[COR0171]

Written Evidence submitted by BT Group (COR0171)

1. BT Group

1.1 BT Group (BT, EE and Plusnet) offers fixed, mobile and public wi-fi connectivity; mobile phones, tablets and mobile broadband devices; and online TV content via set top boxes. Children may access and use our products and services for example via his/her parent: nearly a third of our broadband customers are households with children, and children may use their parents' mobile devices or be given one of their own.

1.2 During the Covid-19 outbreak our focus at BT has been on standing by the country – connecting the new Nightingale Hospitals, helping isolated patients speak with their loved ones, making sure our networks perform to keep everyone working and entertained, offering help to vulnerable customers and support to small businesses that face the challenge of a generation.

1.3 BT has also continued working to make the internet a safer place while respecting personal freedoms, offering free technology tools, supporting online safety education and awareness, and working in partnership with charities, government, and others. Please see the Annex for more information.

2. Online Harms

2.1 The internet has been overwhelmingly positive and empowering, connecting people and information they would not have had access to before. However, we recognize that trust is under threat from a range of potential online harms including child sexual abuse, terrorism, bullying, self-harm, hate speech, sexual and violent content, gambling, and fake news/misinformation. Children are particularly vulnerable to many of these harms particularly when they are spending increasing amounts of time online due to the Covid-19 breakout. In addition, there are economic harms caused by fraud and IP and copyright infringement and broader concerns about the size and power of some online platforms.

3. "Mere conduit" and working with the Internet Watch Foundation

3.1 BT is obliged to protect the confidentiality of its customers' communications. We are a network provider whose role is to deliver our customers' content from A to B. The legal term is a "mere conduit". So we are different from social media platforms such as Facebook or Youtube who can see their customers' content, and for whom being able to do so is an intrinsic part of their business model. What we know about what passes over our networks, and what we can do about it, is limited. We have no legal right to see content, as to access that content could amount to an unlawful interception. It's a bit like the postman opening your letters. Therefore, this makes it difficult for us to determine the nature, prevalence and scale of online harms passing over our networks.

3.2 However, we do work closely with the Internet Watch Foundation (IWF) who notify us of child sexual abuse URLs to block. The IWF have established that during the current crisis, the IWF's list of URLs has remained static at around 5,700 URLs[1]. The IWF have also found that although they have not yet seen an increase in public reports of child sexual abuse on the internet during the Covid-19 outbreak they are concerned that *"all the indicators prior to the*

[1] https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20response%20to%20HASC%20inquiry%20into%20the%20preparedness%20of%20the%20Home%20Office%20for%20Covid-19.pdf

pandemic show that this is an issue which is significantly on the rise and the child protection sector is bracing itself for further increases in cases during the current pandemic and once restrictions are lifted"[2].

3.3 The majority of websites are now encrypted using "Hypertext Transfer Protocol Secure" ("HTTPS"). HTTPS can commonly be seen as a prefix to many popular websites. Whilst many welcome the extra security and privacy that this brings, it does mean that the number of websites on which BT's blocking technology can operate will decrease. BT or any ISP cannot break the end to end encryption of HTTPS in order to examine the URL or object that is the intended destination, therefore the IWF does not place HTTPS URLs on their blacklist.

3.4 The IWF have found that the *"vast majority of child sexual abuse imagery we find is linked to darker places of the internet, hosted in countries outside of the UK, on platforms not commonly known about"*. However, the IWF operates on the open internet, not on messaging services like Facebook Messenger or WhatsApp which are encrypted person-to-person communications. The NSPCC[3] and the Home Secretary[4] have expressed concerns that moves by social media platforms to more encrypted communications will see an increase in the sharing of child sexual abuse across these encrypted platforms. Recent figures uncovered by the NSPCC showed that, of over 9000 instances where police in England and Wales know the platform used in child abuse image and online child sexual offences, 22% were reported on Instagram and 19% on Facebook. But only 3% on WhatsApp, a platform that already has end to end encryption, suggesting that encryption is a barrier to reporting and investigation child sexual abuse crimes.

3.5 The implications of the rise in encryption on websites, services and browsers and how policy makers might engage with this is discussed in more detail in section 6.

4. Covid-19 misinformation and 5G

4.1 There has been an increase in online misinformation linking Covid-19 to 5G technology. As a company that currently operates the UK's largest 5G network, misinformation around Covid-19 is having a material, real world, impact on the UK's digital infrastructure and the BT staff and subcontractors who work to maintain it. Since the UK entered full 'lockdown' on 23rd March, there have been 36 separate incidents of arson, attempted arson and other forms of sabotage on mobile masts delivering services to our customers. These have included incidents involving petrol bombs. We believe the number of attacks on sites operated across all four mobile network operators to be approaching 102 over the same period. Very few of these attacks have been on 5G sites, but they have generated well over 2500 complaints from EE customers mainly about levels of service e.g. calls dropping, slower download speeds. 19 attacks took place near critical infrastructure, such as fire, police and ambulance stations. There have been significant concentrations in the Midlands and in and around Liverpool.

4.2 While incidents of arson have attracted a great deal of media attention, we are also very mindful of the increasing trend of threatening, intimidating and violent behaviour towards staff who are working every day to maintain the digital infrastructure that we are all relying on to live our daily lives. There have now been almost 140 separate incidents involving EE staff and subcontractors alone. These have included threats to kill and vehicles driven directly at staff. We believe the number to be significantly higher when staff at Openreach, its competitors and

---

[2] https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20response%20to%20HASC%20inquiry%20into%20the%20preparedness%20of%20the%20Home%20Office%20for%20Covid-19.pdf

[3] https://www.nspcc.org.uk/what-we-do/news-opinion/facebook-encryption-sexual-abuse/

[4] https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

staff at other mobile networks are considered. It should go without saying that violence, threats, arson and other forms of vandalism are in all circumstances completely unacceptable.

4.3 Our analysis suggests that many of these incidents are in response to unsubstantiated conspiracy theories relating to the perceived harm that 5G masts cause to health, or a perceived relationship between 5G and spread of Covid-19. We note Ofcom's recent confirmation of the lack of evidence for there being any grounds for concern. Their testing programme has shown that 5G sites are operating at a fraction of the radiation limits set by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). Ofcom's maximum measurement for any mobile site was approximately 1.5% of those levels – including signals from other mobile technologies such as 3G and 4G. The highest level from 5G signals specifically was 0.039% of the maximum set out in the international guidelines.

4.4 Beyond this, we do not believe these attacks to be the result of a co-ordinated effort by a specific organisation or organisations. However, we do believe that content shared via social media platforms is playing a significant role in inciting individuals to commit these acts. To date, BT has identified at least 68 specific items of content and/or accounts on Facebook, Youtube and Twitter that, in our view, may have either incited or helped to facilitate these attacks and associated behaviour. We have supplied full details of them to these companies. We have welcomed some platforms approaching us proactively to discuss the steps they are taking to assess and where possible remove this content. We have also worked closely with relevant DCMS officials. A substantial amount of concerning content is also hosted on websites operated independently by groups and individuals associated with this activity.

4.5 We also welcome several specific announcements that social media platforms have made in relation to the steps they are taking. In particular, Google's commitment to remove content from Youtube that links 5G with Covid-19, and Facebook's classification of false claims which link Covid-19 to 5G as misinformation which "can cause physical harm" and can therefore be removed, are valuable steps forward. Facebook have also told us that they are using machine learning alongside human review to remove this kind of content. We would encourage this approach to be used more widely.

4.6 In parallel though, we believe there is scope for greater clarity around the fact that Covid-19 related 'fake news' will not be tolerated on these platforms and that existing efforts to allow users to distinguish between content that is factual and that which is clearly not will be extended. We also need to see further transparency from social media platforms as to how they assess the specific reports that we make in relation to Covid-19 misinformation, what standard of 'misinformation' must be met for a report from us to be acted on, and what proportion of reports they are prepared to take action on in the form of removal, ideally on a site by site basis. This would be hugely valuable in our ongoing efforts to combat the direct impact this misinformation is having on our ability to support the UK economy and wider society.

4.7 We would suggest there is potential to take further action against 'troll' accounts across social media that are promoting disinformation of this nature. Twitter has, for example, undertaken deletions of such accounts before. We would like to work with social media platforms to address this and we are looking at how best to identify such accounts and flag them for removal.

4.8 We should add that we wrote to Julian Knight, Chair of the DCMS Committee on 29 April 2020 about this issue as part of the evidence session on Covid-19 misinformation.

4.9 In terms of adequacy of the government's Online Harms proposals to address issues arising from the pandemic, in our view the rapid rise of 5G conspiracy theories connected to the pandemic and these theories converting into real world harm show the limitations of a "self-regulation" or "regulator enforces the platforms' terms of use" approach to this kind of harm that

lacks a clear legal definition. It has taken a considerable amount of resource and effort from BT and other operators that were experiencing real world criminal damage to gather information on conspiracy theories being circulated online, and then using our relationships directly with social media companies, and with government, to ensure action was taken to remove the most damaging of these stories.

4.10 In our view, a successful regulatory regime should not require the resources, expertise and relationships of several large companies in order to rapidly identify and remove harmful content. BT has found it difficult and labour intensive to ensure such content is comprehensively identified and removed.

4.11 This suggests that a similar framework would be very difficult for smaller organisations or individuals that are the subject or victim of conspiracy theories to get harmful content removed and ensure that future postings of similarly harmful content are pro-actively identified and prevented from being posted, or rapidly removed.

5. Online safety advice during Covid-19 outbreak

5.1 We welcomed the recent publication by the government of online safety advice during the Covid-19 outbreak e.g. “What you can do to stay safe online during the coronavirus (COVID-19) outbreak”; “keeping children safe online” and “fraud and cyber-crime”. Providing people particularly parents and children with the necessary skills, education and awareness is vital to help build online resilience against online harms.

5.2 As part of our BT Skills for Tomorrow programme, we are committed to helping parents, teachers and young people develop the skills they need to navigate the online world safely. We have an ambition to help 10 million people in the UK develop the digital skills they need to make the most of life by 2025, including five million children. Our work includes helping families and children to become empowered digital citizens who know what it takes to keep safe and protect their data online and we have a range of support available through our Skills for Tomorrow portal www.bt.com/skillsfortomorrow. This includes resources for parents developed by our partners Internet Matters (who are funded by ourselves and other ISPs and technology companies) to help parents keep their children safe online through expert support and practical tips. Through our Barefoot Computing programme in partnership with Computing at School we provide free resources for primary school teachers to help them deliver the computing curriculum brilliantly, including online safety. Under this programme we have also launched a series of Top Tips on Tech ad breaks on ITV during the Covid-19 outbreak which includes videos on online safety for kids and how to avoid phishing.

6. BT view of Online Harms White Paper

6.1 We welcomed the direction of the Online Harms White Paper and the government’s response to the White Paper published in February 2020 although we note that this was an initial response. Once the urgency of the Covid-19 breakout has passed we need the government to press ahead urgently with the next phase to introduce the legislation.

6.2 We support the proposed duty of care on social media platforms, and the move towards specific and targeted monitoring established by a clear legal framework. As an ISP we are willing to play our part in an enforcement regime, up to and including blocking sites or content, as a last resort – provided the decisions about what to block are made by an independent regulator with a clear legal process and right of appeal.

6.3 However, more work needs to be done to develop the detail of the future online harms regime as there are currently multiple processes and pieces of legislation addressing different aspects of online harms, from social harms to piracy, fraud, data, and cyber security.

6.4 We would like to see a single, coherent and consistent framework. While we can understand that it might be difficult for the government or the regulator to prescribe a single definition of content currently described as 'harmful but not illegal', we do think it is reasonable to empower the regulator to set principles and illustrate in case studies [working in consultation with the industry] how these 'harmful but not illegal' categories of content should be first identified and then dealt with by platforms.

6.5 A starting point could be for the regulator to establish codes of practice, through consultation with wide range of stakeholders, that content platforms would have some freedom to interpret through their terms of use and community standards, but would also ensure platform users have clarity and some consistency between platforms on how 'harmful but not illegal' content is dealt with. However, we also believe the government should consider giving the regulator powers to go further. In particular, where the regulator receives complaints from the subjects or victims of harm they should be empowered to investigate a platforms' approach to the relevant content and if necessary they should be able to impose meaningful sanctions, including requirements for immediate and ongoing corrective action, as well as appropriate remedies for the victims. We would also like to see the transparency reporting requirements imposed by the regulator address our concerns relating to Covid-19 misinformation and 5G, as described in 4.9.

6.6 We also believe that the regime legislation should include economic harms, including fraud and content piracy.

6.7 We welcomed the approach to private communications as a separate category. We believe that users would have a legitimate expectation that what they communicate privately should remain so, almost all of the time, mimicking the offline world. It could be difficult to define what is public versus private communication but not, in our view, impossible. So where the communication itself is public (so visible to any service user) or where the company hosting the communication is routinely gathering data from the contents of it in order to sell that data, or sell a service based on that data, it should not be considered to be private. A specific set of obligations for private and encrypted services could also be developed, including:

- an obligation to seek out and remove or prevent the most harmful types of content, which would obviously include child sexual abuse material;
- transparency with law enforcement around what operators find through monitoring of their platform;
- and an obligation to remove encryption when directed to do so by law enforcement, under the Investigatory Powers Act frameworks.

6.8 As outlined above in section 3, the current issue in the most serious of online harms such as child sexual abuse is that as the online world becomes increasingly encrypted, both messaging services such as WhatsApp, Skype or Signal, or within browsers themselves, the existing set of tools to identify, investigate and prevent access to the most harmful kinds of content becomes less effective. Private messaging, and the very fact of encryption cannot be left out of the regulatory regime.

6.9 There are valid arguments about the protection that encryption technology can provide to those communicating with each other under oppressive regimes, as well as the benefits for securing financial and other legitimate transactions online. But it is also well evidenced that end to end unbreakable encryption will facilitate the sexual abuse of children. Recent figures uncovered by the NSPCC showed that, of over 9000 instances where police in England and Wales know the platform used in child sexual abuse images and online child sexual offences, 22% were reported

on Instagram and 19% on Facebook. But only 3% on WhatsApp, a platform that has end to end encryption.

6.10 The right regulatory approach is not one which prioritises one group over the other, but one which finds a framework that balances a general expectation of privacy with an imperative to both prevent and prosecute these most serious of crimes within an appropriate legal framework which is limited and includes the right to appeal and so forth.

6.11 The tech industry is proceeding at pace to create private, encrypted and unregulated spaces as well as end to end encryption of messaging and application services. For example Mozilla (Firefox) and Google (via Chrome) are rolling out encrypted domain name service (DNS) resolution in their browser (DNS over HTTPS). Furthermore, Microsoft are starting testing of DNS over HTTPS options for Windows 10. BT welcomes the current intentions of Google and Microsoft to only automatically upgrade customers to DNS over HTTPS if their existing DNS provider supports it. This should reduce the impact to existing ISP DNS based content filtering. However, if they change deployment approaches in the future or couple with additional encryption standards, the effectiveness of network-based content filtering solutions may be reduced. So we also need legislation in a form that can anticipate these and other future technological developments.

6.12 We do not believe the choice is one of allowing encryption or not, rather that services which are encrypted or offer encryption should come with a specific set of obligations to enable both investigation into crimes, and to prevent the circulation of the most harmful of content. These obligations would fall on the service provider that holds the user or customer relationship and could be as set out above (in para 6.7). Or, for intermediate services such as VPNs or browsers, a back-stop obligation to ensure they are <u>not</u> providing a route to circumvent the UK regulatory regime, and be able to evidence this. One route to this is to pro-actively enforce the ICO's Age Appropriate Design Code, to make sure these services understand they are in scope, and to regularly ask them to evidence how they are complying with the Code.

6.13 Once the urgency of the Covid-19 outbreak has passed the government needs to make legislative space available and all political parties should aim to use all the available modes of legislative and pre-legislative scrutiny to flush out whatever industry criticisms and anxieties exist, and get the detail right and to provide the greatest political legitimacy to any future online regulator so it can prevent and address online harms.

[COR0171]

Annex

How BT is working to make the internet a safer place for children

BT Group (BT, EE and Plusnet) offers fixed, mobile and public wi-fi connectivity; mobile phones, tablets and mobile broadband devices; and online TV content via set top boxes. We do not offer products and services directly to children but children may access and use our products and services for example via his/her parent.

We are working to make the internet a safer place for children by offering free technology tools, supporting online safety education and awareness, and working in partnership with charities, government, and others. Further information is provided below.

Preventing access to inappropriate and illegal content

Parental Controls

- We promote a large variety of free parental control tools (network and device) for home and mobile, public wi-fi, and on demand TV content. We also offer and promote tools to protect against cyber-crime and security threats.
- BT Parental Controls cover all devices e.g. laptops, smartphones connecting to the internet via the BT Home Hub, and remain in place outside the home when using BT Wi-fi hotspots. Parents can select their level of filtering (light, moderate or strict) and can customise it depending on the needs of their family e.g. setting the time for when filtering comes on e.g. homework time. We use expert third party companies to create the 16 content categories for Parental Controls and review them frequently to make sure all sites are categorised appropriately. Parents can see the list of what content categories will be blocked by filter level, and they can customise further by selecting Custom and selecting each blocking category they want to change.
- EE is a founding signatory to the UK mobile operators' code of practice for the self-regulation of new forms of content on mobiles which requires mobile operators to offer an internet filter to protect customers under the age of 18 from age inappropriate content. The mobile operator sets its filter in accordance with a framework prepared by the British Board of Film Classification (BBFC).
- We are a signatory to the "Public Wi-Fi Statement" which commits main Wi-Fi providers to provide filtering of pornographic material where children may be present e.g. shopping centres, BT Wi-fi offers site partners e.g. hotels BT Wi-fi Protect a free product that allows site partners to restrict access to pornographic content.

Child sexual abuse (CSA) images

- We block access to CSA images. We are notified by the Internet Watch Foundation (IWF) of which images and sites to block.
- Our customers don't have to take any action to block these images – nor can they unblock access to it. We do this voluntarily to protect children.
- We were the first communications provider to develop technology to block these images when we introduced our blocking system, Cleanfeed, in 2004. Since then, almost all other communications providers in the UK have introduced similar technology.
- We are a founding member of the IWF and until recently had a seat on the IWF Board. We give a significant amount of funding each year to the IWF.
- In the past people attempting to visit blocked sites or images were shown a 404 page error indicating they'd not been found. Today we display a web page explaining that the site contains illegal child sexual abuse images and offering links to counselling services.

- Complementing this, we have a long standing relationship with law enforcement in the UK (e.g. via the Child Exploitation and Online Protection Command and the NCA) but also across the globe (e.g. via partnership agreements with Europol and Interpol).
- BT has submitted written evidence and attended a public hearing on the Independent Inquiry into how the internet facilitates CSA chaired by Professor Alexis Jay.

Supporting education and awareness

- As part of our BT Skills for Tomorrow programme, we are committed to helping parents, teachers and young people develop the skills they need to navigate the online world safely.
- We have a target to help five million children in the UK develop their digital skills by 2020, including helping them to become empowered digital citizens who know what it takes to keep safe and protect their data online.
- We are upskilling primary school teachers to deliver the computing curriculum through the Barefoot Computing programme (funded and managed by BT in partnership with BCS, Chartered Institute of IT) providing free resources and volunteer-led workshops to support teachers. As part of this programme our 'Safety Snakes' activity, created for us by a teacher and his pupils, helps teach young people about how to safely deal with situations they might come across online. The Barefoot programme has reached over 2 million children through c 78,000 teachers in primary schools across the UK.
- BT is also a founding member and funder of Internet Matters which was established in May 2014. Internet Matters creates content and resources to help parents keep their children safe online and get expert support and practical tips to help children benefit from connected technology and the internet safely and smartly. BT and the other three founding industry members will have jointly invested more than £10m by 2020. Last year Internet Matters had over 2.8m users, and almost 9 out of 10 parents report that they would recommend it to others.
- EE has trained staff in more than 600 EE retail outlets to help parents set up their children's mobile phones with the right controls to be safe.
- Our partnership with the Marie Collins Foundation is supporting children and their families who have been harmed and abused online, by delivering face-to-face training to more than 6,500 frontline staff under their Click: Path to Protection programme.
- We sit on the Executive Board of the UK Council for Internet Safety and worked with the Council, government and other Wi-Fi providers to develop and launch a family friendly Wi-fi logo that helps children and families identify 'Friendly WiFi' venues e.g. cafes, shopping centres that ensure that the public Wi-fi that they are accessing is filtered.
- We host the annual UK Safer Internet Centre's youth event at BT Centre (HQ) to promote Safer Internet Day.

BT privacy and free expression reports

Our reports provide more information about our approach to privacy and free expression online. They also describe how we help protect our customers from online harms, and shed light on the different legal obligations we may have with respect to customer data or access to online content.

An important function of these reports is to show how our business can affect human rights – especially privacy and free expression, and how we're working with governments, civil society and other stakeholders to manage this.

[COR0171]

May 2020