[COR0174]

Written evidence submitted by The Internet Service Providers' Association (ISPA) (COR0174)

1. The Internet Service Providers' Association (ISPA) welcomes the opportunity to respond to Home Affairs Committee inquiry into COVID-19 and online harms.

2. 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. 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 the full ecosystem including communications providers that serve consumers and businesses, those that build their own networks and those that resell services via the fixed and wireless networks.

3. Summary of key points
   - ISPA's members played a key part in supporting the COVID-19 response, by keeping their networks running, navigating the shift to widespread remote working and online living and by providing additional help to vulnerable consumers as well as priority support to the NHS and the care sector.
   - Telecoms sector staff were the target of both verbal and physical attacks that were fuelled by COVID-19 conspiracy theories online.
   - The online harms proposals need to be mindful of changes in technology and internet standards to ensure that the regulatory framework for online services remains effective.

The broadband sector's response to COVID-19

4. Throughout the COVID-19 crisis, the internet has become an even more integral part of UK society with more businesses moving their services online and families staying in touch remotely across multiple generations. In many ways, the nation's response to COVID-19 has shown that the internet overall has a truly transformative and positive impact that clearly put a dampening force on the economic and societal impact of Covid-19. Digital connectivity has helped to combat social isolation and maintain a high level of economic activity in those sectors of the economy that allow for home working. Crucially, the internet also enabled Parliament to continue scrutinising and supporting the Government's response to COVID-19 and it allowed for continued interaction between Parliament, constituents and the media.

5. Our members have played a key role in supporting this, by keeping their networks running, navigating the shift to widespread remote working and online living and by providing additional help to vulnerable consumers as well as priority support to the NHS and the care sector.[1] Our members have been working flat out to maintain network

[1] An outline of these commitments can be found in the following Government announcements:
- Connectivity boost for vulnerable consumers and NHS staff

performance, keeping the economy moving and families connected with loved ones. This involved managing network demands, fixing faults and continuing to update and rollout networks to those who need them. Crucially, this required staff of telecoms companies to continue work out in the field, e.g. maintaining cabinets or cables, or travel to work office buildings to keep up customer support and call centres. While employees in the telecoms sector were classed as key workers, concerns were still raised by members of the public, the media and even politicians. We are currently running the Keep Britain Connected Campaign which highlights some of the work that our members have been doing in response to the crisis.[2] Additionally, organisations such as Internet Matters, which have provide additional advice to parents on how to keep their children safe as they spend more time online due to home schooling.

The Impact of misinformation on telecoms companies and key workers

6. The majority of public concerns around telecoms sector employees working during lockdown stemmed from a lack of awareness of the relevant COVID-19 guidance. However, our members have also reported a significant increase in both verbal and physical abuse of their workforce that have been fed by online rumours around a link between 5G and COVID-19.[3]

7. This highlights misinformation as one area of the online harms agenda that can have a clear real-world impact. This becomes especially relevant if this misinformation encourages types of behaviour that affect third parties or society as a whole, e.g. as shown in abuse of telecoms sector staff and the burning of broadband cabinets. Effectively combatting misinformation online requires a combination of work from Government, online businesses and civil society.

8. While Government and the police took an active interest in this area and were actively combating levels of misinformation, the incidents that our members have experienced clearly show this is an area that requires further work, including support from parts of the online value chain where misinformation is spread. As with other internet and policy interventions, we believe that any intervention should take place at a level where the degree of control over online content is greatest (starting with the user, incorporating online platforms and, as a measure of last resort, broadband providers).

Other points of concern: Keeping up with international developments

9. Looking beyond the issue of misinformation, we would like to flag that the concept of broadband providers playing a role in the filtering and blocking of content is coming under pressure from a number of developments in the area of internet standards. In general, we believe that the primary responsibility for removing content should lie with the platforms on which this content is hosted. Blocking and filtering has previously been used either as a last resort measure when other online harms interventions have failed or in the context of parental controls that are offered on a voluntary basis.

- Government agrees measures with telecoms companies to support vulnerable consumers through COVID-19

[2] More information can be found here.

[3] Case studies of how ISPA members and their staff have been working throughout COVID-19 can be found here, including some that outline the impact of public abuse.

10. However, blocking and filtering are becoming increasingly undermined due to changing internet standards. The most well-known development in this context is the rising popularity of DNS-over-HTTPS (DoH)[4], as well as other standards which essentially encrypt different parts of the internet architecture. ISPA generally supports moves to increase security and privacy within the internet architecture, but some of proposed approaches for implementation would prevent ISPs from being able to fulfil their envisaged role of last resort enforcement.

11. We encourage Government and the Committee to investigate how the online harms agenda can be implemented in such a way that it is compatible with the evolving nature of internet standards. This could require:
    a. an extension of blocking obligations to other parts of the value chain (e.g. if DoH was implemented in such a way that DNS resolution is moved away from the current decentralised approach)
    b. an obligation on online platforms and other parts of the value chain to proactively and explicitly consider the impact on user choice, safety and privacy in the development and implementation of internet standards and ensure that there is constructive level of consultation and assessment of all intended and unintended consequences.
    c. Powers in the online harms bill to ensure that platforms respect user choices and preferences when relevant changes are implemented (e.g. user-opt-in rather than opt-out).

12. Some of these points could be implemented throughout the online harms bill while other would require work both in the UK and at international level, e.g. in relation to standards.

Conclusion

13. COVID-19 has clearly demonstrated that, like most other inventions, there are both negative and positive elements to the internet. Online services and broadband providers have played a key role in keeping (large parts of) the UK going throughout the crisis. At the same time COVID-related conspiracy theories had a clear and harmful impact on telecoms sector staff. The online harms bill would provide an avenue to ensure that Government and industry can better react to similar future incidents. There is clear need to ensure that the future regulatory approach is mindful of the changes in technology and internet standards to ensure that the regulatory framework for online services remains effective.

May 2020

[4] DNS is a crucial part of the internet architecture. In layman's terms, it provides an address book function for the internet and helps to translate (human) word-based queries into numbers that locate websites and other resources online. DNS-over-HTTPS encrypts the resolution of DNS queries and, depending on the implementation, also centralises resolution/translation processes.