Response: Online Safety Bill Committee call for evidence

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 fixed and wireless networks.

Introduction

ISPA welcomes the opportunity to respond to the Bill Committee on the Online Safety Bill (OSB). At the outset, 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) who have, for almost two decades, taken the initiative to protect consumers by actively combatting child sexual exploitation and abuse (CSEA) through tools like the IWF watch list and offering parental controls. ISPA supports the Online Safety Bill's focus on regulating services which are closest to the content and therefore best placed to put in place measures deal with content and support users.

Our members still have a role to play in the envisaged regime of the OSB. They are classed as access facilities that will support the backstop enforcement of the regime via Businesses Disruption Measures (BDMs) through blocking non-compliant sites. These backstop enforcement powers will be vital in making the overall regime work, especially since the inclusion of commercial pornography has ramped up the likelihood of these powers being actually used instead of serving merely as an incentive for compliance.

However, we are concerned about the lack of detail in how these BDMs will work in practice and believe that the Bill should more explicitly spell out the types of services that will be asked to carry these out. Failure to be explicit could result in an enforcement regime that is not only ineffective (it does not cover all the relevant players) but also disproportionate (those players that are covered would need to shoulder all the cost burden of operating an ineffective regime).

Responses to the Committee

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

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 can no any longer be seen as 'gatekeepers' to the internet and that providers of online platforms are often in better place to address content and enforcement issues. As ISPA suggested to the DCMS Sub-Committee on Online Safety and Online Harms, it is important that measures to address content issues fall on those parts of the chain that are closest to the content in question as they have the greatest level of control and can carry out the most targeted interventions. With this in mind, ISPA supports the current definition of regulated services as user-to-user services and search services, these are best suited to address and prevent the presence of harmful and/or illegal content online.

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 technical standards that underpin the internet are constantly evolving, and the Online Safety regime must be reactive to new and emerging changes to the internet supply chain. A more recent trend is the attempt to encrypt aspects of traffic handling[1] via new standards such as DNS over HTTPS (DoH), Encrypted Client Hello or Apply Private Relay. Crucially, these types of traffic encryption can be implemented by a variety of players in the internet value chain, including applications, app stores, browsers or operating systems. There are two important aspects to consider:

1. The impact of these developments of online safety and user support mechanisms and the importance of privacy by design
2. The impact of these developments on how the OSB can be enforced and the need to be explicit in how the bill is phrased

Online safety and user support

We generally support the implementation of these standards as they can have positive benefits and enhance privacy or security, however, they can also be implemented in such a way that they deliberately break or undermine existing support mechanisms for users such as ISP parental controls, technical user support and safety systems in schools. 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.

Technical changes and enforcement

These changes also affect how internet traffic is routed and who has visibility of high-level information about online traffic. Traditionally this role fell to the local ISPs, which as stated above had a gatekeeper function and was the prime target of online safety interventions. However, with developments such as DoH, Encrypted Client Hello and Private Relay, the gatekeeper function has become dispersed and essentially moves to other players in the value chain. This put a premium on ensuring that the OSB effectively captures these new developments and is capable of including all relevant players that facilitate users in accessing the internet and thus need to be included in the enforcement regime. The efficiency of the disruption measures would be severely undermined if these changes are not addressed. We set this out in more detail below.

ISPA would like to see a more explicit definition of access facilities in 125(11)

ISPA supports the inclusion of BDMs as they are an important backstop power in the new online safety regime, provided that are used in a proportionate and effective manner. However it is essential that they can be carried out by all players that facilitate users accessing the internet (see previous section). 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 VPNs, browsers, app stores as well as operating systems and apps. The definition of access facilities in the Bill

[1] 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.

does suggest that it is Government intention to have a broad application, but we are concerned the Government refusal to explicitly enumerate a wider range of players on the face of the Bill will undermine the enforceability, especially as a lot of these players are not UK headquartered.

This could be addressed by amending Section 125(11) which currently merely refers to internet access services and mobile app stores and should instead explicitly name the types of services that facilitate internet access, include operating systems and non-mobile app stores. A failure to be explicit could result in an enforcement regime that is not only ineffective (it does not cover all the relevant players) but also disproportionate (those players that are covered would need to shoulder all the cost burden of operating an ineffective regime).

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

Business Disruptions Measures are intended as a backstop power by restricting access to non-compliant services through what the Bill labels "business disruption measures" (BDMs) or more specifically for access facilities "access restriction orders." Throughout the pre-legislative scrutiny, Government emphasised that it only expected these powers to be used sparingly but that was before the decision to include commercial pornography in the regime which is highly likely to increase the use of the backstop power. We have always pushed for more clarity, but the increased use of the power will make this more important. We would welcome an indication form Government on how often the believe these backstop powers will be used and also set out a range of additional areas below.

We welcome the broad structure of the BDMs process and particularly support the requirement for Ofcom to apply to a court, given that BDMs are a serious intervention and should not be taken lightly. However, much of the detail surrounding BDMs is excluded from the Bill. More specifically, critical information regarding time frames, consultation requirements, costs to access facilities, processes for updating consumers and unintended coverage of legal content are currently unknown.

We are concerned that the lack of detail could lead to an enforcement process that fails to take account of the complexity of restricting access to online content. We strongly recommend that access facilities are consulted in the process of making an access restriction order and that the court should be required to take into consideration the technical feasibility of an order. This becomes even more important in the case of access restriction orders where the burden of proof is lower. We would also welcome more detail on how Government intends the process to work once an access restriction order has been made. For example, what is the process for moving regulated services on and off a list of blocked services? How often will this list be updated and how much time will access facilities have to update their systems? Clarity in this context is important as any work to implement an order need to resources and sequenced alongside other requests and general business operations.

We are also concerned that there is no requirement to assess the impact of an access restriction order on access facilities and their position in the market. For example, if access restriction orders only fall on a subset of providers, they could drive consumers to switch providers or utilise apps and services that circumvent blocks. This again highlights the need for access facilities to be properly defined to ensure that enforcement is both effective and proportionate.

We appreciate why some of the detail that we require is being left to secondary legislation, but we still urge the Committee to test Government's approach to structuring the enforcement regime and to seek as much clarity as possible.

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

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 broadcasting or telecoms regulation, the Bill provides the Secretary of State with extensive powers to direct Ofcom to take or revise decisions. This is highly unusual and in our opinion the interests 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 Bill 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 from Ofcom as part of general telecoms legislation and the Bill provides too much leeway to Ofcom to seek further information from them. At a minimum, existing proportionality requirements from Communications Act 2003 (s135, 136 and 137) should be carried over to the Online Safety Bill.

We urge the Committee to limit the direction-making power of the Secretary of State to the setting of strategic priorities for the regulator and uphold consultation and regulatory standards that have been established across the UK in other regulatory regimes.