62] if the reason for modification is national security or public safety in the case of terrorism or CSEA,[63] or the "*affirmative procedure*",[64] if the modification is made for reasons of public policy,[65] this does not change the fact that by

[58] Clause 36 (6) and (7).

[59] Clause 39 (7).

[60] HM Government, 'Online Harms White Paper: Full Government response to the consultation', 2020, p.42.

[61] Clause 39 and 40.

[62] Under the negative procedure unless either House of Parliament resolves not to approve the modification the modification will pass and OFCOM must issue a revised code of practice (Clause 40(5)).

[63] Clauses 39(1) and 40(4).

[64] Under the affirmative procedure a modification must be approved by a resolution of each House of Parliament before OFCOM issues the revised code of practice.

[65] Clause 39(1).

this point OFCOMs expert-led, evidence-based proposals, could have been overruled entirely by the Secretary of State, undermining the government's stated aim of ensuring existing expertise and best practice inform the UK's online regulatory framework;[66] even the affirmative procedure all Parliament is able to do is accept or reject the codes in their entirety. **For this reason, and the reasons outlined in the previous paragraph it is our view that the Secretary of State's power to direct OFCOM to modify their codes of practice should be removed from the Bill.**

41. JUSTICE is also concerned about the broad powers given to the Secretary of State in determining priority content to be regulated by the Bill. Clause 54 would enable the Secretary of State to designate content as "*priority content that is harmful to children*" and "*primary priority content that is harmful to children*." Once designated as "*priority content harmful to children*", service providers have a duty to protect children from such content and mitigate the risk of harm posed by this content on their platforms. In the case of primary priority content service providers also have a duty to prevent children of any age from encountering such content on their platforms.[67]

42. In designating content priority content or primary priority content that is harmful to children the Secretary of State must consider that the content in question poses a "*material risk of significant harm to an appreciable number of children in the UK*." There is no further guidance about what would constitute a "*material risk*" or what is meant by an "*appreciable number of children*." Moreover, whilst the Secretary of State must consult with OFCOM before making a designation, there is no requirement that they undertake any sort of consultation process with experts or gather any evidence in relation to the level or risk or harm particular content poses. Similarly, Clause 194 enables the Secretary of State to add an offence to the list of priority offences in Schedule 7 where it considers it appropriate to do so given the prevalence of the offence, the risk of harm to the individuals in the UK and the severity of that harm. There is no requirement to consult OFCOM when amending Schedule 7.

43. Whilst regulations designating priority content and primary priority content that is harmful to children and regulations amending Schedule 7 would be laid before Parliament and

[66] HM Government, 'Online Harms White Paper: Full Government response to the consultation', 2020, p.42.
[67] Clause 11 and 25.

subject to the affirmative procedure,[68] this process does not allow for back and forth between Parliament and the Secretary of State. Therefore, whilst these regulations are subject to some scrutiny, this does not provide anything like an adequate substitute for a robust consultation process which engages a broad range of experts and stakeholders, with the possibility of making amendments to the designation, rather than a take it or leave it approach.

44. It is our view that decisions about priority content,[69] in so far as they result in children and adults being prevented from accessing certain content, should be evidence led and free from political considerations. In designating particular content priority content, there is a significant risk of depriving individuals of access to crucial sources of information. For instance, Microsoft has highlighted the risk that requirements to remove posts about illegal immigration may also result in the removal of posts about lawful processes to immigrate.[70] Similarly, preventing children from accessing, for instance, material promoting eating disorders, may also prevent them from accessing information about where and how to get help. Whilst it might be entirely necessary and appropriate to include these types of content within the scope of content to be regulated by the Bill, given the potentials risk this poses to individuals‘ right to freedom of expression and access to information, such decisions should only be made following robust research and consultation processes, which engage a wide range of experts and stakeholders.

45. It is our view that OFCOM is most appropriately placed to carry out this function. Not only is OFCOM independent, given its other powers and duties within the Bill it is likely to have access to information relevant to decisions to designate priority content.[71] Moreover, OFCOM is already required to consult with a range of stakeholders when fulfilling some of its duties,[72] it will therefore have a relationship with these stakeholders and will have in place the infrastructure to carry out effective consultation processes with them. Given this,

[68] Clause 197.

[69] Be that in relation to content that is harmful to children or illegal content.

[70] This risk arises as both of these types of content are likely to contain similar language, so maybe identified as similar by automated technologies. Microsoft, ’Online Safety Bill – Parliamentary Briefing from Microsoft,’ 2022.

[71] For instance, OFCOM is required by the Bill to issue notices to certain Part 3 services requiring them to provide information on, amongst other things, the incidence of illegal and harmful content on their platforms. These reports could provide an evidence base for designating illegal content as priority illegal content, or designating priority content that is harmful to children as primary priority content that is harmful to children.

[72] For instance, its duties to prepare codes of practice.

**rather than granting the Secretary of State the power to set new priority content to be regulated by the Bill, the Bill should therefore require OFCOM to identify and form proposals for new priority content, which can then be laid before parliament. The Bill should specify that in forming these proposals OFCOM must consult with a range of stakeholders, including the Secretary of State**.[73]

## Transparency Reporting

46. Clause 64 of the Bill sets out provisions which would require Category 1, 2A and 2B services[74] to produce an annual transparency report containing information described by OFCOM in a notice given to the service. Under these provisions, OFCOM would be able to require these services to report on, amongst other things, information about the incidence of illegal content and content that is harmful to children, how many users are assumed to have encountered this content by means of the service, the steps and processes for users to report this content, and the steps and processes which a provider uses for dealing with this content. [75]

47. JUSTICE welcomes the introduction of transparency reporting in relation to illegal content and content that is harmful to children. We agree with the Government that effective transparency reporting plays a crucial role in building OFCOM's understanding of online harms, and empowering users to make informed choices about the services they use.[76] However, despite the inclusion of transparency reporting in the Bill representing a step in the right direction, we consider that these requirements could be strengthened. First, the Bill should make clear that, subject to appropriate redactions, companies will be required to make their transparency reports publicly available. Second, the Bill should impose minimum reporting requirements in relation to CSEA content.

Making Transparency Reports Publicly Accessible

[73] Clause 36 (6) provides an appropriate list.

[74] The threshold conditions for these categories are to be specified in secondary legislation. One of the threshold conditions which the Secretary of State must consider when making these regulations is the number of users on the service. Schedule 11.

[75] Part 1 and 2 of Schedule 8.

[76] HM Government, "The Government Report on Transparency Reporting in relation to Online Harms," 2020.

48. Whilst it is not clear from the Bill whether companies will be required to make these reports publicly available, JUSTICE considers that in most instances such a requirement would be appropriate. As noted above, one of the stated purposes of transparency reporting is that it would enable service users to make more informed choices about their own and their children's internet use. It's difficult to see how transparency reporting will serve this function if those reports are not made public. Moreover, in so far as transparency reporting would facilitate public accountability, it could also act as a powerful incentive for service providers to do more to protect their users.

49. However, JUSTICE also recognises that requiring companies to publish, for instance, the incidences of CSEA content on their platform may have the effect of encouraging individuals seeking such material towards platforms on which there are high incidents of that content. This must be avoided. Moreover, we recognise that simply having a high instance of CSEA content on a platform does not necessarily mean that that platform is problematic. As noted by Internet Watch Foundation, this may reflect the fact that the platform in question is good at detecting and dealing with such content.[77]

50. JUSTICE therefore considers that **the Bill should make explicit that once provided to OFCOM, transparency reports are to be made publicly available, subject to certain redactions.** To support this OFCOM should be required to produce guidance on the publication of transparency reports and the redactions companies should make before making reports publicly accessible. OFCOM should also retain the power to stop a company from publishing a particular transparency report if it considers that the risk of directing individuals to illegal materials outweighs the benefit of making a report public.

<u>Minimum reporting requirements for CSEA content</u>

51. JUSTICE also considers the Bill should contain additional transparency reporting requirements in relation to CSEA content. As it currently stands, the Bill does not specifically require companies to provide information about CSEA content on their platforms. Rather, OFCOM has discretion as to the types of information it requires

[77] Internet Watch Foundation, "IWF response to the Pre-Legislative Scrutiny Committee of the Draft Online Safety Bill" (2021).

companies to provide. This means that it may require different companies to provide different information, and in some instances may require companies to provide no information at all on CSEA content and the steps being taken to combat it. Moreover, the transparency reporting requirements in the Bill would only apply to a limited number of services, namely Category 1, 2A and 2B services.[78]

52. It is JUSTICE's view that, given its relatively clear-cut nature, **minimum reporting requirements should apply to CSEA content which would amount to an offence under Indecent Images of Children ("IIOC") legislation**. JUSTICE considers that the requirement to produce a transparency report with respect to this kind of content, rather than applying only to Category 1, 2A and 2B services (specific threshold conditions to be defined later, but number of users will be a relevant factor[79]), should be expanded to include all companies with a footprint in the UK. CSEA content amounting to an offence under IIOC legislation is extremely damaging irrespective of the platform on which it is viewed or proliferated and therefore factors such as the number of users should not impact whether a provider is required to produce a transparency report on this content.

53. As recommended in JUSTICE's report, *Prosecuting Sexual Offences*, reporting requirements regarding CSEA content should require internet companies which have a footprint in the UK to declare publicly:

    a) That it is satisfied its platform contains no material the possession of which would amount to an offence under Indecent Images of Children ("**IIOC**") legislation; or
    b) That it cannot confirm that its platform contains no material the possession of which would amount to an offence under IIOC legislation but that it has taken specified steps to check for content offending under that legislation; or
    c) That it has found offending material on its platform, and it has taken specified steps to remove it.[80]

54. Such requirements would not only provide companies with clarity as to their reporting duties in relation to such content, but would also ensure consistency in reporting, which

[78] Clause 68

[79] Schedule 11.

[80] JUSTICE, *Prosecuting Sexual Offences* (2019), para 2.33.

would in turn promote accountability, as relevant stakeholders would be able to hold companies to a clearly defined minimum standard.

## Media Literacy

55. In our report, *Prosecuting Sexual Offences,* JUSTICE highlighted the importance of educating children and young people as early as possible about appropriate sexual behaviour, image-based sexual abuse and how to keep safe online, in preventing offending.[81] As well as advocating for increased education, the report recommended that there should be a concerted strategy for national awareness raising around exploitation and consent, alongside a national campaign that makes people at risk of committing online sexual offences aware that services that offer help are available. [82]

56. JUSTICE welcomes the Government's recognition of the importance of promoting media literacy, as reflected in OFCOMs new duty to promote media literacy set out in s.11 of the Communications Act. However, **we consider that the Bill could bolster this duty by, for example, placing on OFCOM a specific duty to run national awareness campaigns promoting the importance of online safety, in particular campaigns on how to recognise and protect children from online grooming.**

57. In conjunction with this, the Bill should place **a responsibility on OFCOM to run a national advertising campaign that raises awareness of services that help those at risk of offending to tackle inappropriate sexual thoughts**. To support this, the Bill should require OFCOM to conduct research into the effectiveness of, and where appropriate commission and encourage, initiatives which provide these services. A number of these initiatives already exist and are identified in JUSTICE's report.[83]

**JUSTICE**

**January 2023**

---

[81] JUSTICE, *Prosecuting Sexual Offences* (2019), para 2.22.

[82] *Ibid*, para 2.24.

[83] For instance, the Stop it Now! and Aurora initiatives both use splash pages (pages that appear before the main website) to divert individuals who are about to access CSEA content away from that content, by alerting them to the fact that they are about to commit an offence, and directing them to their support services. See JUSTICE, *Prosecuting Sexual Offences* (2019), para 2.37-2.49.