Written evidence submitted by techUK (OSB98)

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 Draft 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 publication of the Draft Online Safety Bill in May 2021 marked a significant step forward in the practical realisation of the Government's vision. It provides some clarity on exempt services listed in Schedule 1 while confirming the focus on user-generated content and related systems and processes that address harms. The Draft Bill also shows clear political intent to protect news journalism and free speech. Its publication has enabled civil society, tech companies, stakeholders, and Parliamentarians to get some new detail and begin to understand how the regime might work in practice.

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: the types of harms in scope and their prevalence are yet to be defined; the thresholds to assign companies to categories are not finalised; the potential number of codes of practice are unknown; and there is no clear picture about how free speech and harmful content will be balanced. These are all fundamental parts of the regime which will need to be clarified to enable the 24,000 businesses 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 companies in scope and the possible detrimental impact of an unclear framework on both the safety of society and tech innovation.

Setting the regulatory scene

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-competitive market regulation which is open for consultation until October 2021. In addition, there are a range of other consultations and strategies being formed over the next 6 – 12 months including the Innovation Strategy, Digital Strategy, National Data Strategy and Online Advertising consultation.[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 techUK is pleased to the see the Government acknowledge the need for better regulatory coordination.

For example, the DCMS Plan for Digital Regulation, published in July 2021,[2] sets out 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.

Separately, the Digital Regulation Cooperation Forum – made up of Ofcom, ICO, CMA, and the FCA – was formed in July 2020 to facilitate regulatory coordination in digital markets, and cooperation in areas of mutual importance.[3] It launched its annual plan for work in March 2021 which included priorities such as joining up regulatory approaches, responding to industry developments and building skills and capabilities.

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.

Summary of techUK response

techUK's response will consider how the legislation can achieve its objectives without giving way to unintended consequences which may divert the Bill away from creating safer online spaces, protecting free speech, and promoting innovation.

We will follow the structure set by the Committee. Section 1 (p 1 – 8) will provide our thoughts on the **objectives** of the Bill, highlighting areas where the current drafting of the Bill may give rise to unintended impacts including safety duties, age verification and free speech.

[1] DCMS Plan for Digital Regulation, Annex: timeline of upcoming digital regulation activity
[2] DCMS Plan for Digital Regulation: Driving growth and unlocking innovation, July 2021
[3] Digital Regulation Cooperation Forum, March 2021

Section 2 (p 9 – 12) will consider the **content in scope** providing our thoughts on the illegal content duties, why economic crimes should remain out of scope of the Bill and the challenges of regulating types of harmful content, including the protections for journalistic content and content of democratic importance for category 1 companies.

Section 3 (p 13 – 14) will look at **services in scope** considering exemptions, categorisation, thresholds, and private communications.

Section 4 (p 15 – 16) will look at the **role of algorithms** before we conclude with Section 5 (p 17 – 18) on the **powers of Ofcom and the Secretary of State**, outlining how the amendment powers in the Bill are problematic and not best practice.

Section 1: Objectives

1.1 Making the UK the safest place to go online and freedom of expression

techUK and its members are committed to user safety of individual platforms. A variety of different tech services and platforms already support initiatives to combat and eliminate harmful and illegal content online through sharing information with law enforcement, providing user reporting mechanisms and outlining in community guidelines how they expect platforms and services to be used in a way that is not harmful to others. The sector is in full agreement with the Government's dual objectives to make the UK the safest place to be online while protecting free speech and is aware that more needs to be done collectively to reduce levels of harmful and illegal content, including hate speech and CSAM, and the harm to users such content causes.

However, the current drafting does not reflect how the Bill is dealing with largely societal issues intersecting individual experiences and expression online. While it is often advertised that online harms regulation is of 24,000 technology companies – ranging from social media to online marketplaces to parental discussion forums and smaller campaigning organisations - the regulation is also moderating individual voices and behaviour with technology companies acting as the channel. As identified in the recent House of Lords inquiry, the inclusion of harmful content within the legislation and its vague definition has the potential to pose a threat to legitimate free speech.[4]

While tech companies in techUK's membership are committed to enhancing user safety and protecting free speech, there is no guidance in the Draft Bill about how the safety duties are to be balanced with duties to protect users' fundamental human rights and to give special importance to certain types of content. As with many aspects of the Draft Bill, 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. 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. These risk amounting to a general monitoring requirement and such obligations would necessitate the use of technology to filter and automatically remove content which would prevent providers from carrying out careful analysis of context. 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 legislation must outline all of 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

[4] House of Lords Digital and Culture Committee, 'Free for all? Freedom of expression in the digital age', July 2021

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 providing evidence for new harms as they emerge and seeking democratic approval for whether they should be included in scope and the potential implications on freedom of expression, while identifying when activity no longer presents a high risk of harm due to changes in systems and user experiences.

In addition, techUK maintains that further efforts should be placed in educating citizens to develop better digital rights and behaviours which prevent them from perpetrating harmful behaviour. Balancing competing individual rights and regulating content online remain very human issues and we should not lose sight of the fact that we are not only discussing regulation of companies who host user generated content but also the regulation of individuals and what they say and do online.

Overall, to balance the two objectives the Bill should provide clear guidelines or definitions around all of the types of harmful content in scope directed towards adults and children and how different types of harmful content should be dealt with. In its current form, the onus is on companies to decide what types of content are harmful and how they should be dealt with through their terms of service. This has the potential to result in inefficient action, inconsistent meanings of harmful content across the sector and an inevitable over-removal of content which could result in wide-spread violations of individual rights to free expression.

techUK and its members are committed to user safety and would like to see the Bill provide further clarity on how in scope services should go about creating safer online spaces while protecting free speech. In its current form, the lack of detail and guidance gives way to ambiguity which could result in unintended consequences for users and society.

techUK urges the Committee to balance the two objectives and consider how clear guidelines around what types of harmful content are in scope and how companies should respond will enable accurate decision making which mitigates harm without having adverse impacts on free speech.

1.2 Greater protection for children

techUK and its members support the objective to provide greater protection for children as a potentially vulnerable group who use the internet and many in-scope services will be introducing further measures under the Age-Appropriate Design Code. However, some of the requirements in the Draft Bill around implementing this greater protection could give risk to unintended consequences for children, including limiting access to online services and benefits.

There is a shared commitment across industry, children's charities, and Parliament to form a process which provides greater protection towards children. The Draft Bill aims to achieve this by requiring all companies in scope to have a duty to protect children from harmful content if the child can access the service. As framed in the explanatory notes, 'a provider is only able to conclude it is not possible for a child to access their service if there are robust systems and processes, such as age verification measures, in place that ensures children are not normally able to access their service'.[5] The implication is that age-verification, coupled with reviews of the effectiveness of the software and systems, has the potential to reduce businesses' compliance requirements under the child safety duties. The risk of this approach is that it could incentivise widespread age-gating which could result in children under 18 being prevented or significantly impeded from access to the internet. While it is right to think about children's special vulnerabilities and risks from online services, it is also important to put this in the wider context of the enormous benefits that technology and access to online services brings to children. These requirements could also require general monitoring for services to be able to verify age, which is in conflict with privacy laws and may conflict with UK law on intermediary liability.

Furthermore, many of the techniques around age verification are imperfect and the technologies are not necessarily tried and tested on scale. Machine learning models can never be 100% accurate as they can only provide a prediction of whether the user is likely above 18. In relation to other verification mechanisms, such as credit card and other ID checks, it is important for the solution to not be overly intrusive and disproportionate to the purposes for age assurance being obtained. This could result in two key issues. First, techniques may result in a conservative approach which denies children access to the benefits of the online world, such as knowledge, connection, enjoyment and expression.[6] Second, new technologies could have implications on children's data collection which may conflict with the AADC.

Although many of the same user-to-user services in scope of the Bill are looking to comply with the AADC which comes into force in September 2021, the legislation does not currently outline in detail how the 'child safety test' will interact with the AADC likely to be accessed by a child test. Given the overlap of companies in scope of both the AADC and the Bill, there is a need to explicitly address the links between the two regimes and any inconsistencies when it comes to protection of children's data. In addition, there is a need to clarify that a decision made by smaller in-scope service to implement safety tools under the Online Safety Bill will not necessarily bring them into scope of the AADC. The responsibility of coordinating these two regimes should lie with the regulators, and at a minimum it would be useful for Ofcom and the ICO to issue a joint statement around how the regimes will interact.

techUK urges the Committee to recognise the delicate balance between children's rights and their protection and that the Bill should enshrine a risk-based approach built on

[5] Online Safety Bill Explanatory Notes (page 28)

[6] University of East London: Institute for Connected Communities, Research for Ofcom on Protection of Minors

available age-assurance methods. This would promote the use of technologies that are fit for purpose and ensure the range of opportunities to learn, create, explore, and socialise online are not denied for under 18s.

1.3 Innovation and competition

As outlined in the Plan for Digital Regulation, policymakers should consider how to 'actively promote innovation' when crafting regulation. The Draft Bill seeks to align with this principle through supporting proportionality and following systems and processes which should enable regulation to be agile in a fast-moving sector. However, in practice the vast number of companies in scope has the potential for ripple effects in the UK economy which could adversely impact competition and innovation in the digital ecosystem.

The Government's impact assessment notes how the Bill will impact 24,000 tech businesses with estimated costs of £2.1 billion. The businesses included vary from discussion forums to online marketplaces to professional platforms and social media and the costs span a range of different sized companies that are part of an inventive, fast moving and constantly evolving tech sector.

The impact assessment includes requirements around establishing compliance teams and developing capacity to moderate content, which does not account for the realities of smaller businesses who may need to divert staff away from venture investment or source additional funding to resource compliance. This could have implications on the ability of smaller companies to compete with their larger comparators and create the need to consider attendant regulatory cost in addition to other economic implications of the legislation.

Furthermore, there are provisions within the Draft Bill which have the potential to stall the growth of investment and invention across a wide range of in scope services. For example, Part 4 allows Ofcom to require a service to use an accredited technology to scan and remove illegal content. This risks disincentivising in scope services from developing more innovative technology and could give rise to unintended consequences. Those intending to cause harm through platforms may look for loopholes in technology to persist with criminal or otherwise harmful online activity. Providers need to be able to adapt their technological solutions to keep ahead of the constant and evolving threats and mandating specific technology solutions will run counter to this, by locking companies into solutions that bad actors will be able to easily learn and exploit to their advantage.

Part 2 on risk assessment duties outlines how companies will need to review and update the assessment when they make a change to their service. These requirements will impose substantial obligations on companies with in-scope services that will entail significant resource allocation. This may result in smaller businesses being deterred from innovation due to a lack of capacity to keep up with levels of administration around risk assessments. Further thought should be given to the way in which any risk assessment requirements are implemented as they may create obstacles for new measures to be developed and implemented in a responsive and timely manner. A more flexible approach to risk assessments should be considered, with a reasonable timeframe for assessments to be completed.

Finally, although considered as a last resort, the proposal to include criminal sanctions for senior managers risks having a chilling effect on smaller companies and investment in the UK digital economy. For some companies, the very existence of turnover fines may be sufficient to deter investment with knock on effects for competition between firms and choice for consumers. 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. Therefore, the Committee should support Ofcom to have a bias towards promoting and supporting compliance and reserve sanctions for cases of non-compliance with reporting obligations or repeated failures to address a systemic issue.

Overall, we welcome the intention for Ofcom to outline its enforcement approach in guidance to give clarity to providers, as it does in relation to other regulated sectors. That enforcement approach should begin with private information or enforcement notices, allowing providers a reasonable opportunity to investigate and, if necessary, take appropriate action. This will no doubt vary from company to company making it particularly important to avoid a one size fits all approach towards compliance.

techUK ask the Committee to consider amendments to address the economic implications of the Bill for smaller businesses, fair competition, and innovation. Over-proscriptive and heavily administrative approaches could overwhelm start-ups and SMEs who are looking to grow and evolve in the tech ecosystem.

1.4 Setting an international example

The strength of the UK Government's framework towards regulating online content is the nuanced and proportionate approach with a focus on systems and processes rather than individual items of harmful content or specific instances of harmful behaviour. These factors, paired with clear political commitments to free expression and protection of journalism, make the Bill more worthy of emulation overseas than similar Bills from other governments.

The Government should however pay attention to features of the Bill which may detract from this. For example, as outlined above, the Bill proposes that the Secretary of State have authority to reject a code and require it to be re-written and to give strategic direction to the independent regulator. In the hands of a non-rule of law government, such powers would not align with UK foreign policy and the Government would not be in a strong position to object if they were copied.

Companies already undertake many safety and self-regulatory initiatives and the Committee should give consideration to the benefits of in-scope services being able to use the requirements of independent schemes such as IWF or GIFCT to meet duties of care, as well as their associated transparency and oversight frameworks. If this approach were to be adopted in the UK, it would free up Ofcom's resources to focus on other issues, rather than duplicate effort unnecessarily. It would also make the regulatory framework more scalable and affordable for in scope companies and avoid needless overlap with existing, effective, work to tackle harms.

While it is important for the UK regime to lead the way and set a global precedent for a proportionate and workable regime, it should also avoid confusion by departing from established and well-understood standards only when strictly necessary. Various standards adopted in the Bill take a different approach to the current regime that applies to online platforms, derived from the eCommerce Directive. First, the Good Samaritan Principle is lost in the Draft Bill which does not serve to build confidence in how the regime will support proportionality and innovation for the 24,000 diverse businesses in scope. Second, the Bill's definition of illegal content includes content which the provider "has reasonable grounds to believe" amounts to a relevant offence. This language is different from existing requirements, well-established following many years of legal development, to take action where a provider has "knowledge or awareness" of illegal activity or information (or of facts or circumstances from which illegal activity or information is apparent). Similarly, under the current regime, on becoming aware of illegal content, the provider must take action "expeditiously" whereas, under the Bill, providers must take action "swiftly".

The use of similar but distinct legal concepts and terms, without further clarity on their meaning, introduces complexity and ambiguity as to the expectations of providers under the forthcoming regime. To avoid undue confusion, language from the current regime could be used in the Bill.

techUK encourages the Committee to consider the benefits of international regimes which provide clear language, guidelines, and definitions for companies, including how they can enable quick and effective decision making around the removal of content.

Section 2: Content in-scope

2.1 Illegal content

techUK members condemn illegal activity being perpetrated on their platforms and services and it is important that the Online Safety Bill continues to prioritise the regulation of illegal content, building on existing laws and practices. The Draft Bill provides definitions and guidelines around CSEA and terror content, as two priority illegal content types in scope, which shows a step forward in supporting a joined-up approach between tech, law enforcement and the regulator. There are already many company-led systems and processes in place to eliminate CSEA and terror content which should be considered as part of how in-scope services can fulfil their 'priority illegal content' safety duties.

To ensure that in-scope services can fully understand the extent of the illegal content duties, the Bill must provide further detail on the additional offences which will be considered 'illegal content' and 'priority' illegal content. This will enable businesses to understand the scope of the obligations they face, comment now on their appropriateness and prepare adequately for their implementation. The Bill provides for these offences to be specified in regulations that are to be made by the Secretary of State. As a result, there will be much less scrutiny over decisions about which offences are included in scope than if those offences were set out in the Bill. There is also little clarity on the process and timelines for the decisions about which offences will be specified including whether those decisions will involve stakeholder consultation.

Furthermore, adding categories of illegal content to the scope of the Bill should follow a risk-based approach. Many services in scope simply do not have context for why a user is in possession of a piece of content which could be considered technically illegal. For example, an academic or journalist may be reporting on content which is illegal activity such as terrorism, yet the purpose for their analysis or upload of content might be educational. This contextual detail coupled with the technical challenge of developing robust automated tools to scan for categories of illegal content, makes it particularly important for any decisions around illegal content to be carefully considered to avoid unworkable outcomes.

2.2 Economic crimes and online fraud

techUK agrees there is a need for a new action plan to address potential harm to consumers arising from online fraud. However, the majority of techUK members believe that the Online Safety Bill is not the right mechanism to address economic crimes.[7] Extending the scope in this way would de-rail the already complex legislation from achieving its stated aims and delay practical action to reduce levels of online fraud. Rather, the solution lies in coordinated action within digital supply chains and between enforcement authorities. We therefore encourage the Committee to forbear a recommendation to extend the scope of the Bill to include economic crimes.

As stated in Principle 1 of the Plan for Digital Regulation policymakers should ensure 'that regulation is outcomes focused', yet there is no clarity on how adding economic crimes to the Online Safety Bill will stop online fraudsters from operating in the UK. The Bill was not written with the intention of regulating economic crimes, it was designed to focus on user-generated content. An extension of scope to include economic crimes and paid for advertising has the potential to take the Bill's attention away from the objectives to provide greater protection for children while enabling freedom of expression and supporting

[7] techUK members BT and Sky do not hold the view expressed here. They are aligned with the Treasury Committee Work and Pensions Committee letter to the Prime Minister dated 21 July 2021, that the government should seek to ensure that the Bill allows for platforms to be made more accountable for tackling content which promotes consumer harms – including fraud, scams, pirated content and poor-quality goods or services, alongside the action taken elsewhere by the Government.

innovation. It would also bring in a much larger set of businesses into scope from various sectors who are required to disrupt the journey of online fraudsters.

The Committee should also note that Home Office has recently launched its 2022 – 2025 Fraud Action Plan to disrupt online fraud and DCMS will publish a separate consultation in Autumn 2021 on advertising regulation which will specifically look at the current regulation of paid-for advertising. Given the research and specialism that has gone into developing the Fraud Action Plan and Online Advertising Programme, these should remain the two appropriate vehicles to consider legislative and non-legislative approaches towards tackling online fraud.

Online Fraud Steering Group

techUK acknowledges the ongoing threat to consumers from online fraud and our members have a shared ambition to enhance collaboration between sectors to build on existing solutions while increasing consumer awareness and resilience. In April 2021, the Online Fraud Steering Group (OFSG) was set up, co-chaired by techUK, UK Finance and the National Economic Crime Centre, to form collective solutions to the respond to patterns of fraudulent activity.

Since being formed, the group has agreed a delivery infrastructure, operational principles, and governance, including how it will engage with the Home Office's Joint Fraud Taskforce. Four key workstreams have begun work to cut across different fraud typologies: 1) online advertising, 2) developing a threat assessment 3) enhancing communications and education and 4) striving for innovative and preventative solutions.

techUK members believe that collaboration across public and private sectors, the DCMS Online Advertising Programme and the Home Office Fraud Action Plan should be prioritised as the appropriate vehicles to review online advertising and form tangible solutions which reduce the threat of online fraud.

2.3 Definitions of harmful content

As we have expressed in the objectives section, there is a need to balance regulating harmful content and protecting freedom of expression which creates an even greater need to have clear definitions and categories of harm listed in the text. The draft Bill does not currently provide this level of clarity around definitions and categories of harm.

In relation to child online safety duties which will involve category 1 and 2 companies, the Draft Bill provides a definition of harm towards children as 'having a significant adverse physical or psychological impact on a child of ordinary sensibilities'[8] with the categories of harm being left to secondary legislation. The explanatory notes seek to clarify how this could include content that causes feelings such as 'serious anxiety, fear, and longer-term conditions such as depression, stress and medically recognised mental health issues'.[9]

[8]

Psychological experiences are often subjective and individual which creates a legal challenge around how companies should determine whether the content is having such an impact that it should be removed. This is further complicated by the ambiguous requirement for providers to assume that the child will have a characteristic or belong to a certain group of people, in the case of content which may particularly affect people with that characteristic or members of that group. The only guidance currently given, in the explanatory notes, on the types of characteristics or groups that may be relevant are 'people with disabilities or people of a particular region'. However, there is a very wide range of characteristics and groups that providers may or may not be intended to assume. Without clear guidelines in the legislation around what types of content will be included in scope as having a psychological impact on individual children, companies will be prevented from acting clearly and decisively to fulfil their child safety duties.

Furthermore, for harmful content towards adults, the Bill does not provide any detail on the categories of harm which will be in scope both in relation to adults and children. Leaving this to secondary legislation delays 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 an urgent review of the implications of leaving the categories of harm to secondary legislation including significant delays in the regime being workable for the 24,000 businesses in scope.

techUK acknowledges 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.

2.4 Journalistic content

In Part 2 of the Draft Bill journalistic content is defined as 'content that is generated for the purposes of journalism which is UK linked' (UK users form target market or is of interest to a significant number of UK users).[10] The explanatory notes outline how this includes news publisher content. It is outlined how this provision will only apply to category 1 services and they will need to outline in their terms of service what 'consists of journalistic content and how the importance of free expression is taken into account when making decisions about journalistic content and the policies for handling complaints in relation to content which is, or is considered to be, journalistic content'.[11]

[9]

[10] Draft Online Safety Bill, Part 2 (page 13)

[11] Draft Online Safety Bill, Explanatory Notes (page 20)

This broad definition does not provide any insight for category 1 companies on where the threshold should lie for content to be considered journalistic content. This could have adverse impacts, such as different meanings of journalism across the sector and the potential for complaints to be raised around the prevalence of harmful content which is perpetrated by an individual who is claiming to be a journalist.

The Government has made clear that the definition of journalistic content is intended to include 'citizen journalism'. However, as the House of Lords Communications and Digital Select Committee noted, under the current definition of journalistic content, there does not appear to be "any prospect of Ofcom or platforms being able consistently to distinguish citizen journalism from other forms of expression by individuals".[12] Further, given that platforms will be required to create additional, expedited appeals processes for journalistic content, the broad definition of journalistic content will result in providers facing an overwhelming number of claims from users that their content is "citizen journalism" and should therefore be subject to the "expedited" complaints procedure. This could make the duty to have an expedited complaints procedure very difficult to comply with, especially if a specific unfeasible timeline is required by a Code of Practice.

Protecting journalism and free speech is central to the maintenance of democratic society, yet to avoid this being abused, the legislation should provide clear definition of journalism which includes outlines of journalistic content and what makes an individual a journalist.

techUK would like to see the Committee provide parameters around the definition of journalistic content to enable businesses to have clear guidelines which will enable quick and effective decision making around how to protect journalists.

Section 3: Services in-scope

3.1 B2B service providers

The Draft Bill outlines a reduction of scope from the Full Government Response with some areas of clarity on the exemptions listed in Schedule 1, including for email, SMS/MMS and one-to-one aural communications.

The usage and functionality of a platform or other internet service has an enormous impact on the likelihood of harm occurring to adults and children, and we recommend that the Online Safety Bill acknowledge this, to avoid over-burdening businesses and inadvertently reducing competition. Specifically, it appears some of the exemptions are because the services are primarily used by adults for work purposes, and to communicate with small groups of known contacts. Content shared in a similar context, such as cloud collaboration software is equally unlikely to be harmful so the same rules should apply.

[12] Communications and Digital Committee Letter to Secretary of State, 'Growing up with the Internet and Regulating in a Digital World' (May 2021)

Furthermore, there is no explicit mention in the Draft Bill of the exclusion of enterprise and business services from the duty of care which departs from Section 116 (2) and 116(4) of the White Paper. Given their role in the value chain, it is understood that the intention is for B2B service providers to be exempt from safety duties and that they should be considered 'access facilities' (Part 7, Section 4 of Draft Bill) who only have responsibilities when Ofcom applies to the court for an 'access restriction order' (Part 7, clause 93).

The Draft Bill's explanatory notes go on to explain what this means in practice saying: *"For example, if entity A buys software from software company B on a software-as-a-service basis, and the software enables entity A to create a regulated service, entity A (rather than software company B) is to be considered the service provider"* (para. 730).

While the guidance is clear, the actual legislation is not. The guidance itself is not law. techUK believes that the most effective way of ensuring that the Government's clearly established intentions are met would be through the finding of a formulation that is based on the guidance, rather than the current one in the Draft Bill which is far less precise, and the formulation to be put on the face of the Bill itself.

3.2: In-scope user-to-user services and categorisation

Despite some welcome exemptions, the broad definition of user-generated content means that there will be 24,000 services in scope. In-scope services are not only diverse because of size and functionality but also because they host different types of content for various purposes ranging from professional to educational and social. The types of content should be considered to determine exemptions and categorisation. For example, if a service is hosting only professional user-generated content, it is likely that the levels of risk of harm will be low which might provide that they should be exempt as a 'low risk' service.

Furthermore, some companies may have more than one service within scope of the Bill, yet the purpose and function of individual services will not be the same even though they are part of the same company. While proportionality is rightly at the heart of the intention of the Bill, this principle must apply to levels of risk on individual services even if they are part of the same company.

Without levels of detail around categorisation and proportionality, the Draft Bill currently poses a challenge for in-scope services to understand how they should begin preparing for the regime and what criteria will result in services moving between categories. This lack of clarity may limit innovation and prevent companies from having confidence that their growth will not automatically result in additional compliance requirements without an appropriate and proportionate lead in time.

Designating companies into categories and outlining the thresholds between category 1 and category 2 - including how a company should comply if one of their services is category 1 while another is category 2 – is a fundamental part of this regime that must not undergo further undue delays.

techUK would like to see the Committee acknowledge the diversity of the 24,000 in scope services, while ensuring that compliance does not follow a one size fits all approach. Delays in timelines around decisions around categorisation and compliance may limit companies understanding and confidence in what will be required of them.

3.3: Search services

While we welcome the inclusion of obligations on search services in a different chapter of the Bill, in apparent recognition of the very different nature of user-to-user and search services, in practice, the obligations on search services are very similar. In particular, the obligations on search services to minimise the risk of users encountering content, including legal but harmful content, do not appreciate that search engines do not host content and are essentially indexes of the web. There are hundreds of new web pages published every second. This makes it impossible to evaluate the context of regulated content.

3.4: Private communications and user privacy

The Draft Bill does not adequately address the need to balance user privacy and safety with certain provisions diverging from the Full Government's Response to the White Paper and the UK's international human rights obligations.

Privacy is important because it enables users to set boundaries, protect themselves from harm and make free choices. The overwhelming majority of users are responsible and law-abiding and have a reasonable expectation of privacy when they share within a limited or controlled group. It is a mistake to assume that all information is either wholly private or wholly public: users may choose to share with one other person; a small, closed group; or a wider audience. They also share information for personal and work purposes and will have a separate privacy expectation in each context. Regulation to mandate removal of content that is ill-defined provides perverse incentives for companies to be overly censorious, particularly when accompanied by strong sanctions. The risk to fundamental freedoms is even greater when regulation mandates proactive reporting of potentially harmful behaviour to law enforcement.

The explanatory notes provide the first mention of encrypted services by outlining how Ofcom may require accredited technology to identify CSEA content on any part of the service (including in relation to encrypted private communications). It is not entirely clear how this would work in practice, although these powers have the potential to amount to Ofcom mandating the use of third-party technology to proactively monitor private communications which would in effect require businesses to carry out interception at scale and remove relevant content. While more needs to be done to prevent CSEA, this provision is highly complex and controversial because it has the potential to significantly undermine the levels of security and privacy available to most users who have not committed illegal crimes. The implications of these provisions need to be addressed in detail to ensure that the approach towards private messaging is balanced and proportionate, taking into account the adverse impact on the average consumer and whether there are alternative solutions to combat CSEA content without overriding encryption.

techUK asks the PLS committee to address the levels of clarity still needed in the Draft Bill to translate the shared commitments to support user safety and protect human rights into a workable framework for 24,000 businesses in scope.

Section 4: Algorithms and User Agency

Algorithms and content moderation

Algorithms can assist human moderators in multiple ways. They can automatically prioritise and flag high-risk or harmful content, quickly and efficiently while learning and adapting 24/7 to improve accuracy of identifying and reducing harmful content online.

However, there are many limitations to relying on algorithms. As a result, we believe use of algorithms should not be mandated. Rather, it should be left to services in scope to determine the appropriate use of algorithms for content moderation. The content that services in scope of the Bill will need to review will often be highly contextual and nuanced, with individual subjective experiences defining harm. This is not only problematic for companies to know how to act but also for algorithms that do not have a broader understanding of cultural and contextual factors which may influence whether content is harmful. For example, some types of harmful and illegal content may be obtained by journalists and academics for legitimate and lawful reasons, although the algorithm may not be able to identify the context and purpose.

Furthermore, online content can appear in multiple different formats such as videos, text chat and memes, with each format requiring a different moderation practice and process. Live content, such as live video streaming, can be particularly challenging as this content must be analysed and dealt with in real-time, thus requiring highly bespoke content moderation systems that can integrate both automated and non-automated tools. In addition, the creation and dissemination of deepfakes also has the potential to be extremely harmful and can be difficult for humans and algorithms to detect. However, solutions in this area are progressing, for example companies such as Adobe have recently developed an authentication tool in the fight against deepfakes.

To add to the complexity, the language and format of online content is evolving rapidly over time, making it difficult for human and automated systems to detect harmful subject matter. To make this more challenging, some users will attempt to subvert moderation systems by adjusting the words and phrases they use. Moderation systems must therefore adapt and keep pace with these changes.

Detection of harmful content heavily relies on the training data used and the parameters set when building the algorithm. Good quality training data and a broad consideration of the factors affecting what makes a piece of content harmful are essential to build robust and accurate AI detection systems. Many organisations are already putting this in place by following a content moderation process which moderates content at one or both of two points in the workflow. 1. Pre-moderation when the uploaded content is moderated prior to publication, typically using automated systems 2. Post- or reactive moderation when content is moderated after it has been published and it has been flagged by other users or automated processes as potentially harmful, or which was removed previously but requires a second review upon appeal.

There is a need to be considerate around the complexity of relying on algorithms for content moderation. An algorithm removing content which is not universally accepted as harmful can result in violations of users' freedom of expression, departing from the Online Safety Bill's stated ambitions.

Section 5: The Role of Ofcom

5.1 Ofcom as the regulator

We welcome the choice of Ofcom as the regulator of the regime given its experience and proportionate approach to regulation in other sectors, as well as the intention for Ofcom to outline its enforcement approach in guidance to give clarity to providers, as it does in relation to other regulated sectors. That enforcement approach should begin with private information or enforcement notices, allowing providers a reasonable opportunity to investigate and, if necessary, take appropriate action. Information requests should be proportionate to the capabilities of different in-scope services and levels of risk to ensure that the cycle of innovation is not damaged. Sanctions should be reserved for cases of non-compliance with reporting obligations or repeated failures to address a systemic issue.

5.2 Powers of the Secretary of State

Throughout the text of the Draft 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 listed in the text to set the threshold for categories of companies and to define which providers will be subject to fees which we consider more technical powers.

There are short-term concerns about some of the technical powers, including delays about when companies will be designated category and 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 three main clauses which we have identified in the text to be problematic relating to the **amendment powers** of the Secretary of State:

- **Part 2, Clause 30 (safety duties and codes of practice)** - The Secretary of State has the powers to amend the online safety objectives for all regulated services. If the Secretary of State makes an amendment, Ofcom must consider whether a review of the codes of practice is required.[13]
- **Part 2, Clause 33 (safety duties and codes of practice)** – The Secretary of State has powers to require Ofcom to modify a code of practice to reflect Government policy.[14]
- **Part 3 (transparency reporting and fees) -** The Secretary of State will have powers to change the kind of information Ofcom will require to be included in transparency reports and the frequency in which the reports are produced.[15]

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, allowing the Secretary of State to amend the safety objectives and requiring Ofcom to review the codes to reflect Government policy may impair effective systems and processes which companies already have in place to moderate content (ones which will likely follow guidance from Ofcom).

As we move through this legislative process, clear delegation of responsibility and transparency in approach will be essential to allow both Ofcom and companies to get the regime set up in good shape quickly and confidently.

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 firmly support's Ofcom as an expert independent body that should be fully trusted to make decisions around codes of conduct and online safety objectives. The powers given to the Secretary of State have the potential to interfere with Ofcom's independence.

techUK would support a process which enables Ofcom to follow guidance from the Secretary of State but ultimately leaves the powers of enforcement and decisions around enforcement with the communications regulator.

5.3 Media Literacy

Balancing competing individual rights and regulating content online remain very human issues and we should not lose sight of the fact that we are not discussing regulation of

[13] Draft Online Safety Bill, Part 2, Clause 30 (page 27)
[14] Draft Online Safety Bill, Part 2, Clause 33 (page 29)
[15] Draft Online Safety Bill, Part 3 (page 46)

companies who host user generated content but the regulation of individuals and what they say and do online.

Digital literacy must be a greater priority and focus in on changing behaviours over time and instilling ‘digital civility’. It is vital that we empower and educate users of all ages to navigate the online world safely and securely.

Education can play an important role in helping society develop digital behaviours and skills online, enabling kinder and more equal individual experiences. Companies already either create their own tools to help empower and educate – whether for children, their parents, teachers or vulnerable adults, or partner with other providers to do this.

It is vital that regulation does not cut across this work, but instead builds on it to ensure there is a concerted effort to create an inclusive strategy that responds to the varying needs of users.

The recent DCMS media literacy strategy provides useful insight into the media literacy capabilities of society while striving to stimulate activity in the UK which both supports online safety and encourages users to make the most of what the internet has to offer. This is a step in the right direction, although the test will be whether this plan is put into action to ensure media literacy remains of equal importance to any form of regulation and we urge the committee to analyse the Government’s plans in this regard as part of the ongoing scrutiny of the Bill.

September 2021