

Online Safety Bill

UK will add criminal liability for tech execs in relation to children

Alice Enders

alice.enders@endersanalysis.com

Niamh Burns

niamh.burns@endersanalysis.com

+44 (0)20 7851 0900

24 January 2023

Cross-party support for an 11th hour amendment to the Online Safety Bill's Commons report stage has forced the Government to agree that a new criminal liability for tech executives will be added in the Bill's passage through the Lords

The Government has caved to pressure to introduce criminal liability for tech executives into the Online Safety Bill (OSB), with Secretary of State Michelle Donelan scrambling over the weekend of 13-15 January to head off a vote on a more extreme amendment. She has committed to introducing an amendment in the Lords modelled on similar legislation in Ireland, whereby executives could be jailed for failing to respond to an order to stop their non-compliance with regulation on children's safety.¹ Until now the Government was only seeking to enable criminal prosecution for tech executives actively lying to Ofcom during its investigation.

This change follows a high-profile backbench campaign to introduce a higher level of criminal liability: in an article published by The Telegraph on 9 January, Miriam Cates MP announced her campaign with Sir Bill Cash to amend the OSB to add the "offence of failing to comply with a relevant duty" in relation to children's safety for the senior manager of a company providing a user-to-user service.² This summarily worded amendment would have represented an unprecedented expansion of the criminalisation of the conduct of senior managers of online platforms, introducing a blanket liability and possible jail time for senior managers found to have connived or engaged in misconduct that led to a failing in any children's safety duty. The Cates/Cash amendment attracted the support of a large number of backbenchers, many of them Boris Johnson supporters, and was supported by the Labour Party—meaning that the Sunak Government would have been certain to lose a vote on the amendment were this compromise emulating the Irish regime not agreed.

The forthcoming amendment, the wording of which is as yet undecided, is being rushed through without proper consultation and is bereft of the considered advice of the legal profession on the nature and purpose of such a sanction with regards to attaining children's safety objectives. The new legislation will patently fail to protect children if it is not consistent with the UK's existing criminal justice system. These updates will not amend the obligations that platforms will have towards children, and will not make platforms more likely to comply with those obligations.

More fundamentally, tech regulation is just one aspect of a wider societal responsibility towards children. Parents have a central role to play in the matter of their children's well-being, and their media consumption. That responsibility cannot be placed exclusively on online platforms, as the most extreme forms of criminal liability of tech executives would ensure. This is especially the case for children under the age of 13, the minimum age applied by many platforms. Children's wellbeing has become an even more urgent issue since the pandemic: YoungMinds reported that suicide rates among

¹ Statement made by Secretary of State Michelle Donelan, [Online Safety Update](#), 17 January 2023. The amendment will be "carefully designed to capture instances where senior managers, or those purporting to act in that capacity, have consented or connived in ignoring enforceable requirements, risking serious harm to children".

² [Miriam Cates, Make Big Tech managers personally liable for child safety breaches](#), 9 January 2023.

15-19 year olds rose 35% from 2020 to 2021.³ Yet resources to treat minors diagnosed with mental illnesses have lagged behind. These must be adequately funded to ensure vulnerable children are referred for the support they need.

The Government has also committed to making amendments that could make “posting videos of people crossing the channel which show that activity in a positive light” an offence—an extreme overreach and affront to free speech that goes against its claims that the OSB has been slimmed back to avoid criminalising otherwise legal behaviour.

The proposed amendment cites faulty precedents, including in financial services, and a new, not yet established Irish online safety regime that is lengthy in procedural steps before criminal sanction

Both the Government’s promised amendment and the Cates/Cash amendment cited financial services and Irish media regulation as important precedents for introducing liability for tech executives. The UK regime of criminalising the “reckless misconduct” of senior managers and directors of failed banks and building societies adopted in March 2016 is clearly not a precedent for the criminalisation of senior managers of platforms for online harms to children. It is designed to address “reckless misconduct in the management of a bank” by personnel of those banks that fail. It was introduced following the 2008-09 financial crisis, which included the failure of RBS, as part of the wider reform of the regulatory regime for banks.

The “reckless misconduct” concept is designed to alter the culture of banks from within, tilting the rewards away from risky behaviour, and to make bank managers and directors more aware of their regulatory responsibilities towards deposit holders, covered by deposit insurance of up to £85,000. But ‘recklessness’ is very difficult to prove, meaning that prosecution remains extremely unlikely. The measure does not address all failures of financial service institutions (notably not the collapse of Equitable in 2020, an insurance services provider). The operation of tech platforms and their ‘failure’ is not directly comparable to that of banks.

The newly adopted Irish regime is now cited directly as a guide to the forthcoming amendment of the Online Safety Bill in the Lords. Ireland’s Online Safety and Media Regulation Act (OSMR) was signed into law in December 2022. The passage of the Irish law is so recent as to make practical assessment of it impossible at this stage, with the country’s new Media Commission (Coimisiún na Meán, replacing the former Broadcasting Authority with a widened remit) only in the process of being formally established.⁴

Crucially, criminal liability acts only as a backstop in the case of the most extreme, provably intentional misconduct. This backstop is an additional measure to assure cooperation with regulators but *it is not the central mechanism in ensuring that children are kept safe online*; the main sanctions are fines and the powers to block noncompliant sites. In the case of Ireland there is an additional backstop to prevent over-application of criminal liability: punitive action could always be appealed to EU level. There is a possibility that such action, and criminal liability itself, could be entirely overturned if found to be disproportionate to the aims of the EU’s Digital Services Act (DSA), which does not introduce criminal liability. Ireland’s OSMR covers much of the same ground as the DSA, and establishes the Media Commission as Ireland’s national enforcer of the DSA, but as a Regulation the latter has direct force in all Member States and supersedes national law.

Any new amendment of the OSB must, at a minimum, retain the higher bar for action of the Irish regime versus the Cates/Cash amendment (though problems of practical enforcement even aside from proof of “connivance” that we anticipate in the UK regime, below, also apply in the Irish case).

³ Disability Rights UK, [Suicide rates record high amongst 15-19 year olds](#), 6 October 2022.

⁴ The Irish Government only announced its intention to appoint the Commission’s leadership on 17 January: [Minister Martin announces forthcoming appointment of Executive Chairperson and Commissioners in Coimisiún na Meán](#).

The introduction of criminal liability will not strengthen the safety objectives of the bill. It is at odds with the approach of the wider regulation, and is practically unworkable

The proposals for criminal liability are at odds with the regulation's approach as a whole, which, while far from perfect, has been tightened over the course of a long period of consultation into a more proportional, systems-based approach that tackles the kinds of harms to children that spread at scale (see [Online Safety Bill: Scaled back for an Act in 2023 \[2023-006\]](#)). Responsibly designed platforms with clear, age-differentiated policies have a role to play in ensuring that children are safe online, and external regulation and transparency is crucial given ample evidence of platforms' failings up to now.⁵ Regulation should establish new conduct to observe, and sanctions should be designed to ensure compliance with those standards—this is how the OSB is designed (Figure 1).

Figure 1: Children’s safety duties in the Online Safety Bill

Sites Included	All sites likely to be accessed by children Based on a self-assessment completed within three months of the legislation being put in place
Risk Assessment Duties	Submit “children’s risk assessment” to Ofcom three months after legislation in place, and before significant design changes
Safety Duties	User-to-user sites: prevent children from encountering priority harmful content; manage risks of other harm to children Search engines: minimise the risks of encountering content that is harmful to children
Age Verification Duties	Age assurance (either through age verification—checking ID—or a less watertight, AI-driven age estimation based on analysis of user behaviour)
Ofcom’s Powers	Ofcom can order services to use content moderation tech on content that is illegal or harmful to children Sanctions for non-compliance: fines of up to 10% of global turnover or blocking access to sites

[Source: Enders Analysis]

The introduction of criminal liability for executives is a dangerous simplification of the issues at play, and out of step with the mechanisms of the regulation as a whole. It wrongly suggests a direct, causal relationship between algorithmic recommendation of certain content and acts such as self-harm, and that the platforms are exclusively responsible for preventing such harm; when in fact there are many other sources of relevant responsibility. And in practical terms, it will not function as a disincentive for certain conduct.

Problems around enforcement of executives’ criminal liability ensure it will not work as a disincentive. There is, for one, the question of *who* should face prosecution. In the vast majority of safety failures, it would be extremely difficult to pin failures down to a single individual who had acted in a provably reckless way. Requirements and sanctions that are instead targeted at systems and companies, even if there are challenges around enforcement, are far more likely to have any practical effect. If an individual is to be held officially responsible, must that individual be based in the UK? Securing extradition would surely be unlikely. If they must be UK-based, this could be a disincentive to companies basing safety teams in the UK—which would hamper the cooperation with Ofcom that is essential to the success of the regime. Indeed, it is not even clear that safety teams, as opposed to product design teams, or higher leadership, would be scrutinised.

It remains to be seen how liability will interact with other duties: the safety duties relating to children are wide-ranging, and it is not at all clear that all non-compliance should be treated equally. One worrying aspect of this is that certain requirements for platforms are still not yet clearly outlined, with a lot to be determined by the content of Ofcom’s

⁵ A number of important “areas of concern” highlighted by the coroner in the Molly Russell case are targeted by the Online Safety Bill’s provisions: including a lack of separation and specificity on policies for adults and children, and a lack of age verification.

extensive codes of practice (see [Online Safety Bill: Taming the online ecosystem \[2022-027\]](#)). To threaten criminal liability when the regulatory regime is still so undefined is a mistake. One example of a lack of clarity is on age assurance. Platforms will be required to employ some form of age assurance to assess whether their sites are likely to be accessed by children, and whether they need to comply with children's safety duties generally. How this works in practice can range from the more extreme ID-verification (which raises privacy concerns) to AI-driven solutions, such as face scanning, that may not have been tested for efficacy or privacy-safety as extensively as would be necessary to enable them to be mandated for use. (The mandated scanning of encrypted private messaging under certain circumstances is another area where the Government risks putting the cart before the horse, with privacy-safe solutions not at the requisite stage of technological development, if not excluded on principle—see [Online Safety Bill: Scaled back for an Act in 2023 \[2023-006\]](#).)

About Enders Analysis

Enders Analysis is a research and advisory firm based in London. We specialise in media, entertainment, mobile and fixed telecoms, with a special focus on new technologies and media, covering all sides of the market, from consumers and leading companies to regulation. For more information go to www.endersanalysis.com or contact us at info@endersanalysis.com.

If your company is an Enders Analysis subscriber and you would like to receive our research directly to your inbox, let us know at www.endersanalysis.com/subscribers

Important notice: By accepting this research note, the recipient agrees to be bound by the following terms of use. This research note has been prepared by Enders Analysis Limited and published solely for guidance and general informational purposes. It may contain the personal opinions of research analysts based on research undertaken. This note has no regard to any specific recipient, including but not limited to any specific investment objectives, and should not be relied on by any recipient for investment or any other purposes. Enders Analysis Limited gives no undertaking to provide the recipient with access to any additional information or to update or keep current any information or opinions contained herein. The information and any opinions contained herein are based on sources believed to be reliable but the information relied on has not been independently verified. Enders Analysis Limited, its officers, employees and agents make no warranties or representations, express or implied, as to the accuracy or completeness of information and opinions contained herein and exclude all liability to the fullest extent permitted by law for any direct or indirect loss or damage or any other costs or expenses of any kind which may arise directly or indirectly out of the use of this note, including but not limited to anything caused by any viruses or any failures in computer transmission. The recipient hereby indemnifies Enders Analysis Limited, its officers, employees and agents and any entity which directly or indirectly controls, is controlled by, or is under direct or indirect common control with Enders Analysis Limited from time to time, against any direct or indirect loss or damage or any other costs or expenses of any kind which they may incur directly or indirectly as a result of the recipient's use of this note.

© 2023 Enders Analysis Limited. All rights reserved. No part of this note may be reproduced or distributed in any manner including, but not limited to, via the internet, without the prior permission of Enders Analysis Limited. If you have not received this note directly from Enders Analysis Limited, your receipt is unauthorised. Please return this note to Enders Analysis Limited immediately.