ISPA Response to Communications Committee 'The Internet: To Regulate or Not to Regulate' Inquiry

1 About ISPA

ISPA is the trade association for providers of internet services in the UK. ISPA has over 200 members, 90% of which are SMEs as well as large multinational companies. We are proud to be an organisation which covers the whole Internet value chain, including companies that provide access, hosting and other online services. We represent communications providers that serve consumers and business, those that build their own networks and those that resell services.

2 Introduction

ISPA welcomes the House of Lords Communication Committee inquiry into internet regulation. The call for evidence raises a number of important issues that affects the UK public but also the conduct of online companies. These issues require careful consideration and for that reason we feel that it is important that the inquiry is conducted on the best evidence base possible.

It is important to recognise as starting point that, rather than being a 'wild west' as is sometimes described, the internet is already subject to both general and specific regulation and we would therefore encourage the Committee to focus its intention on how (rather than whether) the internet should be regulated. This includes oversight in various forms from a large number of regulatory or co-regulatory bodies, from the ICO, Ofcom and BBFC. Moreover, the internet is based on a complex and interlinked value chain that involves both users and a variety of online services that perform different functions. It is important to understand the individual elements of the value chain and the role and responsibilities each part may perform.

The definitions included in E-Commerce Directive provide helpful framework for the role and obligations of Internet companies:

Hosting providers: store data which is selected and uploaded by the users of their service. This data is intended to be stored for an unlimited period of time. Hosting providers can be exempt from liability under EU law if they are "not aware of facts or circumstances from which the illegal activity or information is apparent" or they "do not have actual knowledge of illegal

activity or information". Hosting providers must expeditiously remove such information once they have been made aware of its illegality.

Mere Conduits: deliver either network access services or network transmission services. They transmit large amounts of data for their subscribers. Mere conduits have liability exemptions under EU law when they are passively involved in the transmission of data. An ISP is commonly described as a mere conduit.

Caching providers: temporarily and automatically store data. Caching providers can be exempt from liability under EU law if they meet certain conditions pertaining to their storage of data.

---

3 How should the internet be regulated?

(Q1) Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The internet is a heterogeneous entity that has developed organically over the last three decades and is subject to regulation and specific regulatory activity. Due to the rapidly evolving nature of the internet, self-regulation has also acted as an important part of the regulatory landscape; helping to put in place rules and procedures more quickly and effectively than formal regulation. We can see evidence of effective internet regulation already being carried out by a number of public and private bodies as well as legislation; for example:

- **E-Commerce Directive**, which sets out harmonised rules for online businesses.
- Internet Watch Foundation (IWF), a self-regulatory body founded by the Internet industry that tackles online child sexual abuse content.
- **Counter-Terrorism Internet Referral Unit (CTIRU)**: This organisation is run by the Metropolitan Police and, as of December 2017, has been linked to the removal of approximately 300,000 pieces of 'illegal terrorist material' from the internet.
- **Defamation Act**, which created additional defences to tackle 'libel tourism' and new defences for online publishers.

It is also worth noting that ISPs have stronger data protection requirements than many offline providers, as set out in the Privacy and Electronic Communications Regulations (PECR). Given this, it would be inaccurate to characterise the internet as having consistently weaker protections for individuals and organisations than the offline world. An individual is more likely to leave a trace of their activity online than they are offline; for example, someone is more likely to be challenged over a post they have made on social media than a conversation they have had in the street.

The organic nature in which regulation has developed has led, in some circumstances, to variation in consistency and harmonisation; however, it has broadly worked well, establishing a balance between innovation and rights of redress. Furthermore, it has allowed for the development of the UK's digital economy, to the point where we are a world leader in terms of innovation and the digital economy. The regulation of the internet is a highly dynamic area, shaped constantly by user expectations as well as by policymakers and the industry itself.

ISPA believes that a combination of legislation and self-regulation is most appropriate for the future regulation of the internet. ISPA would also suggest that any regulatory intervention should adhere to the following principles:

- There should be a presumption in favour of the regulation of people by laws of general application.
- Regulation should ensure that offline and online conduct is regulated in an equivalent manner: what is illegal offline should be illegal online. Legality should be applied to the same degree online and offline and nothing that is legal offline should be considered illegal online.
- Regulation should be targeted at the most appropriate part of the internet value chain.
- Regulation should balance the rights of providers and users (while recognising that more than one provider and more than one user can be involved in single online interactions).

4 The E-Commerce Directive

(Q2) What should the legal liability of online platforms be for the content that they host?
(Q9) What effect will the UK leaving the EU have on the regulation of the internet?

Since its inception in 2000, the E-Commerce Directive has served both the public and the industry well with a robust and flexible legal framework. There is currently a live debate about what the nature of the regulation of the internet should be following Brexit and ISPA is eager to make constructive contributions to this debate wherever possible; however, we would caution against diverging significantly from the guiding principles of the Directive which have struck an appropriate balance between the competing considerations at play.

The 'mere conduit' definition in the Directive provides important protections for internet access providers so that they are not inadvertently brought into the scope of legislation targeted at hosting providers. The hosting protections in the Ecommerce Directive provide important safeguards for hosting providers that host the content of third parties. Furthermore, Article 15 of the Directive states that EU Member States cannot impose a general monitoring obligation for internet intermediaries. This means that intermediaries do not have to monitor the information which they transmit or store, nor actively seek indications of illegal activity being undertaken. In order to safeguard both ISPs and user rights, it is important that such protections provided under the Directive are preserve and incorporated into UK domestic legislation.

ISPA would stress that, when drafting legislation that affects operators along the internet value chain, the legislator should adhere to the categories described in the E-Commerce Directive and target any intervention at the entity with the highest degree of control. There is a legitimate case to look at the management of content; however, ambiguity in terminology in this area can lead to an uncertain situation in which other parts of the internet value chain or content types can be inadvertently brought into the scope of content control regulation. The voluntary approach to tackling harmful content, for example, could be addressed through Government's Social Media Code of Practice which ISPA hopes will entail robust policies on tackling harmful content and will be implemented and enforced consistently but also transparently.

Brexit provides an opportunity to make advances in this area at a pace at which is not possible at EU-level; however, we must be careful to maintain the fundamental protections afforded to both users and service providers by the E-Commerce Directive. The Government's commitment in the Digital Charter to make the UK the safest place to be online is commendable and something that our members are keen to support; however, given the need to make the UK an attractive location to do business after Brexit, there must be consistency with existing legislation. There is a danger that, if future regulation in the UK becomes significantly more stringent than that in other jurisdictions, the UK economy will be put at a disadvantage. As such, cooperation and collaboration with international partners could prove more effective and elicit a more positive result for the UK.

5 User Rights

(Q5) What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

In recent years, online content control mechanisms have been developed which go well beyond mere removal-at-source and access blocking. However, the E-Commerce Directive does not prescribe the functioning of notice and action mechanisms. Such mechanisms are founded on proactive content monitoring and are increasingly used for both mandated and voluntary content control. Furthermore, these mechanisms often depend upon the use of automatic detection technologies, as recommended in the European Commission's guidelines on tackling illegal content online.

In this situation, intermediaries find themselves being forced to act as both 'judge' and 'jury' in implementing enforcement and adjudicating disputes. This threatens to significantly undermine the rights of not only the user posting the content but also the user who may find the content harmful and the user accessing the content who does not find the content harmful.

Alongside this trend, in recent years, we have witnessed the ascent of non-judicial authorities both in the UK and the EU. These publicly funded entities act as a proxy for court oversight; they actively search for harmful online content and notify Internet Service Providers (ISPs) of the existence of such content,

before recommending 'voluntary' removal. These non-judicial authorities enjoy the status of 'trusted flaggers': entities that not only make complaints about content but also make decisions about whether those complaints are well-founded.

Trusted flagging mechanisms have been found to work well in certain unique contexts; for example, the Internet Watch Foundation (IWF) has enjoyed significant success worldwide in identifying and removing child sexual abuse content. However, the unique nature of child sexual abuse material means that there is rarely ambiguity relating to its identification and illegality. The extension of the trusted flagger mechanism beyond clearly identified and bounded forms of content is unlikely to result in the same successful outcomes; this is due to the difficulty in accurately identifying illegal content without the assistance of a judicial process. Non-judicial competent authorities cannot be expected to have the same impartiality, legal expertise and interest in balancing competing rights as judicial authorities; as such, the fact that trusted flaggers are can submit takedown requests and order the suspension of domain names poses a threat to the rights of both individuals and organisations.

ISPA maintains that intermediaries should not be asked to be judge and jury and that notices should be filed by competent authorities, ideally a court or other independent and impartial body qualified and with legitimacy to make these kinds of decisions. We recognise the difficulty in having a court-based system provide an opinion on each and every incident, but we feel that this is an area worth exploring and there may be viable options available. Furthermore, content control mechanisms should always respect due process and be backed by some form of statute, with removal-at-source as the default content control measure, with access blocking to be used as a targeted and temporary resort in certain circumstances. If trusted flagging mechanisms are used, clear standards and rules should be provided by the Government in order to avoid the infringement or rights.

6 Conclusion

ISPA welcomes the Committee's exploration of internet regulation and the acknowledgement that more can be done to ensure the internet is regulated in an effective, proportionate and transparent manner. However, as highlighted above, this is an intricate policy area in which any single change carries the potential to have a negative knock-on effect all the way down the internet value chain, and throughout the economy. Given this, ISPA would suggest that any regulation is strongly rooted in the principles and protections of the E-Commerce Directive, particularly Article 15, and must be carried out with the utmost caution and clarity. In addition to this, user rights must be safeguarded against being undermined by intrusive content monitoring obligations and the rise of intermediaries being forced to act as judge and jury; thus, bypassing due process.