Ofcom Call for Evidence: first phase of online safety regulation

CBI response – September 2022

Context

As the country is gripped by a cost-of-living crisis, firms too are facing an uncertain economic environment, from major spikes in the cost of doing business to supply chain and labour market issues. It has never been more important to unlock investment to reignite a bold UK growth story. The government has the right ambition to create an environment conducive for business growth, building on the UK's strategic advantage in the digital economy. The UK already has a thriving digital economy that's worth over $1 trillion and creates a new unicorn company every 11.5 days.[1] But as firms continue to face challenges in the coming months, removing barriers and creating conditions for businesses in the UK's economy to invest and grow will be fundamental to stabilise the economy and improve living standards across the country.

Getting regulation right is a vital lever that government can pull to unlock economic growth. Proportionate, pro-innovation digital regulation will provide the certainty and confidence businesses need to invest. Businesses across the UK wholeheartedly back the ambition of the Online Safety Bill to make the UK the safest and best place to grow a digital business. But as the Bill moves through Parliament it is now crucial we get the detail right. With a suite of digital regulation changes in train (post-Brexit), from the Digital Markets Unit and Online Safety Bill to GDPR reform and AI governance, the eyes of the world are watching the UK's approach.

The CBI welcomes Ofcom's consultation. The proposed timelines have given industry some much-needed reassurance and certainty about Ofcom's approach to compliance, enforcement, and opportunities for stakeholder engagement. This is a brand-new regime and many businesses will be grappling for the first time to implement regulation of this nature; the CBI encourages Ofcom to adopt regular, gold standard consultation and industry engagement. The CBI stands ready to facilitate and support Ofcom's engagement with business across the economy, particularly during the Bill implementation phase. A participatory approach will enable Ofcom to keep pace with the fast-evolving nature of online safety and evolving technology to help ensure that businesses of all shapes, sizes and business models can effectively comply with the regulation. This document highlights two key recommendations and principles Ofcom should consider to support successful implementation of the regime – including codes of practice and guidance.

Over 25,000 organisations are in scope of the Online Safety Bill, from SMEs to retailers hosting online reviews and forums, with compliance costs estimated at almost £1.7bn.[2] Smaller businesses have limited capacity, nor have in-house legal teams to work through this complex legislation in detail, so clear guidance is vital to support compliance. Some businesses are currently considering the impact of the legislation, including the possibility of removing user to user services or shutting down online forums; the cost of one piece of legislation that is impacting the digital economy.

[1] https://www.information-age.com/uk-tech-sector-reaches-1-trillion-valuation-123499066/
[2] DCMS, Online Safety Bill Impact Assessment, 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf (Summary; Analysis and Evidence, Page 3).

1. **Ofcom should provide detailed and flexible guidelines to account for the range of business sizes and models in scope. This includes clear, proportionate definitions of both illegal and legal but harmful material, clear content take-down removal thresholds, and certainty that firms are not required to undertake general monitoring of their services.**

2. **Ofcom should develop a multi-year, multi-step implementation plan that accounts for the complexity of the bill, builds in domestic and international coordination and consistent stakeholder engagement.**

Ofcom should provide detailed and flexible guidelines to account for the range of business sizes and models in scope. This includes clear, proportionate definitions of both illegal and legal but harmful material, clear content take-down removal thresholds and certainty that firms are not required to undertake general monitoring of their services.

- Businesses wholeheartedly back the ambition of the Online Safety Bill to protect vulnerable people online and know they have a key role to play. The Bill currently requires all regulated user-to user services to ‘adapt the design of functionalities, algorithms and other features including taking down content to prevent individuals from encountering priority illegal content’. This includes using proactive technology for ‘content moderation such as image matching or behaviour identification technology’.

- The definitions of harm and thresholds for removal must be clear, proportionate and unambiguous so businesses have clarity on what content to remove including both illegal content and legal but harmful content. General monitoring is a redline for business as this would put the UK out of step with others internationally - this would represent a major departure from international legal norms and have significant impacts on privacy. For avoidance of doubt, Ofcom guidance must make clear distinctions between the proactive monitoring requirements of business to comply within the Bill, and general monitoring. Firms should not be required to undertake general monitoring of their services and Ofcom should provide guidance on how companies can fulfil their duty of care obligations without general monitoring.

Firms are already taking significant action and deploying a range of tools to moderate content

- Businesses are currently deploying a range of measures to tackle illegal content, from image and video hashing to automated scanning technologies to combat and remove CSEA (Child, Sexual Exploitation and Abuse). This reflects the vast range of business types and models that are tackling online harm as well as the different technologies and approaches that are being taken. For example:

    - Many businesses have robust terms and conditions that clearly state they do not allow illegal content on their services. Companies also support this by having existing measures in place to monitor illegal content on their platforms. Some companies use hash matching technology to connect to known databases containing CSEA material to detect and report any illegal material to the relevant authority as well as clear complaints functions for users to raise any concerns directly with the platform.

  - Third party groups are also being utilised by businesses to prevent illegal content such as the Internet Watch Foundation which has the capability to block content on online networks.

Guidance and codes of practice can set principles and guiding frameworks to help firms comply, which will also provide the necessary flexibility for firms to adapt compliance procedures to suit their business models

- As Ofcom undertakes its roadmap to regulation, guidance and codes of practice must reflect the broad spectrum of firms within scope and the activities they are already undertaking, providing clear guidance and actions that firms can take to comply. This is particularly important for SMEs who have limited resource to understand and navigate a complex regulatory landscape. Guidance and codes of practice must be flexible enough that firms can take steps to comply with the regulation for their particular business model, product or service.

- The CBI welcomes Ofcom's acknowledgement that there is no 'one-size-fits-all' approach to managing online risks. Flexible guidance can ensure that businesses are given clear insight into what best practice looks like and how companies can gauge whether they are meeting their requirements. It is vital that businesses are given flex to implement codes of practices depending on their own business model and size.

Ofcom's guidance can support firms to identify and tackle illegal content, balancing their requirements to proactively monitor priority illegal content without over-removal and impacting freedom of expression

- The Bill is not clear how to determine what content is illegal. In particular, firms are concerned about the specific requirements and thresholds that the Bill puts in place for firms to proactively monitor priority illegal content using proactive technology.
  This impacts a firms' ability to put the right system and processes – including automated solutions - in place. For example: the definition of priority illegal harms (Schedule 7) includes a list of 'content that amounts to an offence' such as 'assisting suicide', 'fraud', harassment, stalking and fear of provocation of violence'.

- Businesses have reported that some algorithms can effectively detect CSEA material, but automated systems struggle to detect content such as fraud and illegal immigration. Many of these harms currently have no legal definition and the threshold currently varies from company to company, offering an inconsistent user experience. Business will need certainty to understand what content will be illegal so they can take effective and appropriate action. The list of 'priority illegal harms' that all companies must remove should also remain focused in scope so that the most serious harms can be rightly prioritised by companies.

- The overall lack of clarity on content removal requirements collectively incentives companies to err on the side of caution when it comes down to content removal, to ensure that they are compliant. This potentially places the online experiences of vulernable individuals at risk of being unnecessary removed, as lived 'self-help' experiences such as recalling and documenting recovery from an eating disorder are often context dependent.

- The Bill in its existing form also includes new requirements around Ofcom imposing ‘best endeavours in relation to CSEA content’. Businesses have expressed concerns over the language of ‘best endeavours’, and the scope for this potentially giving a large potential remit for Ofcom’s actions, therefore clarity on what this will entail and consistent expectations from the regulator would be welcome. In addition, businesses have questioned the precedent this sets for enhanced regulatory powers related to regulatory reform and structures in other areas. Clear understandings of regulatory remit and powers will support business certainty and confidence to invest in the UK market.

Ofcom’s guidance can support firms to comply with their obligations on legal but harmful content whilst supporting freedom of speech and expression

- The Bill requires Category 1 providers (the larger highest-risk platforms) to have new obligations to protect adults from ‘legal but harmful’ content such as bullying and advocacy of self-harm. However, the Bill is not clear how to determine what content falls in this category. This impacts firms’ ability to comply and effectively put the right processes – including automated solutions – in place. To address this, Ofcom should include specific language in the codes of practice that reflects the Bill’s commitment to ensure over-removal of legal content is avoided as well as balancing users’ rights to freedom of expression.

Ofcom’s implementation guidance must reiterate that proactive monitoring must not be misconstrued with general monitoring

- Firms are concerned that lack of legal clarity in the Bill regarding proactive monitoring and proactive technology could result in it being misconstrued as general monitoring of all content online. General monitoring is a red line for business and would take the UK out of step will international legal norms in likeminded countries. Changing the fundamentals of internet governance is not proportionate and would represent a major departure from international legal norms, resulting in significant impacts on privacy.

- Ultimately, Ofcom should ensure that all draft codes and enforcement guidance are built on good regulation principles. These include having clear, proportionate definitions of harms and clear guidance on how to implement thresholds for content removal, so businesses know that the proactively monitoring requirement is not misconstrued as general monitoring of all content.

Ofcom should develop a multi-year, multi-step implementation plan that accounts for the complexity of the bill, builds in domestic and international coordination and consistent stakeholder engagement

- The CBI has supported Ofcom as the right regulator for the online safety regime, with expertise in related issues and widely respected as an independent body – both of which are critical for the successful enforcement of the online safety regime.

A multi-step implementation process is important to help empower firms to tackle the most pressing issues first

- Given its complexities, businesses would value a multi-step implementation process that allows them to show progress on resource-intensive obligations and reflects the differentiated reach and risk of online harm. For example, in line with the ambition of the Online Safety Bill to keep vulnerable people safe online, Ofcom’s codes of practice could set out which steps are more urgent than others to support companies (particularly start-ups and SMEs) who are dealing with the wide-ranging new regime. This would make a significant difference for product development and launches. Businesses should be directed to tackle the most serious harms first to support meaningful action. The Bill's impact could be diluted if businesses try to implement everything at once but are unable to do so effectively.

Creating a participatory and collaborative approach to implementation

- A participatory and collaborative approach to stakeholder engagement will be vital to ensure a successful implementation process. This includes Ofcom being well-resourced to field a potential range of questions in the Bill's implementation phase, especially amongst small businesses. Businesses have called for suitable lead times throughout the implementation process – including during categorisation - to allow time to implement changes within product and service development processes and updates. Firms welcome Ofcom's outlined approach to consultation and look forward to continuing to engage as the online safety regime is developed.

Engaging with other domestic and international regulators will support implementation

- Ofcom must continue to support the networks that allow it to quickly and effectively work with other regulators that cover connected aspects of the digital economy, including the ICO given the Bill's links with the Children's Code. Industry welcomed the creation of the DRCF (Digital Regulation Cooperation Forum) as a positive step forward for regulatory dialogue in the digital arena with the CMA, FCA, and ICO.

- Many of the 25,000 organisations in scope are operating across borders and facing a suite of digital regulation in multiple jurisdictions. Where possible, Ofcom's ability to engage and cooperate with regulators in other jurisdictions to support joint compliance across regimes, as well as operating on similar timescales and approaches to enforcement, will strengthen the UK's implementation regime and can provide an opportunity for UK regulatory leadership.

About the CBI

Across the UK, the CBI speaks on behalf of 190,000 businesses of all sizes and sectors. The CBI's corporate members together employ nearly 7 million people, about one third of private sector employees. With offices in the UK as well as representation in Washington, Brussels, Beijing and Delhi, the CBI communicates the British businesses voice around the world.