THE INTERNET COMMISSION

Policy briefing: Online Safety Bill and Digital Responsibility in the UK

Background:

- The UK's regulatory architecture around Digital Responsibility is being established by an Online Safety Bill, published in May[1]. It is based on the idea of a duty of care, a concept that has been well developed, especially through the work of Carnegie UK[2].
- Possible risks to freedom of expression from companies that are incentivized to err on the side of caution, and from the replication of the model in jurisdictions that have fewer checks and balances, mean that the approach is not universally liked[3].
- A joint committee of the House of Lords and House of Commons was appointed in July to scrutinise the bill, including pioneers of digital regulation Lord Timothy Clement-Jones, Damian Collins MP and Baroness Beeban Kidron[4].
- The DCMS committee also launched an inquiry[5], asking among other things whether the draft Bill is sufficiently focused on organisational systems and processes and safety by design, and about lessons from other jurisdictions.
- Government may introduce the bill by the end of April 2022, if it can respond to the committee by the end of February 2022. Allowing for a second reading this would mean that the bill might become law at the end of 2022.
- This policy briefing was prepared based on discussion at Internet Commission's UK Policy Roundtable, co-hosted with LSE Media and Communications[6] in July 2021

Key challenges:

1. Algorithmic accountability

The statutory regulator, Ofcom, could seek access to the algorithms used by organisations to promote and amplify online content, to test whether this is being done in a responsible way. Under the current proposal, advertising is unregulated, which is an inconsistency to be ironed out, as it would allow bad actors to continue to spread misinformation or other harmful content through paid content.

2. Harmful but not illegal

The most sensitive area of the debate may concern the scope of harmful but not illegal content. Organisations will be held to account by Ofcom for delivering on the terms of service that they themselves define. They will be expected to try to spot harmful content as effectively as they reasonably can and to take adequate action in response. It may be unreasonable to expect each and every piece of harmful content to be removed immediately, but organisations might fail in their duty of care if they actively promote harmful content, or if they fail to notice and stop amplification of harmful content on their platforms. In relation to adults' online safety, the proposed core duty is (1) for companies to state how they deal with harmful content, (2) to ensure that this information is clear and accessible to users, and (3) to consistently apply their approach. This approach may protect freedom of expression and allow ethical organisations to lead the way, including in tackling harms to society such as COVID disinformation.

3. Unintended consequences

There are potential unintended impacts of actions intended to prevent harm. For example, the use of filtering and blocking to create safe environments for children and young people might also risk limiting developmental opportunities for them online. And although the roll-out of end-to-end encryption is viewed by many as an essential component of open societies and markets, it may also hide criminal activity and present obstacles to law enforcement.

Important opportunities:

4. Codes of practice

Codes of practice are likely to be central to the new regime and will set expectations for services in scope. Ofcom will prepare specific codes relating to terrorism and child sexual exploitation and abuse. It will also propose one or more codes relating to: (1) safety duties for user-to-user services and search services; (2) duties about democratic importance; (3) duties about journalistic content; and (4) duties about user reporting and redress. These will likely be the subject of debate through the parliamentary process, especially as regards misinformation or disinformation and the concept of harms to society as opposed to harms to individuals. It is important to note that the bill gives organisations the flexibility to adopt alternative measures in line with their own risk assessments where that is the right thing to do: this may be helpful where codes remain undefined or where there are conflicts with the approaches in other jurisdictions.

[1] Draft Online Safety Bill: https://bit.ly/3CC2cFB

[2] Internet Commission, July 2019: "Policy primer, momentum across Europe for wide-ranging Internet regulation", http://inetco.org/reg

[3] Article 19, February 12th 2021: "Online harms: Duty of care would restrict free speech in the UK", https://bit.ly/3s5uwuV

[4] UK Parliament: Draft Online Safety Bill (Joint Committee), https://bit.ly/2VA1cRK

[5] UK Parliament: Digital, Culture, Media and Sport Sub-committee on Online Harms and Disinformation, https://bit.ly/2U7iB3p

[6] https://www.lse.ac.uk/media-and-communications

5. Anonymity

Anonymity may exacerbate bullying, harassment, and intimidation and facilitate online behaviours which are harmful to individuals and to democracy. It is an established feature of some online environments that can be problematic, but it may not be the root cause of much harm. It can also afford protection to minority voices such as LGBT+ communities and can therefore support diversity. But victims of abuse often find it hard to identify who is behind attacks so the police can act. Service providers will have to get better at dealing with abuse, or insist that people put their names to what they say. Verification of users could be a key step in building healthier online cultures, and a digital identity service may be an important enabler that the government could put in place.

6. Ethical business cultures

Ofcom regards improving the culture of the technology sector as central to its new role. Gathering evidence and shining a light on how effective company practices are, is likely to be one of Ofcom's biggest contributions in the first period of the regulatory regime. It sees organisational capacities and capabilities as critical, and does not underestimate the challenge of gathering the right information and applying the right skills and expertise to understand organisational systems and cultures. There may be a risk that competition rules deter companies from sharing information and cooperating on the protection of users. Specific guidance or, if necessary, exceptions to competition rules could facilitate cooperation on online safety, including seeking the views of children and young people.

Our view: **Business organisations are at the front line of digital responsibility** because they operate the Internet and have the capacity to act. They should be encouraged to take the lead and differentiate themselves through digital responsibility and positive social impact, enabled by ethical business cultures.

New approaches to evidence and oversight will be needed to navigate legitimate commercial confidentiality and significant information asymmetry. We envisage a role for trusted brokers, independent of business and government, that can support smart regulation and help organisations to demonstrate digital responsibility across multiple jurisdictions.

International and multi-stakeholder collaboration is vital to foster trust, safety and freedom online. It should focus on understanding how everyday harms are driven by the Internet's complex strategies, systems and processes, and seek to reveal how these drivers result in the symptoms people experience.

Key challenges include algorithmic accountability, the treatment of online content deemed harmful but not illegal, and the potential unintended consequences of filtering and encryption technologies.

Important opportunities include codes of practice, digital identity, and ethical business cultures.

About the Internet Commission:

- **Inside view:** we tackle knowledge asymmetry with insights into organisational culture, strategies, systems and processes, that complement research on user and citizen experiences in the online environment.
- **Cross jurisdiction:** seeking the common ground across jurisdictions may be important for organisations even within areas like the EU, where rules may be more harmonised but definitions of illegal content remain nationally defined.
- **Independence:** we seek to collaborate with business, governments, academia and civil society whilst remaining independent and guided by our mission to advance digital responsibility.
- **Inspiring ethical practice:** sharing knowledge between organisations can support smart regulation by helping to identify and embed best practices and foster purpose-driven and ethical business cultures.
- **On the front foot:** organisations work with us to engage collaboratively with policy makers, get ahead of emerging regulatory trends, and prepare operationally for future requirement.

As an independent, trusted broker within the new regulatory system, the Internet Commission aims to ask the right questions, provide reliable evidence and help organisations to navigate different national and international requirements. It offers independent health check, knowledge sharing and review services to organisations that lead in digital responsibility, and authoritative insight to regulators and other stakeholders. Its evaluation framework and process enable organisations to demonstrate progress in tackling problems such as illegal content, hate speech, cyberbullying and misinformation. The Internet Commission is supported by visionary private and public institutions including Arm, Bates Wells, LSE, Oracle and Wayra. Since 2018 it has engaged widely with Internet companies, content moderation practitioners, academic experts, NGOs and regulators. The Internet Commission is a trading name of Digital Responsibility Network Ltd, a non-profit Company Limited by Guarantee and registered in England and Wales number 11399296.

For more information:

Jonny Shipp	jonny.shipp@inetco.org	+32 488 67 48 78
Dr Ioanna Noula	ioanna.noula@inetco.org	+44 7847 095559
Juraj Kosturik	juraj.kosturik@inetco.org	+55 11 95080 6814
Baran Osmanoglu	baran.osmanoglu@inetco.org	+33 637 17 21 13