BT Group—written evidence (FEO0049)

House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online

BT Group

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.

BT has 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.

Key Messages

- We are supportive of freedom of expression, but that this needs to be appropriately balanced with supporting and protecting other rights online.
- Our commissioned Demos research suggests the public don't think the current situation on social media is getting this balance right.
- Given this, we think the approach to new legislation set out in the Government's full White Paper response to online harms is broadly the right direction of travel.
- We agree it is important to educate citizens, both to behave well online and not behave in a harmful way or post harmful content, and how to protect citizens from harmful content.

1. Is freedom of expression under threat online? If so, how does this impact individuals differently, and why? Are there differences between exercising the freedom of expression online versus offline?

Modern information and communications technologies have enabled unprecedented access to information and exchange of ideas, building bridges between people, geographies and language groups. This has improved many people's lives and has become even more essential in 2020: the ability to communicate in real time has proved essential during the ongoing global pandemic. Networked devices have allowed people around the world to continue working, studying and accessing essential services remotely. In parallel, connected hospitals and social care facilities have improved the quality and availability of healthcare, while industrial IoT have revealed new opportunities to manage natural resources more effectively and combat climate change.

However, the risks posed by harmful activity and content online are now well documented. Online harms such as harassment and content advocating self-harm have had a detrimental impact on children and adults alike. On a broader scale, social networks have proved vulnerable to manipulation through dis- or misinformation and critical infrastructure is increasingly subject to cyberattacks. The consequences – ranging from discrimination, exclusion and loss of trust to insecure elections, national security threats or the loss of life – cannot be minimised or overlooked.

BT support the right to freedom of expression – in parallel, we believe there is scope for greater clarity around the fact that harmful content (misinformation, abusive, suicide and self-harm and so on) will not be tolerated on platforms that enable users to share content, and that existing efforts to address this kind of content will be extended.

BT is a member of the Global Network Initiative (GNI)[1], a multi stakeholder initiative that brings together companies, civil society organisations and investors to tackle challenges around freedom of expression and privacy online. We are also members of Business for Social Responsibility (BSR)[2], and have supported research into how companies can adhere to international human rights standards when faced with contradictory domestic laws or practices[3].

Two fundamental differences in freedom of expression online versus offline are the speed and ease with which online speech can be amplified, and that expression and exchanges online are necessarily mediated by private networks and platforms. While governments around the world are working to determine appropriate mechanisms for regulating online platforms, other segments of the ICT sector, such as telecommunications infrastructure, are already highly regulated due to the critical role they play underpinning our increasingly digitised society. For example, communication service providers must have a proper legal basis to block or restrict their customers' access to content. At the time of writing, over-the-top service providers such as social media platforms remain primarily self-governed. Each platform's services are regulated through their own corporate policies or terms of service, which will differ from company to company.

As legal and regulatory frameworks are modernised to address the impacts and trade-offs described above, care must be taken to ensure policies intended to protect users don't infringe unnecessarily on their free expression, or transfer the burden of protecting fundamental rights onto individuals..

We thought it would be useful to the inquiry to share some latest research on online harms. BT commissioned Demos to carry out research to investigate public opinion on online harms, which was published in October 2020. The research involved a national representative poll of over 2,000 people across the UK, and included interviewing two focus groups of men and women who were asked their views about online harms, and how they considered and understood

---

1 https://globalnetworkinitiative.org/

2 https://www.bsr.org/en/

3 https://www.biicl.org/publications/when-national-law-conflicts-with-international-human-rights-standards

the trade-offs necessary to expand regulation of the online world. The results can be found here.[4]

The polling research asked two questions particularly relevant to this inquiry:

First, it explored the trade off between accessing content and preventing harm. 42% of respondents agreed with the statement '*people should be able to access everything that is written on the internet and social media, even if some of it is harmful*.' While 58% of respondents agreed with the statement '*people should not be able to access harmful content, even if some non-harmful content is censored as a side effect.*'

Second, it explored the trade off between freedom of expression and protection from harm directly: 35% of respondents agreed with the statement '*people should be free to express themselves online, even if what they say causes serious distress or harm to other people.*' While 65% of respondents agreed with the statement '*people should not be free to express themselves online if what they say causes serious distress or harm to other people*.'

Overall, we are supportive of the approach set out in the Government's recent full response to the Online Harms White Paper: to set out in legislation a general definition of harmful content and activity; and to require companies to set out what content is not acceptable in their terms and conditions, and then to enforce this effectively. Balancing this with plans to protect freedom of expression by giving users that have had content removed the right to appeal to the platform seems to us the right approach.

2. How should good digital citizenship be promoted? How can education help?

Given the difficulties of balancing protection of freedom of expression with the protection of other rights online, we agree that widespread public education which helps to create informed and empowered digital citizens has an important role to play.

A helpful framework for outlining key areas for digital citizenship education is the DQ (Digital Intelligence Framework developed by the DQ Institute). This framework sets out a comprehensive set of technical, cognitive, meta-cognitive, and socio-emotional competencies to help individuals harness the opportunities of digital life, focussing on 8 key areas:

1. Digital rights
2. Digital literacy
3. Digital communication
4. Digital emotional intelligence
5. Digital security
6. Digital safety
7. Digital use
8. Digital identity

---

[4] https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf

Some particular areas where education can support the protection of freedom of expression online include: respecting others including how to behave online; knowing how to deal with and report offensive content; respecting copyright and intellectual property online; understanding how to navigate and evaluate information online and recognise misinformation; understanding how your personal data is used; and how algorithms determine much of the content individuals see online.

Through our BT Skills for Tomorrow programme we are seeking to ensure that everyone has the skills they need to make the most of life in the digital world. We offer a wide range of free information, advice and support to help everyone, from school children and teachers, parents and families, businesses and jobseekers, to older and more vulnerable people. Working in partnership with a range of leading digital skills, enterprise and community organisations, we have created and collated some of the best advice, information and support,[5] for example we have a course around digital wellbeing for children which includes being kind online and how to treat others.[6]

We recognise that as children are now digital natives from a young age, it is important that digital citizenship education starts early. Through our Barefoot Computing programme in partnership with Computing at School, we help primary school teachers deliver the computing curriculum brilliantly and equip children with the key digital skills needed to thrive. This includes teaching children about how to stay safe online through our Safety Snakes activity and exploring the concept of consent in sharing information online. Our forthcoming 'Be Cyber Smart' resources from Barefoot, designed in collaboration with the National Crime Agency and the National Cyber Security Centre help primary school teachers prepare their pupils to use technology with an awareness of the risks involved, exploring online ownership, the law and how to protect themselves. Helping them to take advantage of legitimate opportunities, as well as being alive to threats. We also offer a range of support for parents and families to help their children navigate the online world safely and happily, including guides to online wellbeing and the importance of being kind online, understanding the role of online influencers and managing issues such as cyberbullying. A common principle that we draw out through all of these educational resources for children is an appreciation that the online world is as real as the offline world, and that considering what you would find acceptable offline can be a helpful starting point when considering how to be a good digital citizen.

Whilst we support further efforts to improve digital citizenship education for all groups and ages, education alone is not enough. We therefore believe it is important for platforms to have clear terms of use and robust processes in place to deal with breaches of these.

---

5 www.bt.com/skillsfortomorrow

6 https://www.bt.com/skillsfortomorrow/home-life/how-to-support-your-childs-online-wellbeing

3. Is online user-generated content covered adequately by existing law and, if so, is the law adequately enforced? Should 'lawful but harmful' online content also be regulated?

Existing law on freedom of expression has generally focussed on defamation and copyright breaches, which are actioned by private parties. To the extent that law addresses broader societal harm online, it tends to be made up of a patchwork of different pieces of legislation which were not designed specifically with the internet in mind (e.g. restrictions on promoting terrorism). These statutory provisions were not necessarily developed with networked technologies in mind, so it has proved difficult to map and enforce them across the internet ecosystem.

Until the advent and proliferation of user-generated content online, content for public consumption had largely been generated by broadcasting or print media. Longstanding content standards such as the Ofcom Broadcasting Code have not had widespread public visibility, since the standards are implemented by specialised sectors, such as the TV, radio and on-demand industry. As a result, familiarity with these rules is generally limited to the employees who are responsible for ensuring an organisation's compliance with them. By contrast, laws to regulate user-generated content target anyone who generates or engages with content online – in other words, most of the population. As such, provisions must be designed to be easy for the general public to understand what is or is not permissible.

We have long advocated for a single, coherent and consistent framework that regulates 'lawful but harmful' online content, as well as transparency reporting requirements to outline the prevalence of harmful content on online platforms and the measures responsible companies are taking to address them. We believe that economic harms, including fraud and scams, should also be in scope.

See also our answer to question 1 for our view on the Government's intention to set out a general definition of harmful content and activity.

4. Should online platforms be under a legal duty to protect freedom of expression?

We firmly believe that communications services have a positive impact on society, and empower people to exercise their rights and freedoms. Yet we acknowledge that online service providers also have the potential to adversely impact human rights through their operations or business relationships. Along with the right to privacy, freedom of expression is one of the human rights that the tech and telecoms industry have focused on over the last decade when it comes to protecting human rights. More recently, and rightly in our view, industry, policy makers and experts have been considering the extent to which online spaces facilitate violation of other rights, especially the safety of children, and the extent to which an over-emphasis of freedom of expression, or privacy, rather than considering all human rights in the round, are a driver of this.
So it's important to note that freedom of expression and privacy aren't the only relevant rights, or necessarily the most important. Beyond the rights of children

and adults to live free from abuse, the global pandemic has demonstrated, the use of (or lack of access to) digital technologies can also have direct impacts on freedom of association or movement; the rights to equality, non-discrimination and education; or even the fundamental right to life. Looking ahead, the distinction between "online" and "offline" rights will only become more perforated as more parts of our life become digitised.

All companies have a corporate responsibility to respect human rights. This means that business enterprises should avoid infringing on the human rights of others, and work to address adverse impacts that they are involved in. BT was an early signatory of the UN Global Compact[7], and our approach to responsible technology is guided by the UN Guiding Principles on Business and Human Rights (UN Guiding Principles)[8]. These international standards should apply equally to online platforms as they would to any other company. We also set out our approach in our Privacy and Free Expression reports.[9]

Just as blocking websites or internet shutdowns infringes upon people's ability to receive and impart information, the way that online platforms prioritise, moderate or otherwise interfere with the user-generated content also has a direct impact on freedom of expression and the right to access information. These rights can also be impacted in less direct ways; for example, when people self-censor or behave differently when they feel they're under surveillance.[10]

In the research project into online harms mentioned in question one, Demos identified a group of 'self-excluders': 'people disengaging from online discourse in order to protect themselves from negative online spaces, suggesting a silencing effect' of the current prioritising of freedom of expression by many social media operators. This is best illustrated from some verbatims from the focus groups carried out as part of the study:

> "*Unfortunately there is a noisy minority on common threads on Twitter or Facebook that are gaining a bit of traction...Whether it's racism or homophobia or whatnot, they can make themselves quite loud*".
>
> "*I cut down on my Facebook completely…. because it was just a white noise of vitriol that was out there"*
>
> "*But then there are also people our age, or 30s or 40s or whatnot, that have already switched off and they've just picked out sections of the internet that they want…."* -

While the corporate responsibility to respect human rights is important, it neither precludes nor replaces the Government's parallel obligation to fulfil and protect human rights. Legislators, government agencies, regulators and other public bodies must therefore ensure that legal requirements on companies do

---

7 https://www.unglobalcompact.org/

8 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

9 https://www.bt.com/about/digital-impact-and-sustainability/championing-human-rights/privacy-and-fee-expression/report

10 See the 2019 UN Human Rights Council report on Surveillance and human rights: https://undocs.org/A/HRC/41/35

not infringe upon their customers' rights in a way that is unlawful, disproportionate, or unnecessary.

The creation of a new legal duty to protect freedom of expression above and beyond the minimum rights protections that already exist in UK law would need to be thoroughly assessed by all stakeholders for potential unintended consequences on fundamental rights, public policy objectives, or the capacity for innovation within the private sector.

5. What model of legal liability for content is most appropriate for online platforms?

The eCommerce Directive (ECD) and UK implementing regulations provide a legal framework for online platforms which includes provisions relating to intermediary liability for content. We understand that the Government has no current plans to change the UK's intermediary liability regimes post-Brexit, although we acknowledge that updates may be required to reflect changes as a result of the EU Digital Services Act, EU Digital Markets Act, or parallel UK legislation.

The different types of internet intermediaries reflected in the eCommerce Directive (ECD) and related UK legal frameworks and regulations are:

- "Mere conduits" – communications service providers like BT that transmit communications.
- "Caches" – typically cloud storage providers (like BT Cloud) that store on a server which can be accessed later.
- "Hosts" – entities that host online materials users, including participative platforms like Facebook and YouTube.

We agree with this categorical distinction, and maintain that measures should be targeted and proportionate, based on the level of risk exposure to users, the capabilities of the provider, and the potential for adverse impacts as a result of intervention. As such, we agree with the ECD's principle that companies hosting user content have limited liability for that content, but are expected to act on known illegal content.

However, the ECD can dis-incentivize platforms to take proactive measures against illegal activities. Under the "notice and takedown" regime, if you don't "notice" illegal activity, you don't need to do anything. In trying to correct this, the challenge is to promote proactive measures without undermining the "no general obligation to monitor" concept in Article 15 of the ECD. This is akin to finding a needle in a haystack – you cannot find the illegal content without looking through the rest of the (legitimate) content on the platform. Recital 48 of the ECD recognises the potential value of supplementing its provisions with a 'duty of care' obligation on hosts in order to 'detect and prevent certain types of illegal activities'. Neither the EU nor any Member State has previously taken the cue from Recital 48. The UK could modernise the law (post Brexit) underpinning online liability without undermining the key principles in the ECD that has

allowed for innovation and creativity in the online sector. The key challenge in introducing such a duty will be in balancing such an obligation to detect illegal content with the principle of "no general obligation to monitor". It seems reasonable to ask social media services that already monitor all the content they host in order to make recommendations to their users and monetise their service to identify and address illegal content at they do so. Caution will also need to be exercised to ensure that any modification of this principle in relation to hosts will not affect caches or mere conduits, which have a very distinct business model which is often premised on privacy. A key element of that "duty of care" provision would be to ensure that online platforms enforce their own terms and conditions effectively and consistently to keep users safe. One way to resolve the tension between Article 15 and the need for more proactive measures to address illegal content online would be to empower independent "trusted flaggers"[11] to provide a reference or 'hash' database of illegal content that hosting services would be obliged to check posted content against, as well as contribute to when they identify new illegal content.

It also worth noting that the aforementioned Demos research found that there was a strong sense from UK citizens polled that online platforms such as social media platforms were the primary bearer of responsibility for content hosted on their platforms, in contradiction to the thesis that as platforms rather than publishers they bear little responsibility.

6. To what extent should users be allowed anonymity online?

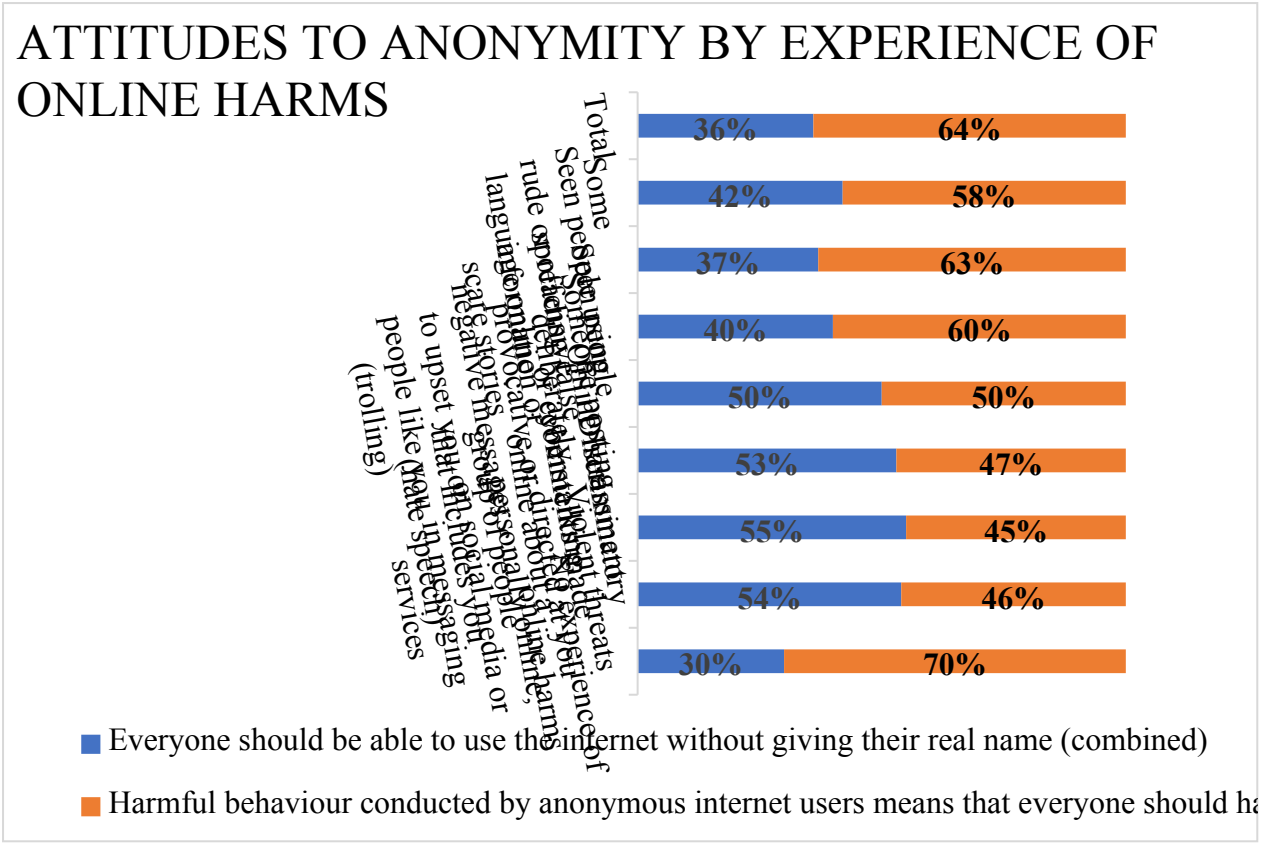
The Government's December 2020 response to the Online Harms White Paper states that *"the police have a range of legal powers to identify individuals who attempt to use anonymity to escape sanctions for online abuse, where the activity is illegal. The government will work with law enforcement to review whether the current powers are sufficient to tackle anonymous abuse online".* We welcome this approach by Government and ask that crimes committed online should be pursued as they would have been offline.

We would also propose that user anonymity to other users on an online platform does not mean being anonymous to the provider of the online platform.

The aforementioned Demos research also touched on harmful behaviour conducted by anonymous internet users. It found that 64% of people believed that everyone should have to use their real name online because of harmful behaviour conducted by anonymous internet users, compared with 36% who believed people should not have to use their real name. There was also agreement in the focus groups that preventing anonymous use of online services could help reduce some online harms. However, there were also concerns at people being deprived of the positive benefits to using online pseudonyms. The research also found that 54% of those polled who had experienced violent threats said that everyone should be able to use the internet without giving their real name. Those most strongly in favour of ending online anonymity had no experience of the online harms surveyed.

---

11 Independent bodies with expertise in identifying illegal and harmful content such as the Internet Watch Foundation



Source: Demos October 2020

7. How can technology be used to help protect the freedom of expression?

Network security is vital for people to exercise their digital rights. More concretely, private and secure connections are necessary for people to freely exchange ideas, search for information, or hold and consider viewpoints without interference. We believe the better tech companies like us are at safeguarding cyber-security, the better our customers are able to control their information, manage their privacy and exercise their free expression and other rights.[12]

There are clearly difficult trade-offs associated with questions about how individual rights and the public interest should be balanced. However, the need to keep private data secure – from health data and bank details to trade secrets and information about national security – will only grow. It will also become more complicated, as the number of devices connected to the internet is forecast to grow from nearly 27 billion in 2017 to 125 billion in 2030.

In this context, encryption and privacy-enhancing technologies are key tools to protect privacy, security and – by extension freedom of expression. BT remains a leader in this space, contributing to significant advancements on revolutionary technologies like homomorphic and encryption quantum key distribution[13]. We

12 https://www.bt.com/about/digital-impact-and-sustainability/championing-human-rights/privacy-and-free-expression

13 https://business.bt.com/solutions/resources/quantum-key-distribution/

also help our customers with advice on protecting their identities and data online[14] , as strong passwords and being alert for phishing emails go a long way toward keeping personal information secure.

8. How do the design and norms of platforms influence the freedom of expression? How can platforms create environments that reduce the propensity for online harms?

No response

9. How could the transparency of algorithms used to censor or promote content, and the training and accountability of their creators, be improved? Should regulators play a role?

In order for algorithms to be transparent, and their creators accountable, it is critical to take an "ethics by design" approach. That means embedding transparency and accountability into the development of an algorithm at the very outset, for example by incorporating features into the build that allow the algorithms to be interpretable, reviewing the source data to ensure it is accurate and representative, and ensuring that the team working on the algorithms are suitably diverse and trained to recognise the risks e.g. of bias in algorithms. Many users are not aware that much of the content they see is determined by algorithms that use data about user online activity. Users should be made aware in an easy to understand and accessible way of the criteria and data used by algorithms to make recommendations and how to enable/disable the parameters for recommendations. Also, users should have an effective route of appeal.

In terms of regulatory involvement, an appropriate starting point would be the ICO's Explainability guidance and also it's AI Auditing Framework.

10. Are there examples of successful public policy on freedom of expression online in other countries from which the UK could learn? What scope is there for further international collaboration?

Governments and regulators around the world are developing new policy approaches to address online content and freedom of expression issues. Because the internet allows people to express themselves and access content regardless of frontiers, regulation of online activity or user-generated content necessarily involves difficult questions around the applicability of national jurisdiction and potential for extra-territorial sovereignty. Broader collaboration and consistency across these efforts is needed, both to facilitate the adoption and enforcement of new regulation as well as to minimise the complexity and cost for businesses operating in these environments.

14 https://www.bt.com/help/security/

11. How can content moderation systems be improved? Are users of online platforms sufficiently able to appeal moderation decisions with which they disagree? What role should regulators play?

No response.

12. To what extent would strengthening competition regulation of dominant online platforms help to make them more responsive to their users' views about content and its moderation?

The Digital Markets Taskforce, led by the Competition and Markets Authority, has recently advised Government to create a new Digital Markets Unit (DMU) to further the interests of consumers in digital markets. The Taskforce has recommended that the DMU designs a new regulatory framework to drive competition in digital markets, and address consumer problems arising out of competition concerns in these markets.[15]

We support the Taskforce's overall recommendations. In our response to the Taskforce's call for information, we argued that lack of competition in digital markets is causing harms to consumers. Some large global digital firms operate in markets that are prone to tipping, and allow them to gather data from their users in a manner that smaller rival firms cannot replicate. These digital markets therefore have a tendency of having a few large players, who can use their position of market power to prevent smaller rivals competing with them fairly, to the detriment of consumers in the long run. We therefore support a new regulatory framework that identifies digital firms with 'strategic market status' and a) imposes a Code of Conduct to prevent anti-competitive conduct and b) applies other pro-competitive interventions (such as data remedies) to lower barriers to entry for smaller new entrants in digital markets.

The primary intent behind the Taskforce's recommendations is to address competition concerns. As part of its recommendation to Government, the Taskforce also identified a number of issues in digital markets that could extend beyond digital firms with market power. For example, digital technologies increase the ease with which activity or content which harms customers can be hosted on platforms. Similarly, users' tendencies to go with default settings and lack of understanding over how to switch platforms means users may be unable to switch to a different platform even if they wish to.

Increasing competition in digital markets can only partly address these types of concerns. Greater choice of digital platforms could enable users to exercise their preferences over online content and switch to their preferred platform. However, the strength of network effects in many digital markets means it is unlikely that there would a large choice of platforms in many of these markets. The benefits arising to users from being able to connect with friends on a single social media platform, or the benefits to businesses from accessing a large portion of their customers over a single e-commerce platform means these markets will tend to

---

15 Competition and Markets Authority, December 2020. A new pro-competition regime for digital markets, Advice of the Digital Markets Taskforce.

tip towards a few large players. In these cases, the Taskforce's proposed Code of Conduct is best suited to address harms arising out of lack of competition.

However, the Taskforce recognises that consumer law is better suited to tackling other forms of consumer harm, including unlawful or illegal activity/content appearing on digital platforms.[16] The CMA has previously used its powers to investigate breaches of consumer protection law in digital markets like secondary ticketing websites, social media endorsements and online hotel booking.[17] In many of these cases, the plurality of digital firms did not prevent consumer harms, partly because consumers did not have the ability to freely exercise their choice. In such instances, promoting competition will not be sufficient to prevent consumer harms. We agree with the Taskforce that reforms to consumer protection law are better suited to tackling harms related to certain types of digital content.

We also note that Government is minded to make Ofcom the future regulator for regulation of harmful online content.[18] Given consumer harms from types of digital content do not solely arise out of lack of competition, we support Ofcom's work in this area, including reforms that improve consumers' understanding of digital markets and how to better exercise choice.

15 January 2021

16 Competition and Markets Authority, December 2020. A new pro-competition regime for digital markets, Advice of the Digital Markets Taskforce, Appendix G.

17 See CMA investigations into secondary ticketing websites, social media endorsements and online hotel booking.

18 Ofcom, 11 December 2020. Ofcom's proposed plan of work 2021/22. P21.

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.

- Our Home Tech Experts who visit homes to help customer set up, are trained to help customers set up parental controls at home.

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 10 million people across the UK develop the skills they need to make the most of life in the digital world, 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 Computing at School (part of BCS, Chartered Institute of IT). We provide engaging cross curricular lessons/classroom resources, free workshops (both face to face and online) and helpful online guides. Online and offline home learning content is also available to support learning beyond the classroom.

- 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 2.8 million children through c 85,000 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. Last year Internet Matters had over 2.8m users, and almost over 80% of 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.

- EE launched in July 2020 'Set Up Safe', a free new SMS service to help parents quickly and easily set up their child's phone with safety features. The service provides parents with guidelines for their children's online activity. This includes settings such as adult content lock, spend caps, preventing charges to bill, and blocking calls and texts to premium numbers, so parents can feel confident their child is safely using their phone outside the home.

- 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 7,000 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[19] 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.

---

19 https://www.btplc.com/Digitalimpactandsustainability/Humanrights/Privacyandfreeexpression/Privacyandfreeexpressionreports/index.htm

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.