Written evidence submitted by the Coalition for a Digital Economy (Coadec)

DCMS SUB-COMMITTEE ON ONLINE HARMS AND DISINFORMATION - ONLINE SAFETY AND ONLINE HARMS INQUIRY
RESPONSE FROM THE COALITION FOR A DIGITAL ECONOMY (COADEC)

About Coadec

I. The Coalition for a Digital Economy (Coadec) is the policy voice of UK tech startups and scaleups in Westminster and Whitehall. Since 2010, we have worked to engage on behalf of tech startups in public policy debates in the UK across a range of priority issues for startups including access to finance, immigration and skills, and technology regulation. We work directly with the Government across a range of issues; our Executive Director sits on the Digital Economy Council, Telecoms and Tech Trade Advisory Group, and the Jet Zero Council.

Coadec's view of the Draft Online Safety Bill

II. Coadec and its community welcomes the attempt to create a framework to improve safety online. However, the approach put forward in the Draft Online Safety Bill is too wide-ranging, convoluted, unclear and will damage the UK's position as a leading digital economy. Additionally, it is impossible to properly evaluate the effectiveness of the proposed regime while existing uncertainties remain around what content is in scope and what services are in scope. These uncertainties mean that the current framework is both impossible to effectively implement and impossible for businesses to effectively comply. If passed in its current form, the BIll will harm digital innovation in the UK.

Key points

III. The Bill must include an explicit definition of harm. There are obvious difficulties in achieving this but current proposals are subjective, and leave it to service providers to make the ultimate determination whether something is harmful or not. Instead the Bill should set out specific and defined requirements for content removal with this only applying to illegal content.

IV. It is welcome that the Draft Bill has included a level of service differentiation through the creation of category 1, 2A and 2B designations. It is right that there is a tiered approach to ensure that higher risk services face proportionate regulatory burdens. It is important that specific criteria for categorisation, and the powers of the Secretary of State are clearly set out in the final Bill to provide certainty for businesses.

V. The categorisation framework is still too broad, and should be further separated. As the Draft Bill stands, there is little difference between what is required of category 1 and category 2B services and the Draft Bill captures any service of any size which facilitates user interaction, not just social media. This will have a chilling effect on competition in digital markets and on the willingness of entrepreneurs to found businesses that may be in scope of the online safety regime. This will, in turn, protect the incumbents. The framework should reduce the burden on smaller services that pose little risk. Additionally, the framework should bring forward strict exemptions for startups to avoid having a negative impact on innovation and competition.

VI. Requiring platforms to determine the appropriate 'proportionate systems and processes' to minimise priority content is the correct decision. It is not practicable to adopt a one-size-fits-all approach and, if this were the case, it would again benefit large incumbents with greater resources and would put startups at a disadvantage. If the final Bill were to mandate the use of specific technologies it would make the UK a more expensive place to do business, making it less attractive to new investment on the international stage and hamstringing the UK's world-class digital economy.

VII. There remain a significant number of contradictions within the Draft Bill. At its heart, the framework requires services to monitor and moderate all content, but with express carve-outs for journalistic and democratically important content alongside freedom of expression obligations. This is unworkable and could be avoided by reducing the scope of the final Bill. The carve-out for business-to-business (B2B) services is unclear, is open to interpretation and is likely to bring in scope a number of B2B services which would be expected to be exempt. This section of the Bill needs redrafting to more effectively determine which B2B services are in scope.

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

VIII. The change in focus from 'online harms' to 'online safety' in the Government's Draft Bill, as compared to the approach originally taken in the April 2019 Online Harms White Paper, was a necessary shift.

IX. The ambition and scope of the Draft Online Safety Bill means that service providers will be required, by law, to process, monitor, assess and moderate the interaction between users online. This is expansive and is only possibly achievable by having services adopt specialised processes which minimise the spread of specified content without creating a general monitoring obligation. This is especially important given the vast amount of content that is currently in scope of the Draft Bill. This will require processes that can be run at sufficient scale: many services deal with multiple billions of pieces of content per day. The only way for this to be managed is if the use of a process-driven approach, rather than a case-by-case approach.

X. In contrast, taking an 'online harms' approach would see services judge content on a case-by-case basis, working backwards to remove content that may have been subjectively deemed to be harmful. Such an approach would focus on the wrong things, placing an emphasis on individual occurrences, rather than encouraging platforms to invest in systems that promote safety.

XI. In moving towards encouraging the use of systems and processes to reduce the risk of harm, the Draft Bill has taken a step in the right direction. However, without workable definitions of harm (described below) it remains unclear what such systems will be required to achieve, and this means they will be impossible to design and implement.

Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

XII. The Draft Bill fails to properly define content which is legal but harmful to children or to adults. The Draft Bill currently places the responsibility for making this determination on to service providers. This creates an unworkable and uneven playing field between services and for users. Different services, each with unique functionalities, will ultimately adopt different standards for what content is harmful and what is

acceptable on their platforms. There are obvious difficulties in setting out a definition of harm, and in recognition of this the approach set out in the Draft Bill represents the Government's third attempt at a workable definition.

XIII. The definition set out within the Draft Bill requires that service providers set out their own subjective assessments of 'a significant adverse physical or psychological impact' for an adult, or a child, with 'ordinary sensibilities'. Subjective assessments means that different platforms will implement the new rules in different ways. This represents a serious problem for implementation, especially given the sensitivities involved. This makes the latest attempt at defining harm a clear step backwards from the initial categories of defined harms which were floated in the original White Paper.[1] This approach also further entrenches the position of large incumbents, with startups far less able to dedicate resources to consider these issues and make these determinations.

XIV. There are distinct risks to pressing ahead with such an approach. For example this could give rise to: a) overregulation of content on some platforms leading to the censoring of acceptable content, including content which is protected by the Draft Bill such as journalistic content or content of democratic importance and; b) potential legal action by service providers who find themselves unable to enforce the rules properly and by users who have their content taken down.

XV. In order to be workable the Bill needs to set out, in explicit terms, which content is and is not acceptable. The easiest way to go about this would be to adopt a narrow and accepted definition which is not subjective or open to interpretation. The only workable definition of harm is therefore likely to be content which is already clearly defined as illegal.

Does the Draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

XVI. The Draft Bill is right to let services determine their own 'proportionate systems and processes' to minimise the presence of content, to minimise how long that content is present and to minimise the dissemination of such content. Different services function in different ways, processing varying amounts and types of content and with different user bases. For this reason it is not practicable to create and enforce a one-size-fits-all approach or to be prescriptive in setting out the specific measures a service should implement.

XVII. Implementing new technology to improve safety is expensive and very often creates its own risk by overlaying new layers onto products, requiring the collection of new data, or the involvement of a third party. There is a risk that mandating specific safety measures could be detrimental to competition, in particular damaging SMEs. SMEs, in complying with new safety requirements, are likely to pay disproportionately more to align themselves with measures designed for bigger services for whom such features are more appropriate.

XVIII. Recent research, commissioned by the Department for Digital, Culture, Media and Sport and completed by EY, looked at the measures that platforms with video-sharing capabilities take to protect users from harmful content online. The report found that smaller companies were spending over £45 per user compared to the biggest platforms which spent £0.25-50 per user.[2] This suggests that compliance costs are

1. 'Online Harms White Paper', Department for Digital, Culture, Media and Sport, April 2019

2. 'Understanding how platforms with video-sharing capabilities protect users from harmful content online', EY, August 2021

likely to be seriously difficult, if not impossible, to meet for SMEs. This could reduce competition in the market, and could dissuade new business creation in the UK's digital economy.

XIX. The Draft Online Safety Bill's Impact Assessment fails to consider the impact on startups. It notes that 'It is unclear what percentage of businesses would be required to adopt age assurance measures or what kind of systems they would employ'. It also pointed to the lack of clarity around the cost of implementing such technology.[3] Additionally, the Impact Assessment failed to describe the transition costs for small businesses on a cost-per-user, or as a percentage of revenue, while at the same time noting that 81% percent of in-scope businesses are likely to be microbusinesses. This oversight is likely to mean that the proposed framework could have a significant and disproportionately negative financial impact on startups with key metrics overlooked in the Impact Assessment.

XX. There have been growing calls to mandate the use of age assurance and age verification technologies, something which is currently not required in the Draft Bill. Requiring the use of such technologies on such a large scale is unproven. It could also only occur at significant cost, particularly to startups companies operating in the online space and would create a barrier to conducting operations in the UK. Collecting, verifying and storing sensitive user information creates significant risk for user privacy and security.

XXI. There is a risk that, in mandating the implementation of new technologies, the Bill could place substantial financial obstacles to the emergence of new market entrants, further entrenching the bigger, higher risk, companies and severely limiting competition. Further, these requirements will make the UK a more expensive place to do business, making it less attractive to new investment on the international stage and hamstringing the UK's world-class digital economy.

Are there any contested inclusions, tensions or contradictions in the Draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

XXII. There are substantial contradictions throughout the Bill. In-scope services are required both to monitor and moderate content, but to do so with express carve-outs for certain categories of content such as journalism and content of democratic importance. At the same time the Draft Bill requires platforms to have a 'duty to protect rights to freedom of expression and privacy'. Such an approach is contradictory and unworkable, as what may be considered freedom of expression by one individual, may be considered harmful to or by another.

XXIII. There are other fundamental issues which the Bill must address. Firstly, the issue of service categorisation. The inclusion of Category 1, 2A and 2B designations within the Draft Bill is a step in the right direction and rightly acknowledges a different approach is needed for companies of a different size. However, despite these categories, the Draft Bill fails to set out a solid set of thresholds to determine categorisation, instead passing this power to the Secretary of State and Ofcom to decide upon at a later date. Additionally, it is possible for startups to move between category designations at short notice as they expand, this is again potentially damaging for competition as it acts as a disincentive to grow.

XXIV. It is impossible to judge the appropriateness, effectiveness and the proportionality of measures set out within the Draft Bill, particularly when it is unclear what size of business will be brought under either the Category 1 or Category 2 umbrellas. For this reason strict criteria setting out thresholds for users and

3. 'The Online Safety Bill, Impact Assessment', Department for Digital, Culture, Media and Sport, April 2021

functionalities should be included when the final Bill is published. Additionally, startup businesses should be given special recognition and be excluded from categorisation in order to avoid a negative impact on competition and innovation.

XXV. While it is right that the Draft Bill seeks to create exemptions for business-to-business services through its 'internal business services' carve-out, the framework needs to provide more clarity. As it stands this section of the Bill is unclear, is open to interpretation and is likely to bring in scope a number of B2B services which would be expected to be exempt. This section of the Bill needs redrafting to more effectively determine which B2B services are in scope.

What are the lessons that the Government should learn when directly comparing the Draft Bill to existing and proposed legislation around the world?

XXVI. There are lessons that can be learned from international experience with other countries having already implemented similar legislation. Many of the frameworks being pursued internationally offer far more clarity on content which is to be regulated and which companies are to be in scope, and typically achieve this by setting out specific categories of unacceptable content.

XXVII. On defining harmful content, a number of countries have opted for tighter, more enforceable definitions. This is the case, for example, in the German NetzDG approach, where content is clearly in-scope if it is illegal.[4] This approach is echoed in the European Union's Digital Services Act (DSA) which focuses primarily again on illegal content, with much less prescriptive rules for harmful content.[5] Other approaches such as in Australia's Online Safety Bill or Ireland's Online Safety and Media Regulations Bill more closely mirror the UK, but have clearer categories for in scope content, such as the sharing of intimate images without consent or material promoting self harm.[6] [7] Strict definitions of in-scope content, particularly making rules apply only to illegal content, or clearer content categorisation, can make online safety legislation more enforceable allowing businesses to effectively comply.

XXVIII. On setting out which companies are in scope, other nations have offered more clarity than the UK. For example, in Germany services are only in scope if there are more than two million registered users in the country. In the EU's DSA, only platforms with 45 million monthly users face the most stringent regulations. The DSA also goes further, setting out specific requirements for different types of platform and it differentiates between intermediary services, hosting services, online platform services and very large online platforms. This is a tiered approach which the UK should look to adopt to make sure that firms have an appropriate level of regulation according to their size and risk, such as category 1 inclusion being limited only to the largest services with a statutory minimum number of users.

---

[4] Network Enforcement Act, Bundesministerium der Justiz und für Verbraucherschutz, July 2017

[5] Digital Services Act, European Commission, December 2020

[6] Online Safety Bill 2021, The Parliament of the Commonwealth of Australia, July 2021

[7] 'Online Safety and Media Regulation Bill', Gov.ie, January 2020