Response to CMS Committee Online Safety Inquiry

Introduction

The Internet Services Provider's Association is the trade association for the internet industry in the UK. ISPA has over 200 members from across the sector, including a large number of access provider ISPs from small to large, content platforms, hosting providers and others. ISPA therefore works across the areas in which the Committee is looking and we welcome the opportunity to provide input into the Committee's inquiry.

We believe that the Committee's terms of reference for the inquiry identify the key issues that are currently of relevance in relation to online safety. However, we would like to emphasise that the issues that have been identified should not be conflated. The issue of tackling child abuse content, which is clearly illegal, requires a different response from industry and Government than the availability of extremist material which may or may not be illegal. Protecting children from accessing potentially harmful content again requires a different response as it may cover content that is clearly legal but simply not appropriate for children and young people under 18.

We further welcome that the Committee considers that any potential dangers of the internet are a "correlation of the immense benefits provided by unimpeded communication and free speech" and that "any attempts to mitigate harms have to be proportionate and, where possible, avoid disadvantageous consequences." We believe that the recognition of this correlation is of vital importance but are concerned that policy-makers sometimes disregard it which often leads to disconnected and potentially harmful policy-making.

Variety of Internet companies

It is important that the Committee understands that there is a considerable diversity of companies that operate internet services. When considering the steps that industry can take, it is important to consider that each type of company may be playing a different role, and they will have varying degrees of ability to deal with potentially illegal or harmful content. The below description provides a rough guide[1] to the various kinds of companies that are involved in making the Internet work. If it were felt to be helpful, we would be happy to brief the Committee in more detail about the position of each company type in the internet value chain.

Access providers

Access providers are commonly referred to as Internet Service Providers. They connect customers to the Internet – either through fixed or wireless connectivity. As the ISP does not initiate or modify their users' communications and is only passing traffic across a network, they are deemed "mere conduits" under the E-Commerce Regulation 17 which grants limited liability.

[1] We merely consider the e-Commerce Regulations and online companies may have duties and defences through other legislation.

Hosting providers

Hosting providers store others' content online, often for a charge. Traditionally hosting providers have hosted complete websites of individuals and companies and even Government hosts some of its websites with these private hosting providers.

More recently, new types of hosting provider have emerged. These providers, e.g. social networks, generally provide a platform on which users can upload content (videos, blog posts, images etc.) which they themselves have created. These kinds of hosting provider do not have editorial control over what is posted on their services, but may have active or passive moderating policies that allow them to remove content or restrict its availability.

Under Regulation 19 of the e-Commerce Regulations both traditional and modern hosting providers are not considered to be liable for the content they host as long as they do not have actual knowledge of unlawful activity or information. However, upon obtaining such knowledge, hosting providers become liable if they do not act expeditiously to remove or to disable access to the information.

Websites where operators have editorial control

Individuals, companies and other organisations that run their own websites can be regarded as having editorial control over content that is available via their website and so are considered to have more direct responsibility. However, it is important to point out that websites can contain both content where the operator of a website has editorial control, e.g. a news article, and user generated content, e.g. comments about that news article.

Search engines

Search engines index web pages by scanning the Internet. They use algorithms to display relevant results based on what search terms users input but generally do not exercise editorial control over the links that they present to users. Search engines can be considered as "cachers" under Regulation 18 of the e-Commerce Regulations and act expeditiously to remove or to disable access to any information if they are made aware of that the fact that this information may be illegal.[2]

How does this apply in the real world?

It is worth considering three different examples:

1. A website hosting child abuse images
2. A person who posts a potentially illegal message on a website operated by the same person
3. A person who posts a potentially illegal message on a forum operated by a third party

In relation to the first example, ideally the hosting providers who provides the space for the website should be notified that illegal material is being hosted on a website on one of its servers. This notification is being done on a regular and effective basis by the IWF. If the operator is based

[2] Regulation 18 defines providers as "chashers" if the information that is processed by them is "the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request", i.e. the provider merely processes information and only stores it temporarily.

outside of the UK and responds slowly or not at all to a notice from the IWF or its international partners, the IWF can add this page to its list of illegal websites. Access providers accept the judgment of the IWF, which has great expertise in this area, and use the IWF's list to filter out the relevant page (i.e. they make the URL of that website inaccessible, and a user would see an error message if they attempted to access it).

In relation to the second, the person should be approached directly as they have editorial control of the comment and the website on which it can be found. If the person does not respond then it may be necessary to contact the hosting provider who provides the space for the website who may then need to make an expeditious assessment of the content and take it down if appropriate. The access provider would theoretically be able to block access to the website but this would be less timely and cost efficient than approaching the hosting provider and generally requires a valid takedown notice.

In relation to the final example, again, the person who posted the content should be approached directly. However, if the person does not respond, or cannot be identified, the third party who operates the forum should be approached who will then need to make an expeditious assessment of the content and take it down if appropriate. If the third party does not react then it may be necessary to approach the hosting provider, however, this should be a matter of last resort as the provider would generally only be able to remove the whole forum, thereby curtailing the service and rights other forum users. The same would be true if an access provider would block access to the forum.

In all these examples it is important to note that it is often not clear cut whether content is illegal or not and online companies cannot be expected to be the judge and jury of others' content.

Industry has a role to play

We strongly believe that the industry has a vital role to play in protecting minors from accessing inappropriate content and would like to emphasise that the UK is widely regarded as having one of the most advanced online safety frameworks.

Family friendly filters

- The main consumer facing ISPs are moving to system where new and existing customers are presented with an unavoidable choice of whether to apply filters or not. These filters cover the whole home, i.e. apply to all the devices used on a connection, put users in control and allow parents to choose from a list of content that should be filtered including adult content, extremism and self-harm. This has involved significant investment, both financially and time.
- Some smaller consumer-facing providers are considering solutions that offer family friendly filters but can be deployed on smaller scale and at lower costs. ISPA is currently discussing this issue with its members.

Child sexual abuse content

- ISPA and many ISPs have helped to setup the IWF and have consistently supported the organisation which is considered to be world class in preventing people from access child abuse content and facilitating the removal of that content at source.
- Many ISPs have committed to increase funding of the IWF to enable a proactive remit to identify and remove child abuse content online. Further funding for education and awareness campaigns from industry has been forthcoming.

Allegedly/potentially illegal content

- Industry has worked with the Home Office and law enforcement regarding the Counter-Terrorism Internet Referral Unit (CTIRU) which members of the public can report potentially unlawful terrorist material from the internet. If hosted in the UK the content is removed and this framework is underpinned by the Terrorism Act 2006. So far approximately 6,500 pieces of online content have been removed through CTIRU action.[3] However, what constitutes terrorist material is not always clear cut.
- Providers of social media platforms and websites that contain user generated content will remove illegal content whenever they are made aware of it and can apply their terms and conditions to other types of content that may not be illegal. They also often provide their consumer with report facilities to flag up any inappropriate behaviour.
- Providers have been working alongside Government and Parliament to reform the defamation law to ensure that online freedom of speech is adequately balanced with the right of those who feel they have been defamed online.

Industry cannot solve these issues on its own

However, we are concerned that the current policy debate is sometime too strongly focused on finding a technological fix to a problem that often has societal roots and is sometimes present in both the offline and online world.

For example, in the relation to the accessibility of adult content, we accept that ISPs should play a role in empowering their customers to better determine what content should be available in their household. However, even the most comprehensive filtering solution cannot guarantee that adult content will be unavailable. Over and underblocking of content is inevitable and it is important that filtering tools are viewed as part of a wider package alongside education and parental mediation. There needs to be more emphasis on enabling parents and teachers to teach children how to behave responsibly online, one possible action could be the updating of sex education in the curriculum so that it keeps pace with technological and societal developments.

In relation to abusive or threatening comments online, we would like to emphasise that ISPs should not be used as proxy for enforcing the law and perceived societal standards. Social media networks can and often take action against users that behave inappropriately. However it has to be taken into account that the Crown Prosecution Service's Guidelines on prosecuting cases

[3] HL Deb, 23 September 2013, c421W

involving communications sent via social media state that "[j]ust because the content expressed in the communication is in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage the criminal law." This should not be regarded as a get out clause for providers but it is important to point out that providers cannot be expected to go beyond what is required by the law. In this context, it worth highlighting that Parliament has recently amended the Defamation Act which encourages hosting providers to assist the resolution of disputes between users that cannot be resolved by the hosting provider themselves

Conclusion

We have shown that industry has made available a number of tools, services and advice to help protect minors from accessing adult content. There is cooperation between industry and law enforcement to tackle extremist material when legal thresholds are crossed. Websites have in place mechanisms to prevent abusive behaviour and the law had been used to prosecute individuals in some instances.

The Internet has had a significant impact on modern societies. It has changed how we do business, communicate, educate and consume content. These changes came about because internet companies developed innovative products and consumers have found even more innovative and sometime unexpected ways of using these products. As such the Internet is an extension of the established offline world and it would be wrong to simply ask ISPs to fix any issues that may arise.

Technological fixes can play a role and support customers but we will only be able to comprehensively tackle the problems that the Committee outlined in its terms of reference by involving industry, Government, parents and users and by looking at both the symptoms and causes. The Internet industry has reviewed and improved its offering to customers in recent times. It is willing to actively engage with the online safety agenda but we hope that this can be done in a more positive environment based on collaboration.