Written evidence submitted by techUK (OSB17)

Written response to Public Bill Committee on Online Safety Bill

Introduction:

techUK and its members are committed to online safety and want to create safer online experiences for the whole of society. We welcome the Online Safety Bill and firmly support the objectives to make the UK the safest place to go online while upholding free speech and supporting innovation.

For several years, Parliamentarians, officials and a broad range of stakeholders have been debating and discussing at a theoretical level how to create safer online spaces. The passage of the Online Safety Bill through second reading to Committee stage marks a significant step forward in the practical realisation of the Government's vision.

Overall, we support the proportionate approach of the Bill which relies on systems and processes and remains risk-based, as well as the appointment of Ofcom as the specialist regulator. However, as we will go on to discuss, some of the key elements of the regime remain vague.

This poses a challenge for in-scope companies and the regulator to assess the full extent and workability of the proposed framework**.** For example: key definitions of harmful content are left to secondary legislation; the Secretary of State has wide-reaching powers to significantly amend the regime which may interfere with Ofcom's independence; business-to-business services do not have clarity on the face of the Bill that they are exempt from duties; and in-scope services are potentially subject to conflicting laws across regions around intermediary liability.

These are all fundamental parts of the regime which will need to be clarified or amended to enable the 25,000 services in scope and Ofcom to fully inform the legislative processes, and then begin preparing for the legislation in a confident and coherent way.

The ultimate test of this legislation will be whether it provides clear guidelines to enable in-scope companies and the regulator to make effective decisions which meet the stated policy objectives and, in turn, result in protections of free speech and a reduction in levels of harm experienced by individuals. If the legislation fails to meet this goal, it will likely give rise to levels of ambiguity which may lead to ineffective action and risk significant damage to fundamental user rights, freedom of expression and privacy. It would also place a significant burden on smaller businesses who are looking to innovate and grow in UK markets.

We ask the Committee to think pragmatically about this legislation considering the diversity of 25,000 companies in scope and the possible detrimental impact of an unclear framework on both the safety of society and tech innovation.

Setting scene: the UK's Plan for Digital Regulation

The Online Safety Bill is one form of digital regulation that will impact the UK's diverse tech sector. Its provisions overlap with the Age-Appropriate Design Code (AADC) which came into force in September 2021. It will supersede the Video-sharing Platform (VSP) regime which is currently being formed and it will involve many of the same companies who are expected to benefit from the UK's new pro-competition Bill announced in the Queen's speech.

In addition, there are a range of other consultations and strategies being formed over the next few months including the Innovation Strategy, Digital Strategy, National Data Strategy and Online Advertising Programme.[1]

Amidst the range of regulatory initiatives, there is a need to form a balanced and workable online safety framework which delivers on the objectives while supporting innovation and investment in the UK economy, especially by smaller businesses.

The Online Safety Bill cannot be viewed in isolation and it is important that the FCA, CMA, Ofcom and ICO continue working together through the Digital Regulation Cooperation Forum (DRCF) which was set up in July 2020 to facilitate regulatory coordination in digital markets, and cooperation in areas of mutual importance.[2] We welcome the DRCF acknowledgement of the potential disproportionate costs of the Online Safety Bill on smaller businesses and the ongoing tensions with competition policy.[3] To prevent smaller businesses from being overburdened, DRCF regulators need to have enough independence to make proportionate and balanced decisions.

Separately, we are pleased to see the Government acknowledge the need for better regulatory coordination through the DCMS Plan for Digital Regulation. The Plan was published in July 2021[4] and sets out the government's objectives for innovation-enabling regulation with three key principles for policymakers to follow when crafting digital regulation: 1) actively promote innovation 2) achieve forward-looking and coherent outcomes 3) exploit opportunities and address challenges in the international arena.

Overall, as we will go on to discuss in this written response, there are certain provisions in the Online Safety Bill such as the Secretary of State Powers that do not support the independence of Ofcom, have the potential to undermine long standing principles against general monitoring and stifle innovation for smaller businesses which would appear to be contrary to the aims of the Plan for Digital Regulation.

techUK would like to see the Committee ensure that the Online Safety Bill leads the way in promoting innovation-enabling regulation for the thousands of in-scope digital businesses, while supporting Ofcom to understand their duties around decision-making.

---

[1] DCMS Plan for Digital Regulation, Annex: timeline of upcoming digital regulation activity
[2] Digital Regulation Cooperation Forum, March 2021
[3] Online safety bill risks stifling start-ups, says UK tech regulator chief, Financial Times, April 2022
[4] DCMS Plan for Digital Regulation: Driving growth and unlocking innovation, July 2021

Summary of techUK response:

techUK's response will focus on 5 key areas which we would like the Committee to consider as they analyse the Bill line by line, before concluding with some suggested amendments.

- Secondary legislation and 'legal but harmful'
- Powers of the Secretary of State and Ofcom's independence
- Senior Management Liability
- General monitoring and international norms
- Business-to-business services

Secondary legislation and legal but harmful:

Listing the types of priority illegal content offences on the face of the final Online Safety Bill is a welcome development and something techUK has long called for. Some of these requirements however still need further development. For example, the new offence of cyberflashing should be adjusted so it is consent-based, rather than intent-based. This would provide greater clarity for enforcement and offer better protection for women against receiving unwanted sexual imagery.

Despite these improvements to put illegal content offences on the face of the Bill, the legislation still relies significantly on secondary legislation, with no clear timelines on when these decisions will be made, and fails to provide the level of clarity that businesses need to prepare for and comply with the regime. For example, as currently drafted, the Online Safety Bill does not provide any certainty on the types of content that will be designated as considered harmful towards adults and children under the Bill.

Tech companies in techUK's membership are committed to enhancing user safety and protecting free speech. However, there is very limited guidance in the Online Safety Bill itself to help companies balance and make judgements where safety duties may cut across other user rights, for example on privacy rights, freedom of expression, or requirements in the Bill to give special importance to certain types of content.

As with many aspects of the Bill being left to secondary legislation, it remains unclear whether the codes of practice, to be published by Ofcom, will specify exactly how services are expected to balance these competing duties.

We note that the DRCF in its 2022-23 workplan says it will publish a joint statement on how its regulators plan to work together to address areas of interaction between the online safety and privacy regimes as well as developing a clear articulation of the relationships between competition and online safety policy. However, these statements are not given clear timelines and it is not clear how they will relate to Ofcom's codes of practice.

Some of our members are concerned about the safety duties in respect of legal but harmful content and how they create a requirement for providers to use systems and processes in a way that could prevent access to a wide range of lawful content. The inability of providers to understand their obligations has the potential to push services into designing systems in a way that removes legitimate and lawful "grey area" content, seeing this as the safer route to compliance.

To help create safer online spaces – while avoiding forms of censorship becoming the norm in democratic societies – the primary legislation must outline all the types of harmful content which will be in scope with codes of practice providing descriptions of the types of content which should be interpreted as harmful or not harmful towards adults or children.

In addition, an evidence-led and democratic process is needed to identify future harms, as well as to evaluate the levels of risk associated with existing harms and whether they should remain in scope. This could involve setting up an independent committee responsible for assessing evidence for new harms as they emerge and seeking democratic approval for whether they should be included in scope. Any such assessment must also review the potential implications on freedom of expression and other rights, while also seeking to identify when activity no longer presents a high risk of harm due to changes in systems and user experiences. As the regulator Ofcom should have a clear role in gathering and providing evidenced recommendations, as it does around, for example, offensive language on TV and radio[5]

Overall, leaving fundamental decisions around definitions and codes to secondary legislation delays clarity and certainty on an essential part of the regime which will impact the confidence of the range of companies in scope when thinking about the systems and processes which they will need to put in place. Placing the onus on companies to decide what is and is not acceptable online has the potential to create unequal standards, interrupt technological innovation and undermine democratic process and individual rights.

techUK calls for further clarity on the face of the Bill about the content that is to be considered harmful towards adults and children. We acknowledge the need for the regulation to adapt to future activity and recommend that there should be a democratic mechanism to update definitions and types of harms as they develop, either through an independent committee or Parliament.

Powers of the Secretary of State and Ofcom's independence:

Throughout the final Online Safety Bill there are several clauses which allow the Secretary of State to amend the provisions of the regulation. These amendment powers are in addition to the responsibilities of the Secretary of State to consult Parliament before setting out a list of strategic online safety priorities (Part 9, Clause 144) and to give direction to Ofcom (Part 9, clause 145 and 146) which we consider more technical powers.

There are short-term concerns about some of the technical powers, including delays about when Ofcom and in-scope services can start preparing for the regime. However, our broader

concern around the powers of the Secretary of State relates to the amendment powers and how they will be used by current and future governments.

There are two main clauses which we have identified in the text to be problematic in relation to the **amendment powers** of the Secretary of State:

- **Part 3, Clause 40 (codes of practice and public policy)** – The Secretary of State has the powers to require Ofcom to modify codes of practice 'for reasons of public policy'. Once Ofcom has made changes, the Secretary of State can direct Ofcom to make further modifications until the Secretary of State is content.
- **Part 7, Clause 80 (categorisation and threshold conditions)** – The Secretary of State holds the powers to define and change the threshold conditions between categories of companies, following guidance from Ofcom.

The far-reaching amendment powers of the Secretary of State have the potential to fundamentally change the underlying parameters of the Bill which could undermine efforts which companies of all sizes are looking to invest in their systems to confidently comply with the law. For example, the lack of clarity around the definition of 'public policy' coupled with limited checks and balances on how this power may be used opens the regime to significant change that has the potential to be politically motivated.

Furthermore, allowing the Secretary of State to retain the power to change the threshold conditions between categories following guidance from Ofcom could result in companies arbitrarily moving between categories. The lack of certainty around the transition between categories is particularly concerning for thousands of smaller and lower risk tech businesses who are already considering the need to divert existing resource away from other parts of their businesses to comply with the regime. These companies may not be able to continue innovating and growing if they are moved to category 1 where the obligations are vast and have been designed with larger companies in mind.

Overall, we welcome the choice of Ofcom as the regulator for this regime given its experience and proportionate approach to regulation in other sectors. The expansive amendment powers of the Secretary of State have the potential to damage Ofcom's independence and should be removed to enable Ofcom to make decisions that are risk based and proportionate to levels of harm and types of companies.

techUK and its members understand the need for the regulatory regime to change with the times but providing these powers to the Secretary of State is problematic. They could have adverse impacts on both the efficacy of the regime and Ofcom's enforcement.

techUK urges the Committee to amend the Bill to remove the powers of the Secretary of State to modify Ofcom's codes to align with 'public policy' and to remove the Secretary of State's decision-making powers around the thresholds between categories.

Senior Management Liability:

Although considered as a last resort, the proposal to include criminal sanctions for senior managers as soon as the regime comes into force risks having a chilling effect on smaller

companies and investment in the UK digital economy. This would be a poor outcome and conflict with the Government's broader goal for the digital economy set out in many strategies and the Digital Regulation Plan.

Furthermore, it is unclear whether these provisions are necessary for the Online Safety Bill to achieve its objectives and – coupled with the lack of clarity around types of harmful content in scope – could result in significant unintended consequences for free speech. As outlined in the section on secondary legislation and legal but harmful definitions, in-scope services may feel that the easy route to avoid criminal liability is over-removal of content from their sites.

techUK asks the Committee to support Ofcom to have a bias towards promoting and supporting compliance and reserve criminal sanctions for cases of non-compliance with information requests or repeated failures to address a systemic issue.

General monitoring and international norms:

As drafted, the Bill imposes several duties that suggest providers will be required to undertake general and proactive monitoring of content on their services. For example, the child safety obligations outlined in Part 3, clause 11 poses a duty on user-to-user services to use proportionate systems and processes designed to prevent children from encountering "primary priority content" and to protect them from other "content that is harmful to children". These duties therefore apply to, and require service providers to proactively identify, a very broad range of content which could amount to a general monitoring obligation.

Further this type of proactive algorithmic review is also not technically possible for all types of harmful content, particularly those that require a contextual analysis in order to ascertain whether the content is illegal or harmful, or entirely legitimate.

In addition to the child safety duties, Part 7 clause 116 of the Bill grants Ofcom powers to mandate the use of proactive technologies for both illegal and harmful content towards children. This would apply to all in-scope services that can be accessed by children and is a significant shift in approach from existing targeted monitoring that is focused on illegal content. This could result in general monitoring either through the types of technologies that Ofcom is issuing or as a de facto reality for businesses looking to ensure that they are not issued with a technology notice from the regulator.

The risks with general monitoring are well-known: it encroaches on fundamental rights and freedoms, tilting the balance between protecting users from harm and protecting their freedom of expression toward more restriction of legitimate speech, leading to over-removal of legitimate content. General monitoring directly contradicts established international norms in this area and given the breadth of content in scope of the Bill, is unlikely to be achievable at scale with any degree of accuracy given the limitations on automated tools.

We understand that it is not the Government's policy intention to override existing intermediary liability protections including prohibitions on general monitoring that are laid out in Article 15 of the eCommerce Directive. Derogating from this principle has the potential to add to the regulatory complexity of the Bill and many tech businesses will find themselves in a position

where they are required to comply with competing and conflicting laws across regions which may not be technically feasible. Many smaller businesses will struggle to absorb the significant additional cost of implementing general monitoring which would necessarily include both technology and human oversight. This risks making the UK a less attractive place for tech growth and investment which does not align with the Government's vision for a strong digital economy.

techUK asks the Committee to amend the text to increase certainty around the Government's policy intent and make it explicit that general monitoring obligations are not an obligation for businesses to comply with the Bill.

Business to business exemptions:

The Government has stated publicly that Business-to-Business services will be out of scope of the Online Safety Bill.[6] However, the Online Safety Bill does not deliver on this exemption when put into legal practice.

The explanatory notes provide some indication of how the Government's policy intention might be delivered with B2B services being considered as access facilities. However, they do not have legal force. To remove any doubt that B2B services fall outside of scope while ensuring that the Government's policy intention has legal force, there should be an explicit exemption for B2B products and services inserted into the Bill.

Our understanding of the Government's current position is that there is indeed a clear policy intention of this kind, but that there is no need for an explicit exemption for B2B services as a class on the face of the Bill as they are not in scope in the first place. Effectively, that the policy intention can be achieved without change to the Bill. We question the accuracy of this view.

Moreover, if the Government does have the broad policy intention of excluding B2B services, it is unclear why the burden of achieving that result should fall on a couple of highly technical exceptions, which are likely to produce arbitrarily different results depending on detailed technical and other features of a service and which by their technical nature may give rise to unforeseen gaps.

To address the legal uncertainty around the policy intention of B2B exemptions, techUK would encourage the Committee to review the definition of user-to-user service outlined in Clause 2. As currently drafted, nothing in the definition stipulates any limitation on the purpose for which a user makes use of the service. The definition is on the face of it wide enough to cover a corporate or individual user making use of the service for business purposes.

Amending the text of the definition would be entirely consistent with other statutes or statutory instruments which provide for exemptions where an activity or service is provided for the purposes of a business. Such examples can be found predominantly in statutes relating to financial services, including the Consumer Credit Act (1974), the Consumer Credit (Agreements) Regulations 2010/1014 and the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) (No. 2) Order 2013/1881.

[6] OHWP reference to be inserted

techUK urges the Committee to amend the definition of user-to-user services as the most obvious way to achieve the Government's policy intention for a general B2B exception written into Clause 2 of the Bill. This would be consistent with the Draft Bill which provided more certainty about the B2B exemptions than the current version.

END

Proposed amendments:

Amendment one - Increase Certainty Regarding General Monitoring Requirements

Part 2 – Clause 7 scope of duties (new text in red)

Nothing in this [Act] shall be construed as:

a. an imposition of a general monitoring obligation.

Amendment two – clarify definitions of user-to-user services

We suggest that the Committee puts forward amendments to the Bill as follows (note new text shown in red):

Section 2 – Meaning of "user-to-user service" and "search service"

(1) In this Act "user-to-user service" means an internet service by means of which content that is generated by a user of the service or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service, other than an internet service provided to an entity or individual primarily in connection with or for the purpose of their business.

(2) For the purposes of subsection (1)—

(a) it does not matter if content is actually shared with another user or users as long as a service has a functionality that allows such sharing;
(b) it does not matter what proportion of content on a service is content described in that subsection.

(3) For the meaning of "content" and "encounter", see section 189.

(4) In this Act "search service" means an internet service that is, or includes, a search engine (see section 183).

(5) Subsections (6) and (7) have effect to determine whether an internet service

that—
(a) is of a kind described in subsection (1), and
(b) includes a search engine,
is a user-to-user service or a search service for the purposes of this Act.

(6) It is a search service if the only content described in subsection (1) that is enabled by the service is content of any of the following kinds—

(a) content mentioned in paragraph 1, 2 or 3 of Schedule 1 (emails, SMS and MMS messages, one-to-one live aural communications) and related identifying content;
(b) content arising in connection with any of the activities described in paragraph 4(1) of Schedule 1 (comments etc on provider content);
(c) content present on a part of the service in relation to which the conditions in paragraph 7(2) of Schedule 1 are met (internal business service conditions).

(7) Otherwise, it is a user-to-user service.

May 2022