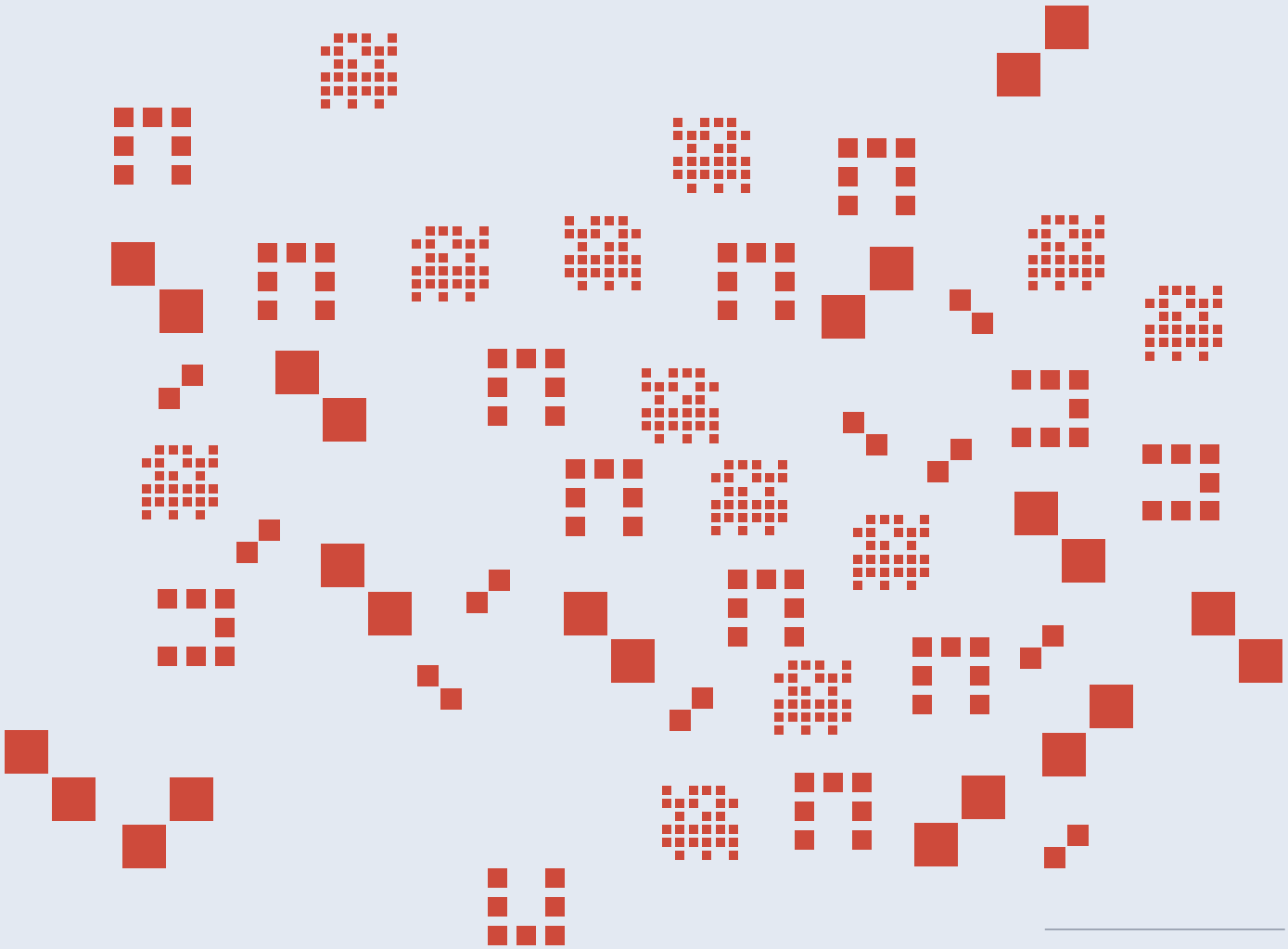
GLOBAL PARTNERS DIGITAL

The proposal to expand criminal liability for social media managers in the UK's Online Safety Bill

Policy Briefing

Authored by: Jacqueline Rowe



February 2023

The UK government is considering amending the UK's Online Safety Bill to expand the scope of criminal liability to cover individual social media managers who have failed to comply with their duties to protect children from harmful content.

In this briefing note, we:

- Set out the background to the proposed amendment;
- Compare the UK's proposal to relevant provisions in Ireland, Australia and New Zealand's online safety legislation;
- Highlight a number of human rights and practical concerns relating to the new amendment

We strongly urge Parliament to reject the proposed amendment on the grounds that it does not meaningfully strengthen protections for children online, while posing unacceptable risks to freedom of expression and making the UK tech sector a less attractive market for tech companies.

Contents

Introduction 3

Existing enforcement powers in the Online Safety Bill 3

The proposed amendment 5

How does the proposed amendment compare to other online safety regulations? 6

Concerns about the proposed amendment 10

Human rights concerns 11

Practical concerns 14

A way forward 16

Annexes 17

1. Introduction

The UK's Online Safety Bill (OSB) has undergone many changes during its long and winding route through government. Following extensive scrutiny and discussion on the 2019 White Paper on Online Harms and the draft version of the Bill published in 2021, the Bill was formally introduced in the House of Commons in March 2022. It underwent significant changes after its Committee and Report stages in autumn 2022,[1] before passing its 3rd reading in the Commons in January 2023. It now awaits scrutiny and discussion in the House of Lords, and its text must be agreed upon by both Houses and passed by Royal assent before the end of the Parliamentary session in autumn 2023, as it cannot be carried over to a new Parliamentary session a second time.[2]

In January 2023, as the Bill approached its final reading and assent in the House of Commons, 37 MPs jointly tabled an amendment which sought to make senior managers of social media platforms criminally liable for non-compliance with child safety duties.[3] Under pressure from this group of MPs, who threatened to block the passage of the Bill unless their amendment was incorporated,[4] the government announced that it would work with members of the group to re-draft the amendment and propose it at a later date.[5] This final amendment text is not available at this time, and so we base this briefing and analysis on the information available from the original proposed amendment and the government's response.

2. Existing enforcement powers in the OSB

The OSB in its current form would give Ofcom (the UK Communications Regulator) a range of enforcement powers over online platforms and search engines.[6] For example, Ofcom will be able to issue civil fines to companies that fail to comply with their duties of up to ten per cent of their annual global turnover;[7] apply to court for business disruption measures, such as blocking or restricting access to the service, in cases where the company has continually failed to respond to Ofcom's enforcement measures;[8] and request information from companies through "information notices" and audits, including a requirement for the company to name a "senior manager" who is responsible for ensuring compliance with such notices.[9] Under the current version of the bill, Ofcom also has the power to require the online

---

[1] See, for more information, Lorna Woods, "The Online Safety Bill – Status Report", 1 December 2022, *London School of Economics,* https://blogs.lse.ac.uk/medialse/2022/12/01/the-online-safety-bill-status-report/; Jacqueline Rowe, "The return of the UK's Online Safety Bill: What's changed and what's next?", 20 December 2022, *Global Partners Digital,* https://www.gp-digital.org/the-return-of-the-uks-online-safety-bill-whats-changed-and-whats-next/

[2] Scott Chalinor, "Current session of Parliament extended to Autumn 2023", 16 December 2022, *The Leaders Council,* https://www.leaderscouncil.co.uk/news/current-session-of-parliament-extended-to-autumn-2023

[3] Online Safety Bill Amendment Paper, Thursday 12 January 2023, New Clause 2 (p.2), https://publications.parliament.uk/pa/bills/cbill/58-03/0209/amend/onlinesafety_rm_rep_0112.pdf.

[4] Charles Hymas, "Ministers consider concessions after rebel Tories demand jail for tech executives over online harms", 12 January 2023, *The Telegraph*, https://www.telegraph.co.uk/politics/2023/01/12/ministers-prepare-back-tory-online-safety-law-revolt/

[5] Michelle Donelan, [UK Secretary of State for Digital Culture, Media and Sport], "Online Safety Update" 17 January 2023, Statement UIN HCWS500, https://questions-statements.parliament.uk/written-statements/detail/2023-01-17/hcws500

[6] Online Safety Bill, HL Bill 87(Rev) (as brought from the Commons), 18 January 2023, https://bills.parliament.uk/publications/49376/documents/2822

[7] OSB, Schedule 13

[8] OSB, Sections 131-135

[9] OSB, Chapter 4 and Schedule 12

platform or search engine to name a senior manager responsible for compliance with the information notice or audit request,[10] and this individual can be held individually and criminally liable for failing to provide the relevant information, punishable by a fine.[11] If the individual provides Ofcom with deliberately falsified information or information which is in an encrypted format so that Ofcom cannot interpret it, or if they destroy or suppress relevant information, they can face a fine or up to two years imprisonment.[12]

This model of narrow individual criminal liability for "information offences" only has been informed by various consultations by the UK government on the drafting of the bill. In its 2019 *Online Harms White Paper,*[13] the government stated that, in addition to fines, information requests and public notices, it was seeking input on the appropriateness of three additional enforcement powers: disruption of business activities; ISP-blocking; and criminal sanctions on individual social media company managers. In the White Paper, the government noted the challenges associated with senior management liability if adopted, including how to prescribe relevant roles and how to ensure that the requirements were proportionate for smaller companies. Many of those who provided inputs to the White Paper raised concerns over the criminal liability proposal, pointing out that it posed risks to freedom of expression and would reduce the attractiveness of the UK tech sector.[14] The government stated in its response that it would therefore **focus criminal sanctions only on ensuring compliance with the regulator's need for timely access to relevant information,** that such sanctions would not be introduced until at least two years after the regulatory framework comes into effect and depending on an impact review of the framework, and that they would be used only as a **last resort** if industry failed to meet their information-sharing responsibilities.

The question of individual criminal liability arose again as the draft bill—published in 2021—underwent pre-legislative scrutiny by a Joint Parliamentary Committee. The Committee's report of December 2021 made three recommendations in relation to enforcement and criminal liability for senior executives:

1. The Bill should require that companies' risk assessments be reported at Board level, to ensure that senior management know and can be held accountable for the risks present on the service, and the actions being taken to mitigate those risks;
2. A senior manager at board level or reporting to the board should be designated the "Safety Controller" and made liable for a new offence: failure to comply with their obligations as regulated service providers when there is clear evidence of repeated and systemic failings that result in a significant risk of serious harm to users; and

[10] OSB, Chapter 4
[11] OSB, Section 101
[12] OSB, Section 101
[13] UK Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, *Online Harms White Paper*, April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf, pp. 60-61.
[14] UK Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, *Online Harms White Paper: Full Government Response to the consultation*, December 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf, p.75. See also *Online Harms White Paper Consultation: Global Partners Digital Submission*, July 2019, Global Partners Digital, https://www.gp-digital.org/wp-content/uploads/2019/07/Online-Harms-White-Paper-Consultation_GPD-Submission.pdf; *Policy Responses to Online Harms White Paper,* May 2019, Open Rights Group, https://www.openrightsgroup.org/publications/org-policy-responses-to-online-harms-white-paper/

3. Criminal sanctions for failures to comply with information notices should be introduced within three months of Royal Assent.[15]

Importantly, the Joint Parliamentary Committee explained that individual criminal liability as outlined in (2) **should be a "proportionate last resort for the Regulator"**, and stated that, like any offence, it **should "only be initiated and provable at the end of an exhaustive legal process."**[16]

The government response to the Joint Parliamentary Committee's report was published in March 2022.[17] It stated simply that the government supported the Committee's belief that senior executives should be held accountable for the actions of their services, and that criminal sanctions for failures to comply with information notices would be introduced as soon as possible (likely two months) after Royal Assent. It did not take up the first two recommendations or broaden the scope of criminal liability of the Draft Bill.

3. The proposed amendment

The amendment proposed by the coalition of 37 MPs in January 2023 sought to expand the scope of senior management criminal liability to include non-compliance with duties laid out in **Section 11** of the Bill relating to safety and protections for children,[18] subject to fines or imprisonment for up to two years.[19]

Section 11 duties apply to any user-to-user services that are likely to be accessed by children and any part of those services which may be accessed by children. There are seven core duties for platforms (listed in full in **annex 1**), each of which relates to how they should manage and mitigate the risks to children posed by their services. These duties include preventing children of any age from encountering "primary priority content" (which is yet to be defined by the Secretary of State in secondary legislation[20]) and preventing certain age groups from encountering non-designated content judged to be harmful to them. "Proportionate" measures under these duties would be determined in relation to the levels of risk and severity of potential harm to children as identified in the company's child risk assessment, as well as the size and capacity of the provider of a service.

---

[15] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021–22,* https://committees.parliament.uk/publications/8206/documents/84092/default/, paras. 360-369

[16] Ibid., para 368.

[17] UK Secretary of State for Digital, Culture, Media and Sport, *Government Response to the Report of the Joint Committee on the Draft Online Safety Bill,* March 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1061446/E02721600_Gov_Resp_to_Online_Safety_Bill_Accessible_v1.0.pdf

[18] Please note that these duties have nothing to do with treatment of child sexual abuse material (CSAM) online. This content is and has always been illegal and falls under alternative provisions in the bill. Section 11 duties relate to content which is or may be harmful to all or some children, not to CSAM content.

[19] Online Safety Bill Amendment Paper, New Clause 2

[20] The government issued a statement in July 2022 indicating that it anticipated including pornography, self-harm, eating disorder and suicide content in the list of primary priority content which is harmful to children. Now that promotion of self-harm, eating disorders and suicide content are to be criminalised on the face of the Bill (supra footnote 1), at present there is no indication of what would be included in this content category beyond pornography. Nadine Dorries [UK Secretary of State for Digital Culture, Media and Sport], "Online Safety Update", 7 July 2022, Statement UIN HCWS194, https://questions-statements.parliament.uk/written-statements/detail/2022-07-07/hcws194.

In response to the proposed amendment, Michelle Donelan—the current Secretary of State for the Department for Digital, Culture, Media and Sport (DCMS)—issued a statement confirming that the government would work with the MPs concerned to reword the amendment and table it in the Lords.[21] She stated that the aim of the amendment will be to capture instances where senior managers have "consented or connived in ignoring enforceable requirements, risking serious harm to children", and that it will not affect those who have acted in good faith to comply in a proportionate way. She also stated that the government will ensure that the amendment does not make the UK tech sector unattractive to technology companies. Finally, she said that the final text of the amendment would come "at the end of ping pong between the Lords and the Commons", **indicating that the proposed text may not be published for some time and that it may be subject to only limited scrutiny by either House of Parliament before the Bill is passed**.

4. How does the proposed amendment compare to other online safety regulations?

The Secretary of State's announcement mentioned that the government would base their revised text on similar provisions in Ireland's Online Safety and Media Regulation Act, which was passed in December 2022. Yet the Irish Act is fundamentally different in many ways to the UK's OSB. We explain the key differences below.

Ireland's Online Safety and Media Regulation Act, 2022

Ireland's Online Safety and Media Regulation Act of 2022 (OSMR) amended the Broadcasting Act of 2009 to introduce a Media Commission and new responsibilities for online platforms relating to online safety.[22] For the most part, its provisions relating to individual criminal liability are similar to the information offences in the current draft of the UK's OSB, relating to a senior manager's failure to comply with information requests, audits or investigations by the Commission, or their provision of falsified or encrypted information in response to those requests.[23] However, the Irish OSMR also introduces individual criminal liability for an individual employee of a technology company after repeated failure to comply with Commission orders in relation to a contravention of the online safety regulation by the company, punishable by up to ten years in prison and/or a fine of up to €500,000.[24]

This form of individual criminal liability in the Irish Act differs from the proposed amendment to the UK's Online Safety Bill in three important ways:

1. **The contravention of an Online Safety Code triggers individual criminal liability only if the Commission has exhausted a number of other enforcement powers relating to the contravention.** To arrive at the point of individual criminal liability for a social media executive for contravention of an Online Safety Code, the company would have had to continue its contravention throughout an investigation by the Commission, and following receipt of an administrative fine, and receipt of a written

[21] Michelle Donelan, "Online Safety Update", fn 5.
[22] Ireland's Online Safety and Media Regulation Act 2022, https://www.gov.ie/pdf/?file=https://assets.gov.ie/234910/c1d7f6ae-7189-4fbe-b4d8-360056565e90.pdf#page=null
[23] Sections 139F, 139O, 139P, 139ZC and 139ZJ of the Irish Broadcasting Act, 2009, as introduced by Part 11 of the Irish Online Safety and Media Regulation Act, 2022.
[24] Section 139ZT (4,5) of the Irish Broadcasting Act, 2009, as introduced by Part 12 of the Irish Online Safety and Media Regulation Act, 2022.

notice.[25] Individual criminal liability is a "last resort" option, contrary to the proposed amendment in the UK where criminal liability could be imposed immediately.[26]

2. **The Online Safety Codes are to be designed by the Irish Media Commission, not by the Irish government, and will relate to how a platform addresses harmful online content, not how it performs on a range of child safety metrics.**
Under the OSMR, a "contravention" by an online platform which could eventually trigger individual criminal liability is a failure to comply with an Online Safety Code, which will be designed by the Media Commission independently of the Irish government.[27] These Codes will be designed in the knowledge that their contravention by a platform could eventually lead to individual criminal liability, meaning that they must be formulated clearly and provide enough information for an individual to reasonably understand what conduct they prohibit.

   In contrast, the Section 11 child safety duties under discussion in the UK's OSB have been drafted by the government, and include a broad range of responsibilities relating not only to platforms' treatment of harmful content but also their risk management and mitigation measures and their use of age verification technology. The breadth of the responsibilities included in Section 11 makes it difficult for an individual to know exactly what conduct or actions would constitute non-compliance and result in criminal prosecution.

3. **The Online Safety Codes will relate to how a platform manages "harmful online content" as defined by the Act itself, not all content which may pose a risk to a child.**
The Online Safety Codes under the Irish Act will lay out how platforms are required to deal with "harmful online content", which is explicitly defined in primary legislation (in the OSMR itself) as content which: (1) constitutes a criminal offence; (2) is subsequently specified as harmful online content by the Commission, and confirmed as such by the Minister through an order; (3) falls into the categories of bullying, promotion of eating disorders, self-harm or suicide; **or** (4) meets the "risk test" in that it gives risk to a person's life, or risks significant and reasonably foreseeable harm to a person's physical or mental health.[28] While this definition of harmful online content still restricts a broader range of content than would be considered a permissible restriction on freedom of expression under international human rights law,[29] it can only be altered only by an independent proposal from the Media Commission.

   In contrast, in the UK's OSB, Section 11 duties relate to platforms' treatment of content including "primary priority content harmful to children", which will only be defined in secondary legislation, and not by Ofcom but by the Secretary of State. Section 11

[25] Under sections 139ZA, 139ZK and 139ZT respectively.
[26] For more commentary, see Kir Nuthi, "Ireland's Latest Online Safety Law Is Unfair Parallel for Changes in UK's Online Safety Bill", 27 January 2023, *Centre for Data Innovation,* https://datainnovation.org/2023/01/irelands-latest-online-safety-law-is-unfair-parallel-for-changes-in-uks-online-safety-bill/
[27] Sections 139K and 139Y(a) of the Irish Broadcasting Act, 2009, as introduced by Parts 11 and 12 of the Irish Online Safety and Media Regulation Act, 2022.
[28] Section 139A of the Irish Broadcasting Act, 2009, as introduced by Part 8 of the Irish Online Safety and Media Regulation Act, 2022.
[29] For example, the scope of what content would be considered to constitute "bullying" or posing "reasonable foreseeable harm to a person's…mental health" is not clearly defined and may encompass a broad range of content types. For more information, see *Briefing Note: Online Safety and Media Regulation Bill,* September 2022, Irish Council for Civil Liberties, https://www.iccl.ie/wp-content/uploads/2022/09/OSMR.pdf

duties also include platforms' treatment even of content which has not been designated as harmful by the Secretary of State, but which the platform's risk assessment has identified as posing potential harm to children. The responsibilities that would carry criminal liability in the UK OSB under the proposed amendment therefore relate to an almost impossibly broad range of content.

Other jurisdictions

As well as Ireland, it is worth considering relevant provisions in the online safety regulations of other jurisdictions like Australia, Canada, the European Union and New Zealand. Some of these do not include criminal sanctions against platform employees, while others do but in specific and limited circumstances:

- **Australia**'s Online Safety Act[30] (OSA) makes it an offence for any person to not comply with an order from the eSafety Commissioner to provide evidence or documentation relevant to an investigation by the Commissioner. This is punishable by twelve months imprisonment, or a civil penalty of 100 units. Separately, Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019[31] (CCA) sought to reduce the incidence of online platforms being misused by perpetrators of violence. The law made it an offence for providers of content and hosting services to fail to remove access to abhorrent violent material expeditiously, punishable by a fine and/or up to 3 years' imprisonment for an individual,[32] or a fine of up to 10% of the annual turnover of a company in the case of a corporation.
- **Canada**'s Proposed Approach to Online Harms[33] (PAOH) proposes enforcement powers ranging from compliance orders, publishing decisions, information and inspection powers and administrative fines. No mention is made of criminal liability in the early plans set out by the Canadian government.
- The **European Union**'s Digital Services Act[34] of 2022 does not introduce criminal liability for social media platforms or individual employees, providing only for civil sanctions and fines.
- **New Zealand**'s Harmful Digital Communications Act 2015[35] (HDCA) empowered District Courts to order online content hosts to take down or disable public access to specific material, to identify a user to the court, to publish a correction or to give an affected individual a right to reply. Under the Act, it is an offence for an online content host to fail to comply with these court orders, punishable by imprisonment for 6 months or a fine of up to $5,000 (in the case of a natural person) or a fine not exceeding $20,000 (in the case of a body corporate).

---

[30] Australia's Online Safety Act 2021, Section 205, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6680_aspassed/toc_pdf/21022b01.pdf;fileType=application%2Fpdf,
[31] Articles 474.33 and 474.34 of Australia's Criminal Code, as added by Schedule 1 of Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, https://www.legislation.gov.au/Details/C2019A00038
[32] See page 12 for criticism of this provision from two United Nations Special Rapporteurs
[33] Canada's Proposed Approach to Online Harms, Module 1(D), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html
[34] Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065
[35] New Zealand's Harmful Digital Communications Act 2015, https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

We compare these criminal liability provisions in the two tables below (with detailed versions of each table including relevant provisions from each law in **Annexes 2 and 3).**

Table 1: Comparison of types of criminal liability included in online safety regulations by Australia, Canada, the European Union, Ireland, New Zealand and the UK

	Includes criminal liability for "information" offences? (i.e. misleading the regulator?)	Includes criminal liability for broader content moderation / online safety duties?
Australia (OSA)	Yes	No
Australia (CCA)	No	Yes
Canada (POAH)	No	No
European Union (DSA)	No	No
Ireland (OSMR)	Yes	Yes
New Zealand (HDCA)	No	Yes
UK (OSB)	Yes	Yes (Proposed Amendment*)

Table 2: Comparison of approach to criminal liability for content moderation in Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, Ireland's Online Safety and Media Regulation Act 2022, New Zealand's Harmful Digital Communications Act 2015, and the proposed amendment to the UK's Online Safety Bill.

	Must alternative enforcement avenues be used before imposing criminal liability?	Is the nature of the offence defined or determined by an independent body?	Is criminal liability only triggered in relation to a well-defined and clear category of online harm?
Australia (CCA)	No	Yes	Yes
Ireland (OSMR)	Yes	Yes	In part
New Zealand (HDCA)	Yes	Yes	No**
UK (Proposed Amendment*)	No	No	No

* While the text of the actual amendment is not yet available, for the purposes of comparison we have used the text put forward by 37 MPs in January 2023.
** The court must, however, consider the degree of harm caused and other factors before making an order.

If the UK government chooses to expand the scope of individual criminal liability for social media managers to include non-compliance with a broad range of child safety duties, **it will diverge considerably from the approach taken by like-minded countries as outlined above**.

Furthermore, such an approach may have international repercussions as other, less democratic nations also seek to regulate online platforms ("if the UK arrests company

employees for the political speech carried on their platforms, why shouldn't they?")[36] Several authoritarian regimes have already implemented so-called "hostage-taking" clauses for regulating online platforms, to considerable concern that such clauses will be used to threaten or bully employees into compliance with government requests. For example, Turkey amended its Law on Internet Crimes in 2020 to require social media platforms to open physical offices in Turkey and designate a "contact-point" employee who would be individually responsible for compliance.[37] Russia introduced similar requirements for social media platforms in 2021,[38] and when Google refused to take down an app built by an opposition politician from its play store, the Communications regulator reportedly threatened a top Google executive with imprisonment for continued non-compliance with the order.[39] If the UK still wishes to be recognised as a "global leader in innovation-focused digital legislation",[40] it must consider the consequences of other countries following its example.

5. Concerns about the proposed amendment

Regardless of how other jurisdictions are approaching the issue of individual criminal liability, we now evaluate the proposed amendment on its own merit. The proposed amendment ultimately fails to provide sufficient clarity for an individual to reasonably know what conduct is prohibited under the law, thus failing to fulfil the standard of legality for criminal law provisions.[41] Furthermore, the amendment is likely to encourage online platforms operating in the UK to take one of the following steps:

1. ban children entirely from their services and enforce these bans through nascent age verification technologies;
2. proactively remove any content that could in any circumstance be considered harmful to any child, censoring vast swathes of perfectly legal adult speech and content;
3. Conduct less thorough risk assessments under Schedule 10, so as to trigger fewer requirements that could result in criminal liability under Schedule 11;

---

[36] Written evidence from Open Rights Group (OSB0118) to the Joint Parliamentary Committee on the Draft Online Safety Bill, 21 September 2021, *Open Rights Group*.
[37] "Turkey tightens grip on social media platforms", 22 July 2020, *RSF,* https://rsf.org/en/turkey-tightens-grip-social-media-platforms
[38] "What does Russia's new "hostage-taking" law mean for social media companies?", 21 February 2022, *Global Voices,* https://globalvoices.org/2022/02/21/what-does-russias-new-hostage-taking-law-mean-for-social-media-companies/
[39] Joshua Zitser, "Putin's agents reportedly threatened a top Google executive in Moscow with a 24-hour ultimatum – Take down Russia protest vote app or go to prison", 12 March 2022, *Insider,* https://www.businessinsider.com/russia-agents-threatened-google-exec-to-remove-voting-app-moscow-2022-3?r=US&IR=T
[40] Department for Digital, Culture, Media & Sport and The Rt Hon Oliver Dowden CBE MP, "New plan to make Britain global leader in innovation-focused digital regulation", 6 July 2021, https://www.gov.uk/government/news/new-plan-to-make-britain-global-leader-in-innovation-focused-digital-regulation
[41] According to the principle of legality applied to criminal law an offence must be clearly defined in the law and it must be foreseeable for any person. Legality principle in criminal law is recognised by Article 7 of the European Convention on Human Rights (ECHR), which is part of the Human Rights Act 1998. *"Since the criminal law is arguably the most direct expression of the relationship between a State and its citizens, it is right as a matter of constitutional principle that the relationship should be clearly stated in a criminal code the terms of which have been deliberated upon by a democratically elected legislature"*. The Law Commission (LAW COM. No. 177). A Criminal Code for England and Wales, volume I, Report and Draft Criminal Code Bill. 1989. Para. 2.2. https://www.lawcom.gov.uk/app/uploads/2015/06/Criminal_Code_177_1.pdf

4. Withdraw from the UK market altogether.

All of these courses of action pose risks to individuals' human rights and raise questions about the practical implementation of the proposed amendment. We explore these concerns in detail in the following sections.

Human rights concerns

The legality principle in criminal law is established in Article 15.1 of the International Covenant on Civil and Political Rights (ICCPR), according to which criminal offences and punishments can only be set by law and must be clearly defined so people know which acts are criminal and their consequences.[42] Moreover, international human rights standards and accompanying guidance are clear that criminal sanctions on social media employees in relation to content moderation pose unacceptable risks to freedom of expression. The open nature of the description of criminalised conduct in the current proposal does not fulfil the legality test for freedom of expression restrictions according to Article 19 of the ICCPR. Furthermore, the proposed amendment would strongly incentivise banning or restricting children from accessing large portions of an online platform using untested and unregulated age verification technologies, and also strengthens a top-down, platform-led approach to harms management, rather than empowering parents and children to make informed decisions about the content they wish to see online. Here, in more detail, are the key issues with the amendment from a human rights perspective.

1. Criminal sanctions on social media employees in relation to content moderation duties have a "chilling effect" on freedom of expression

Under international human rights law, the right to freedom of expression and the right to receive and impart information and ideas without interference by public authority are guaranteed under Article 19 of the ICCPR and Article 13 of the International Covenant on the Rights of the Child (ICRC). Restrictions on these rights are only permissible when they are provided by law, pursue a legitimate aim, and are necessary and proportionate. While the UK government's aim appears to be protecting children from exposure to harmful content or behaviour online, which would be a legitimate aim insofar as it prevented a child from being harmed, introducing criminal sanctions for failure to prevent children accessing legal content online is a disproportionate response and would encourage companies to censor legal speech, contrary to the UK's obligations to protect and promote freedom of expression.

International human rights law and guidance is very clear on the disproportionality and dangers of introducing criminal sanctions for individual online platform employees for content moderation duties. In a 2018 report on the regulation of user-generated online content, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression highlighted the importance of states ensuring an "enabling environment" for online freedom of expression, and specifically recommended that:

> *"States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality,*

[42] ICCPR, Article 15.1: *"No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time when the criminal offence was committed. If, subsequent to the commission of the offence, provision is made by law for the imposition of the lighter penalty, the offender shall benefit thereby"*.

> *necessity and legitimacy. States should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression."*[43]

The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism also previously condemned the provision on criminal liability introduced in Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, 2019 (see p.7) as inconsistent with Australia's human rights obligations:

> *"The time and effort required to make such nuanced assessments of context and preserve protected exercises of freedom of expression are at odds with the proposed obligation on service providers to "expeditiously" remove content. Given these conflicting considerations, the threat of criminal sanctions is likely to tip the scales in favor of disproportionate restrictions on freedom of expression, which may undermine rather than protect the public interest."*[44]

Importantly, the Australian law imposed criminal liability for social media executives **only in relation to the hosting of the most egregious and violent content, and was still considered disproportionate by leading human rights experts.** The Section 11 child safety duties under consideration for criminal sanctions for non-compliance in the UK's OSB are considerably broader in scope, both in terms of the nature of responsibilities in question and the scope of content categories that may be implicated. The sanctions proposed in the OSB amendment would therefore be even less proportionate than those in the Australian law critiqued by the special rapporteurs.

Finally, criminal penalties on staff of social media platforms in relation to content moderation duties have recently been criticised as inconsistent with international standards on freedom of expression by the United Nations Educational, Scientific and Cultural Organization (UNESCO). The current draft of their new guidelines for states on the regulation of digital platforms—which are being developed in consultation with UNESCO member states, private sector representatives, technical experts and civil society organisations—explicitly states that states should:

> *"Refrain from subjecting staff of digital platforms to criminal penalties for an alleged or potential breach of regulations in relation to their work on content moderation and curation, as this may have a chilling effect on freedom of expression."*[45]

While Section 11 of the UK's Online Safety Bill concerning child safety duties does include brief mention of platforms' responsibilities to consider freedom of expression and privacy in the

---

[43] United Nations Office of the High Commissioner for Human Rights, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," 6 April 2018, A/HRC/38/35, https://www.ohchr.org/en/documents/thematic-reports/ahrc3835-report-special-rapporteur-promotion-andprotection-right-freedom

[44] United Nations Office of the High Commissioner for Human Rights, "Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 4 April 2019, https://freedex.org/2019/04/04/comments-on-new-australian-law-on-online-abhorrent-violent-material/, p.5.

[45] United Nations Educational, Scientific and Cultural Organization, "Guidelines for regulating digital platforms: a multistakeholder approach to safeguarding freedom of expression and access to information: Draft 2.0", February 2023, https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en, Para. 27(g)

implementation of their child safety duties, the weak protections for these rights in the Bill and the lack of enforcement measures relating to platforms' disregard for these rights mean that if criminal sanctions are introduced for non-compliance with Section 11 duties, platforms are overwhelmingly likely to err on the side of caution and remove content which is permissible and should not be restricted under international human rights law. There is also a wealth of evidence that suggests that this overcautious censorship disproportionately impacts marginalised users, whose speech, images and content are more likely to be erroneously flagged and removed by online platforms.[46] The proposed criminal sanctions may also therefore introduce new risks to individuals' right to non-discrimination.[47]

2. Age-gating the internet is a disproportionate response and relies on untested technologies for implementation

If companies do not remove legal content which may be harmful to children in order to comply with Section 11 duties, they will instead have to age-gate children's access to such content or portions of their services which host such content. In practice, this is likely to mean that even if only 1% of material on a website or platform may be harmful to some children, the platform is incentivised to remove all children from that website or platform in order to escape criminal liability for a child encountering such content. This poses risks to children's rights to freedom of expression and rights to access accurate information, shutting them out not only from content which is harmful to them but also content which may be helpful, contrary to guidance from the United Nations Committee on the Rights of the Child on facilitating children's rights in the digital environment.[48]

Furthermore, mandating platforms to age-gate their services in this way drastically increases their reliance on nascent age verification and age assurance technologies. These tools are largely untested and as yet unregulated, and many have raised concerns around how such tools treat private and personal information, and relating to the known risks of bias and discrimination of some biometric age estimation tools.[49] Until there are clear codes of

---

[46] See, for examples: Oliver Haimson et al, "Disproportionate removals and differing content moderation experiences for conservative, transgender, and black social media users: Marginalization and moderation gray areas", October 2021, *Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2),* https://dl.acm.org/doi/abs/10.1145/3479610, pp. 1-35; Nosheen Iqbal, "Instagram censorship of black model's photo reignites claims of race bias", 9 August 2020, *The Guardian,* https://www.theguardian.com/technology/2020/aug/09/instagrams-censorship-of-black-models-photo-shoot-reignites-claims-of-race-bias-nyome-nicholas-williams; Maarten Sap et al, "The Risk of Racial Bias in Hate Speech Detection", July 2019, *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf

[47] ICCPR, Article 26.

[48] United Nations Office of the High Commissioner for Human Rights, "General Comment No.25 of the Rights of the Child Convention on children's rights in relation to the digital environment", 2 March 2021, *CRC/C/GC/25,* Section VI, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[49] See, for example, Sonia Livingstone, Mariya Stoilova and Svetlana Smirnova, "Can the internet be age appropriate, or at least not inappropriate or harmful? The promise of age verification and parental control tools", 9 September 2021, *EUConsent,* https://euconsent.eu/can-the-internet-by-age-appropriate-or-at-least-not-inappropriate-or-harmful-the-promise-of-age-verification-and-parental-control-tools/; "ORG – EDRi Joint Submission To The Ico Technology And Innovation Foresight Call For Views: Biometric Technologies", 7 February 2022, *Open Rights Group,* https://www.openrightsgroup.org/publications/org-edri-joint-submission-to-the-ico-technology-and-innovation-foresight-call-for-views-biometric-technologies/; "Online age verification: balancing privacy and the protection of minors", 22 September 2022, *Commission nationale de l'informatique et des libertés,* https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

practice and safeguards surrounding the use of age verification and age assurance technologies by online platforms, it would be unwise to force social media managers to roll them out at scale in order to avoid criminal charges for non-compliance with Section 11 duties.

3. Criminal sanctions increase platforms' top-down content governance, rather than increasing parents' and children's agency over what they see online

Development varies considerably among children; what may be harmful or distressing for one child may not be for another. The criminal liability amendment would serve to strengthen the top-down enforcement model of the Bill, whereby platforms make blanket decisions affecting millions of users to escape sanctions—what is described as a "feudal" approach by Wikipedia's founder.[50] As such, the amendment is likely to further entrench the existing power of platforms to dictate what people can and cannot say online, restricting people's access to varied and accurate sources of information and interfering with legitimate expression. The OSB should instead focus on giving users greater agency to use and navigate such platforms on their own terms—for example, by empowering parents to set appropriate guardrails around their children's online lives and empowering and educating children about how to report harmful content. This would support children to navigate online spaces safely while protecting their rights to freedom of expression and access to information online, and to have their views considered in issues that affect them according to their progressive autonomy.[51]

Practical concerns

Beyond the potential human rights impacts of the proposed amendment, it will also be very difficult to construct the proposed offence in a manner which is sufficiently clear for individuals to know what conduct is prohibited, due to the broad nature of Section 11 duties. The implementation of expanded criminal liability in practice is also likely to disproportionately impact smaller online platforms, further entrenching the power of existing platform monopolies. We examine these concerns below.

1. It will be very difficult to formulate an amendment text which would provide a suitably clear definition of the proposed offence

The government's own Parliamentary Under-Secretary of State for Tech and the Digital Economy of the United Kingdom highlighted in the Public Bill Committee of 15 December 2022 that it would be very difficult to broaden the scope of criminal liability to child safety duties in such a way that senior managers could foresee exactly what type of conduct constitutes the offence:

> *"For a criminal offence, a precise statement of the prohibited behaviour must clearly be set out—in other words, that a particular act or omission constitutes the criminal offence. In this case, a failure to comply with the relevant duties listed in the amendment would depend on a huge number of factors. That is because the Bill applies to providers of various sizes and types. In most areas, the framework is flexible, rather than prescriptive: it does not prescribe certain steps that providers*

[50] Keumars Afifi-Sabet, "Jimmy Wales: Online Safety Bill could devastate small businesses and startups", 8 February 2023, *IT Pro,* https://www.itpro.co.uk/business-strategy/startups/370036/jimmy-wales-online-safety-bill-could-devastate-small-businesses

[51] United Nations Convention on the Rights of the Child (ICRC), Article 12. See also UN OHCHR, "General Comment No.25 of the Rights of the Child", paragraphs 20-21.

must take. That means that it may be difficult for individuals to foresee exactly what type of conduct constitutes an offence, and that can easily lead to unintended consequences and to tech executives taking an over-zealous approach to content take-down for fear of imprisonment."[52]

It is for this reason that modelling the amendment on the Irish bill—which imposes criminal liability on individual employees only in relation to a specific contravention of an Online Safety Code, identified and investigated in full by the Commission—is impractical. **Providing sufficient clarity on what the proposed offence actually is would require substantive re-drafting of Section 11 duties,** or identification of specific circumstances in which individual criminal liability would be triggered in relation to such duties, and how negligence or criminal intent would be proven. At this late stage in the legislative process, and with limited time to pass substantive amendments, this is likely to prove difficult.

2. The amendment would disproportionately impact smaller companies, entrenching existing monopolies

The introduction of criminal liability for senior managers of online platforms in relation to child safety duties is likely to disproportionately affect smaller companies, which may not have the resources to roll out age verification technologies at scale, to upscale content moderation teams to deal with a considerably broader scope of potentially harmful content, or to afford expensive legal advice that may be necessary in negotiating the new provisions. Furthermore, it may be more challenging for smaller companies to be able to find or designate an individual willing to take on criminal liability for compliance with these duties, either because salaries are less competitive or because employees at smaller companies may fulfil a variety of different roles at the same time. Section 11 duties relate to work and decisions by a vast range of product, policy, legal and trust and safety teams across a company's operations and workforce; it may be only the largest of technology companies that would be able to pay an attractive enough salary for someone to assume this high level of responsibility.

These factors are likely to further increase the dominance of a small number of very large platforms over the UK market, stifling startups and innovation and further entrenching the power of Big Tech over public discourse and users' freedom of expression.[53] For example, it is not clear how OSB responsibilities will apply to platforms like Wikipedia, where none of the 700 paid staff or contractors play a role in content curation or moderation, relying instead on a global community of volunteer moderators to make democratic decisions on content moderation informed by public discussion and negotiation.[54]

3. The amendment may incentivise companies to conduct less holistic risk assessments

---

[52] Paul Scully [Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport], Online Safety Bill Deb, 15 December 2022, c142, https://www.theyworkforyou.com/pbc/2022-23/Online_Safety_Bill/03-0_2022-12-15a.138.0?s=speaker%3A25335

[53] For more information, see "UK: Criminal liability in the Online Safety Bill will threaten free speech", 16 January 2023, *ARTICLE19,* https://www.article19.org/resources/uk-criminal-liability-online-safety-bill-threatens-free-speech/

[54] Keumars Afifi-Sabet, "Jimmy Wales: Online Safety Bill could devastate small businesses and startups"; Wikimedia Policy, "Deep Dive: The United Kingdom's Online Safety Bill", 17 November 2022, *Medium,* https://medium.com/wikimedia-policy/deep-dive-the-united-kingdoms-online-safety-bill-b7020723dd39

Some of the child safety duties in Section 11 are informed by the companies' child risk assessments, which are a requirement of Section 10 of the Bill. Yet applying criminal liability only to compliance with Section 11 may incentivise companies to deliberately reduce or minimise the scope of risks identified through their risk assessment process; precisely because, if risks are identified through this process which are not subsequently dealt with by the company as per Section 11 requirements, this would trigger individual criminal liability. The amendment may therefore incentivise "checkbox" minimum compliance with the risk assessment duties, rather than more genuine attempts to identify and mitigate risks through holistic and far-reaching risk assessments.

6. A way forward

The proposed amendment poses a number of concerns, and international human rights norms and guidance clearly indicates that criminal sanctions on individual social media company employees for content moderation duties are incompatible with states' responsibilities to respect, protect and fulfil human rights, particularly individuals' and children's rights to freedom of expression and access to information.[55] **In light of this, we strongly recommend that the UK government should not expand the scope of individual criminal liability for senior managers of social media companies within the OSB to include non-compliance with child safety duties laid out in Section 11.**

If the UK government insists on strengthening individual criminal liability for employees of online platforms in relation to child safety, **we strongly recommend that the amendment should not broadly relate to "compliance" with all Section 11 duties, nor to duties in relation to legal and as yet undefined "primary priority content for children".**[56] Instead, criminal liability in relation to child safety online should only be triggered when:

- **a senior manager has persistently ignored clear direction from Ofcom in relation to responsibilities under the OSB, and all other enforcement powers to incentivise compliance have been exhausted;**
- **the conduct of the senior manager relates to non-compliance with responsibilities relating to illegal content only** (i.e. that which has been confirmed as illegal by a jurisdictional authority);
- **the conduct of the senior manager has resulted in significant and demonstrable harm to a child or children using the service.**

Finally, it is vitally important that such a major amendment be discussed properly by policymakers and legislators, and that the government seek multistakeholder input on such an important regulatory mechanism in an open, inclusive and transparent fashion as they draft the text. **Rather than introduce the text of the amendment at the end of the process—when the government is likely to be under intense pressure to pass the Bill before the end of the Parliamentary session—DCMS should publish the text of the amendment as soon as possible and introduce it as an amendment during the Lords Committee or Report stages so that it can follow the regular process of scrutiny and debate.**

---

[55] ICRC, Art. 13; ICCPR, Art 19.

[56] Given that the government has separately introduced the promotion of self-harm, suicide and eating disorder content as criminal offences in other amendments, it is our view that the most egregious content which would cause harm to a child will now be captured under provisions relating to illegal online content, meaning that criminal liability should be reserved for circumstances involving illegal content only and not the more broadly defined "(primary) priority content which is harmful to children".

Annexes

Annex 1: UK Online Safety Bill–summary of child safety duties laid out in Section 11

The child safety duties laid out in Section 11 are as follows:

1. a duty to take proportionate measures to mitigate and manage the risks of and impact of harm to children identified by the company's child risk assessment;
2. a duty to implement proportionate systems and processes to prevent children of any age from encountering primary priority content that is harmful to children, and to prevent children in age groups judged to be at risk of harm from other content that is harmful to children from encountering it through the service;
3. a duty to specify in the terms of service how children are to be prevented from encountering primary priority content which is harmful to children and non-designated content which is judged to be harmful to children in different age groups;
4. a duty to apply the provisions of the terms of service mentioned in (3) consistently;
5. a duty to specify in the terms of service what measures are applied to prevent children from accessing all or part of the service, if applicable, and to apply such provisions consistently;
6. a duty to specify in the terms of service what proactive technology is used for the purpose of compliance with duties (2) or (3);
7. a duty to ensure that the provisions of the terms of service mentioned for duties (3), (5) and (6) are clear and accessible.

N.B. Duties 1 and 2 apply across all areas of a service, and may include age assurance, regulatory compliance and risk management arrangements, design of functionalities, algorithms and other features, policies on terms of use, policies on user access to the service or to particular content present on the service, content moderation, content ranking, user support measures, and staff policies and practices.

N.B. Duties 2 and 3 are to be taken to extend only to content that is harmful to children where the risk of harm is presented by the nature of the content (rather than the fact of its dissemination)

Annex 2: Comparison of types of criminal liability included in online safety regulations by Australia, Canada, the European Union, Ireland, New Zealand and the UK

Country	Legislation	Includes criminal liability for "information" offences? (i.e. misleading the regulator?)	Includes criminal liability for broader content moderation / online safety duties?
Australia	Online Safety Act	**Yes.** Section 205 prohibits any person from refusing to cooperate with an investigation by the Commission (for example, by failing to give evidence or answer questions as required) without a reasonable excuse. The penalty is 12 months imprisonment or 100 civil penalty units. These provisions could apply to an individual employee of a social media platform who was required by the Commissioner to give evidence or information in relation to an investigation.	**No**
Australia	Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act	**No.**	**Yes**. The Amendment Act adds to Division 474 of the Criminal Code. New article 474.34 makes it an offence for content services and hosting services not to "ensure the expeditious removal" of abhorrent violent material which is accessible from or hosted by their service. If committed by an individual, this offence is punishable by imprisonment for up to three years and/or a fine of up to 10,000 penalty units. If committed by a body corporate, it is punishable by a fine of up to 50,000 penalty units or 10% of annual turnover (N.B. New article 474.33 also makes it an offence for an internet service provider, a content service or a hosting service to fail to report such material to Australian police. This carries a penalty of 800 penalty units but appears not to be directed at individuals within those companies, as 474.34 could be).
Canada	Proposed Approach to Online Harms	**No.**	**No.**
European Union	Digital Services Act	**No.**	**No.**

Ireland	Online Safety and Media Regulation Act, 2022	**Yes.** Under new sections 139F, 139O, 139P, 139ZC and 139ZJ of the Irish Broadcasting Act, introduced by Parts 11 and 12 of the OSMA, offences relating to provision of information to the regulator include: - Failing to comply with requests for designation-related information - Failing to comply with information notices - Providing false information in response to information notice - Failing to cooperate with an audit notice - Obstructing an investigation by an authorised officer, including by destroying evidence or providing false evidence - Providing false or misleading material in response to a request for further information related to an investigation by the commission The first three are Category 1 offences, punishable by imprisonment of up to ten years or a fine of up to €500,000; the rest are Category 2 offences, punishable by imprisonment of up to five years or a fine of up to €50,000. (Section 139ZZ)	**Yes.** Under new section 139ZT of the Irish Broadcasting Act, introduced by part 12 of the OSMA, it is a Category 1 offence not to comply with a written notice to cease a contravention of media or online safety rules (139ZT). Category 1 offences are punishable by imprisonment of up to ten years or a fine of up to €500,000
New Zealand	Harmful Digital Communications Act 2015	**No.**	**Yes.** Section 19 (2) provides District Courts with the power to order online content hosts to comply with court orders to take down or disable public access to specific material, to identify a user to the court, to publish a correction or to give an affected individual a right to reply. Section 21(2) makes it an offence for an online content host to fail to comply with these court orders, punishable by imprisonment for 6 months or a fine of up to $5,000 (in the case of a natural person) or a fine not exceeding $20,000 (in the case of a body corporate).
UK	Online Safety Bill (as brought from the Commons) and Amendment Paper (New Clause 2)*	**Yes.** Under Section 101, a senior manager of an online platform or search engine can be held individually and criminally liable for failing to provide Ofcom with requested information, punishable by a fine. If the senior manager provides Ofcom with deliberately falsified information or information which is in an encrypted format so that Ofcom cannot interpret it, or if they destroy or suppress relevant information, they can face a fine or up to two years imprisonment.	**Yes.** New Clause 2 would make it an offence for a senior manager to fail to comply with a "relevant duty", meaning a duty provided for in Section 11 of the Act.

Annex 3: Comparison of approach to criminal liability for content moderation in Australia, Ireland, New Zealand and the UK

Country	Legislation	Must alternative enforcement avenues be used before imposing criminal liability?	Is the nature of the offence defined or determined by an independent body?	Is criminal liability only triggered in relation to a well-defined and clear category of online harm?
Australia	Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act	**No.** Individual criminal liability could be incurred before any other enforcement powers were directed at the platform.	**Yes.** Under new articles 474.35 and 474.36, the eSafety Commissioner would provide a written notice identifying specific abhorrent violent content available on the the specific content or hosting service in question. This would then have to be proven in a court of law in order to prosecute an individual for recklessness under this offence.	**Yes.** New article 474.31 defines abhorrent violent material as that which depicts abhorrent violent conduct, which is defined in 474.32 as terrorism, murder, torture, rape or kidnapping.
Ireland	Online Safety and Media Regulation Act, 2022	**Yes.** Individual criminal liability would only be incurred after a Commission Investigation into the contravention in question (new section 139ZA) and an administrative fine levied on the company (139ZK).	**Yes.** The offence would be in relation to a contravention of a specific part of an Online Safety Code. The Media Commission will design the Online Safety Codes, and will also determine whether a specific contravention has occurred through an independent investigation.	**In part.** The Online Safety Codes will relate to how a platform deals with "harmful content", which is defined in new section 139A as one of 4 content types (see p. 6 for details). While this does provide some clarity over what content would be in scope, new content categories may be added over time by the Commissioner, and the scope of what content would be considered to constitute "bullying" or posing "reasonable foreseeable harm to a person's...mental health" is not clearly defined and may encompass a broad range of content types.
New Zealand	Harmful Digital Communications Act 2015	**Yes.** Corporate criminal liability is only triggered after the platform has failed to respond to the court order to remove the content.	**Yes.** The platform would only be liable for non-compliance with a court order to remove specified content.	**No.** Under section 19, there is no definition of the type of content that the District Court could order the removal of. However, the court must consider the content, the harm it may cause and the intent of the sender, amongst other factors, before making an order.
UK	Online Safety Bill (as brought from the Commons) and Amendment Paper (New Clause 2)*	**No.** Individual criminal liability could be incurred before any other enforcement powers were directed at the platform.	**No.** The "relevant duties" in Section 11 have been designed by the government, not by Ofcom. Furthermore, the Secretary of State has the power to specify new content types that would trigger broader criminal liability under Section 11 without adequate legislative oversight.	**No.** Section 11 duties relate not only to "primary priority content harmful to children" which has not yet been defined, but also non-designated content that may be identified through a risk assessment as posing harm to children, meaning that virtually all content is in scope.

* While the text of the actual amendment is not yet available, for the purposes of comparison we have used the text put forward by 37 MPs in January 2023.