Written evidence submitted by the Internet Service Providers' Association (ISPA)

Response: DCMS Sub-Committee on Online Harms and Disinformation Inquiry

About ISPA

ISPA is the trade association for providers of internet services in the UK. ISPA has approximately 150 members, 90% of which are SMEs, as well as large multinational companies. Our members provide internet access, hosting and a wide range of other services to consumer and businesses and we represent a wide eco-system of providers including those that build their own networks and those that resell services via the fixed and wireless networks.

Introduction

ISPA welcomes the opportunity to respond to this public consultation on Online Safety and Online Harms. It is important to recognise that the UK already boasts one of the most developed online safety frameworks in the world, due in part to action taken by ISPs (or access/network providers)[1] who have, for almost two decades, taken the initiative to protect consumers by actively combatting child sexual exploitation and abuse (CSEA). A large number of UK ISPs are members of the Internet Watch Foundation (IWF) or implement the IWF's watch list to block CSEA via third parties. Many ISPs also offer parental controls which allow parents to set restriction levels and filter various categories of online content, some, including the largest ISPs, at network level and others by providing tools to parents.

Responses to the inquiry themes

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

ISPA supports the Bill attempt to address the whole value chain through the online safety regime

The internet is a complicated, multi-layered value chain and ISPA has always argued that measures to address content issues should fall on those parts of the chain that are closest to the content in question, have the greatest level of control and can carry out the most targeted interventions. UK Government and law enforcement have traditionally relied on UK-based access providers to carry out online safety interventions, yet with numerous changes to online business models and the architecture of the Internet, it has become apparent that access providers cannot any longer be seen as gatekeepers to the internet and that providers of online platforms are often in better place to address content issues. With this in mind, ISPA supports the current definition of regulated services as user to user services and search services as these are best suited to address and prevent the presence of harmful and/or illegal content online.

While access providers rightly do not fall under the duty of care, the Draft Bill envisions them to support the regulator in enforcing the online harms regime by restricting access to non-compliant services. ISPA supports this inclusion, as long as the independent court process is maintained, but we would welcome

[1] Also defined as "Internet Access Services" in the explanatory notes for the Draft Online Safety Bill

clarity on the practicalities of access restriction orders. It will further be important to ensure that business disruption measures can be carried out by all players that nowadays facilitate in users accessing the internet. Alongside access providers this should include a variety of companies and services that have recently started to carry out some of the functions that are necessary for the use of the internet, including browsers, app stores and in certain circumstances operating systems and apps. The definition of access facilities in the Draft Bill does suggest that it is Government intention to have a broad application, but we would urge the Committee to test this further as part of its inquiry to ensure that the enforcement elements of the Bill effectively work in practice.

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?

ISPA would like to see a greater recognition of the impact that technical changes and encryption will have on how the internet is accessed and used

As indicated previously , the Internet is constantly evolving, and the Online Safety regime must be reactive to new and emerging changes to the internet supply chain. This includes, but is not limited to, new forms of encryption such as DNS over HTTPS (DoH) which is being rolled out by Mozilla (Firefox) and Google (via Chrome), as well as Private Relay which Apple will enable for a large part of its user base. Alongside the enabling of encryption, these technical changes also influence how internet traffic is handled.[2] These developments can have positive benefits and enhance privacy or security, they can also impact the effectiveness of existing online safety measures, such a parental controls, and limit the ability of access providers to support their users. Ultimately, this should not result in a debate about the benefits of encryption, but it does put a stronger emphasis on how these technologies are implemented and how they impact internet users and especially the choices of parents and children. For example, enabling DNS-over-HTTPS by default within an app, a browser or a social network has privacy, security and safety implications and all three should be taken into account before an online service or platform makes such a decision. We would like to see greater recognition of this admittedly complex issue in the new online safety framework, e.g. through a greater recognition within safety-by-design principles and a broad application of definitions such as access and ancillary facilities.

ISPA would like to see more clarity about how Business Disruption Measures will work in practice

Business Disruption Measures (BDMs) are an important back stop power in the new online safety regime, and we support the court based process that has been suggested in the Draft Bill. However, we would like to see greater clarity of how the BDM process will work in practice, including time frames, consultation requirements, costs to ISPs, processes for updating consumers and unintended coverage of legal content. There also needs to be a clear process to ensure that BDM orders are proportionate, technical feasible and that they can be served on all relevant companies that help the facilitate access to the internet. We urge the Committee to seek more clarity on this to ensure that this important back stop power can be implemented effectively.

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

ISPA would like to see more clarity around the relationship between Government and Ofcom

[2] These technical changes are not about encrypting content but more about encrypting those parts of the internet that determine how data is routed and how requests for content are resolved.

ISPA welcomes Ofcom's appointment as regulator for the online safety regime. However, we have concerns regarding the interaction between the Secretary of State and Ofcom as a regulator. Unlike as in the areas of broadcasting or telecoms regulation, the Draft Bill provides the Secretary of State with extensive powers to direct Ofcom to take or revise decisions (e.g. clauses 33(1), 109 and 113). This is highly unusual and in our opinion that interest of the public and industry tend to be better served by an independent regulator that is isolated from short-term political thinking.

That being said, while Ofcom should be independent, its powers should still be clearly prescribed in the final Bill. We urge the Committee to seek more clarity regarding Ofcom's requirements to consult with the sector ahead of imposing Business Disruptions Measures and seek a tighter definition of Ofcom's information gathering powers – our members are already subject to extensive information gathering requests form Ofcom as part of general telecoms legislation and the Draft Bill provides too much leeway to Ofcom to seek further information from them under Clause X. At a minimum, existing proportionality requirements from Communications Act 2003 (s135, 136 and 137) should be carried over to the Online Safety Bill.