Written evidence submitted by BT Group

DCMS Sub Committee Call for Evidence on Online Safety and Online Harms

Written Evidence from BT Group

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 section Online Harms and the Annex for more information.

Key Messages

- The approach to new legislation set out in the Bill is broadly the right direction of travel and now the government needs to press ahead with legislation.
- We are on the whole supportive of the approach to illegal harms but believe that the approach to legal harms could and should be further strengthened.
- Ofcom should have information gathering powers equivalent to those in telecoms and broadcast to enable it to best execute its regulatory role and responsibilities.
- The Bill should address and anticipate how the tech industry is proceeding at pace to create private, end to end encrypted and unregulated spaces - encrypted services need to comply with the requirements of the Bill and not be used for circumvention purposes.
- We are willing to play our part to help enforce the new regulatory regime, but this should be as a last resort with there being a clear legal process that includes a right of appeal if the business disruption measure is technically unworkable.
- The Bill should address all the ways online consumer harms, especially fraud, are marketed online, via advertising and user generated content.
- We think the Bill can only be considered a success if there is a considerable decline in the volume and force of abusive and harmful behaviour and content online. The Bill makes some good progress in this direction, but we think it can be further improved.
- The Bill should include a framework for delivering a media literacy strategy, which enables Ofcom to set ambitions and aims, and to scale and fund activity appropriately.
- The principle of regulatory independence is important and enables good decision.

Online safety

- 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, racism, sexual and violent content, and fake news/misinformation. Children are vulnerable to many of these harms particularly when they are spending increasing amounts of time online due to the Covid-19 pandemic. In addition, there are economic harms caused by fraud, IP and copyright infringement and broader concerns about the size and power of some online platforms.

BT commissioned research on online harms

- We thought it would be useful to the Inquiry to share some recent 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 the trade-offs necessary to expand regulation of the online world. The results can be found here.
- 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.'

Draw The Line and Hope United

- We would also like to take this opportunity to share with the Committee information about our Draw The Line campaign, accompanying research and related Hope United initiative.
- In April this year we launched Draw The Line – the first stage of a multi-million pound BT campaign to step up and stand against hate speech and abuse on social media. New YouGov research commissioned by BT revealed the true societal scale of social media abuse:
    - More than one in ten, over five million people, have received online abuse over the last twelve months.
    - Half the population have seen online abuse in the past year.
    - Online abuse is worse for women with one in five women that received online abuse saying it was about their appearance.
    - The younger the age the more likely you are to experience abuse, sixteen per cent of all 18-34 year old's have experienced abuse.
    - Twenty-three percent of people who identify as gay or lesbian have received online abuse about their sexual orientation.
    - One in seven people believe that those working in the public eye should expect abuse
- BT Sport has spotlighted the issue across the channels and introduced an anti-online abuse policy, deleting, blocking, or reporting hate and abuse on its own channels and being an active bystander.
- The next stage of our Draw The Line campaign has been our Hope United initiative which we launched ahead of the UEFA European Football Championship to galvanise the nation to make a stand against online hate. Managed by Rio Ferdinand and Karen Carney, Hope United features a squad of footballers who, drawing on their own experience of online hate, feature in BT Tech Tips content and free resources helping to give people the digital skills they need to tackle hate online. These cover areas including recognising hate crime, behaving better online, supporting kids online and being a good team player online. The campaign is empowering people to take action with one in four (24%) of people who saw our social advertising 'now more likely to report offensive behavior online', and one in six (17%) feel they are now more likely to call out their friends if they see them say something online they don't think is acceptable.
- While BT it committed to playing its part through this and other efforts (see annex) we believe that robust regulation is vital to drive meaningful and lasting change.

BT response to Inquiry questions:

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

- We welcome the Bill and think the approach to new legislation set out in the Bill is broadly the right direction of travel but now the government needs to press ahead with legislation.
- We believe there needs to be an effective and fair regulatory regime, not just to meaningfully reduce the amount of harmful content posted and circulated online, but also to improve individual users' experiences of being online.
- We do not consider the shift from "online harms" to "online safety" as very significant; the shift to online safety perhaps puts an increased emphasis on ensuring children and adults' safety, before they have or might experience harm, which is welcome.

Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

- The Bill outlines types of illegal content in scope including "a terrorism offence" and "a CSEA (child sexual exploitation and abuse) offence", while other types of harmful content are not specified in the Bill and will be left to secondary legislation. This could be creating ongoing uncertainty, but as a structure it enables a level of ongoing flexibility to address different harms that could arise in the future driven by social norms at the time.
- Within this flexibility we would like to see a single, coherent, and consistent framework. To achieve this on harms without a legal definition the Bill should empower the regulator to set principles, flag a few key terms or words of concern and illustrate in case studies (working in consultation with the industry) how these categories of content hate speech, abuse, self-harm, misinformation should be first identified and then dealt with by online platforms.
- Thus when establishing the statutory Codes of Practice, Ofcom should issue guidance which will provide platform users with clarity and some consistency between platforms on how 'harmful but not illegal' content is dealt with while platforms operators would still have freedom to interpret and implement through their terms of use and community standards.
- However, we also believe the government should consider giving Ofcom powers to go further. Although the new regime allows users to report their concerns to Ofcom, Ofcom will not be able to investigate. Receiving user complaints will instead be part of Ofcom's horizon scanning, research supervision and enforcement activity. We believe that when Ofcom 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 with strict timeframes where content is clearly illegal, as well as appropriate remedies for the victims.
- More generally we believe Ofcom should have information gathering powers equivalent to those in telecoms and broadcast to enable it to best execute its regulatory role and responsibilities.

Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

- We welcome that the Bill encourages companies to meet their duty of care by putting in place systems and processes that improve user safety on their services. Ofcom's statutory Codes of Practice will also set-out expectations for these systems and processes, and the proposed Safety by Design Framework aims to support companies to understand how they can improve user safety through platform design.

- 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.
- 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. 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.
- 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 the most serious of crimes within an appropriate legal framework which is limited and includes the right to appeal.
- 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 and these threaten not just to make the proposed legislation less effective, but to also roll back existing protections and practises.
- Well known examples are messaging services that offer end to end encryption such as WhatsApp and Signal. However, services which provide a gateway to or vehicle for much of users' internet activity are also seeking to implement encryption. For example, Mozilla (Firefox) and Google (via Chrome) are rolling out encrypted domain name service (DNS) resolution in their browser (DNS over HTTPS). Currently, another large device manufacturer is seeking to launch a new version of cloud storage linked to their mobile devices which will provide a new form of comprehensive encryption for much of the online activity of customers using their cloud services.
- All of these have or will render ineffective the software that ISPs and mobile companies currently use to block images of child abuse and other extreme or illegal content. They disable or circumvent users' existing parental controls and security settings and hinder the ability of providers to track and manage the data and services that their customers buy.
- Services should not be able to make unilateral changes which have such significant consequences for citizens and customers, such as ending or impacting the effectiveness of network level protections like 'parental controls'. Rather there should be a new obligation to notify Ofcom for approval when a service proposes changing the way it hands over traffic in the internet architecture which will impact consumers existing choices and experiences.
- 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. Or, for intermediate services such as VPNs or browsers, a back-stop obligation to ensure they are not providing a route to circumvent the UK regulatory regime, and be able to evidence this.
- Therefore, we think the approach in the Bill, to require all services to find CSAM material, with powers for Ofcom to follow up if it is not satisfied is the right one. If a service can find and report CSAM whilst using encryption, that would satisfy the requirements of the Bill. The government is focusing on the outcomes' services operating in the UK will have to live up to, it is not the government's role to specify how that should be achieved, rather it is for service operators to work out how they need to adjust their approach to comply with the law.
- The enforcement regime of the Bill will be delivered via business disruption measures where Ofcom can apply for a 'Access Restriction Order' on ancillary services which include payment services (direct and indirect), search engines, user to user services, services which display advertising on a regulated service, as well as app stores and internet access services. As an ISP we are willing to play our part via, up to and including blocking sites or content, as a last resort

– provided the decisions about what to block are made by Ofcom with a clear legal process and right of appeal.

- However, we believe the Bill does not make sufficient provision for the responsibilities on ancillary services in ensuring that the proposed online safety regime is workable. The encryption developments such as DNS over HTTPS and Apple iCloud Private Relay pose significant challenges for implementing such Access Restriction Orders.
- The best route for addressing this issue would be to make such service providers subject to requirements under an Access Restriction Order for the purposes of enabling the order so that they take the steps necessary (whether by removal of security protections or otherwise) to implement or enable the implementation of the Order. This would make it easier to implement than the converse approach of introducing offences or penalties for obstructing such Orders, which we consider would be very difficult to implement.
- Ultimately, we need legislation in a form that can anticipate these and other future technological developments.

- We think the Bill can only be considered a success if there is a considerable decline in the volume and force of hateful and / or abusive behaviour online. The Bill makes some good progress in this direction, but we think it can be further improved as follows:
    - Provisions relating to 'illegal content' (clauses 5(2), 7, 9 et al and 11:
        - Ofcom should issue regularly updated guidance to services on what passes the threshold for 'illegal harms', so criminal abuse. The guidance should include specific terms, phrases and patterns of behaviour that are or are likely to constitute criminal behaviour and are the minimum requirement (services may choose to review a longer list) to be thoroughly reviewed by the service before it decides whether the service should prevent it being posted, and whether the attempt to post it should be reported to law enforcement. This guidance should cover racist abuse; misogynistic or gender-based abuse; homophobic abuse; threatening, indecent or explicit discriminatory language, behaviour, or content; death or violent threats; hardcore trolling; spam content or bot accounts which generate or circulate the same.
    - Where content does not meet the threshold for 'illegal content' but is still harmful to adults:
        - To strengthen the existing measures on 'ex post' content examination – so that services must review posts using certain words or terms (as above guidance on which terms to be issued by Ofcom and regularly reviewed), as well as if a user flags a concern. This guidance should then clarify, by giving examples, where content does not meet the threshold for 'illegal content' but is still harmful to adults and what characteristics mean companies should nevertheless remove it, when they should invite a user to rephrase, or when they should post a warning beside it.
    - Hateful behaviour that falls short of a criminal threshold – duty to protect adults (Clauses 7(6), 7(7) and 11:
        - The Bill should put more onus on services to (i) change their upstream systems and process so hateful abuse (at a minimum, following Ofcom's guidance on criminal abuse) is not systematically promoted by their algorithms / recommendations; and (ii) an obligation to spot, intervene and halt patterns of abusive behaviour which are identifiable and /or predictable (frequent messaging from bullies, to abusive pile on involving multiple users); and (iii) an obligation to put higher standards of pro-active prevention, monitoring and review of activity around key users and dates for example, footballers involved in the Euro 2020 final or MPs.
        - Similar requirements to adjust upstream services should be applied to self harmful content and misinformation to likewise reduce the volume of this content in

circulation, to flag the content as harmful to service users and suggest alternatives or sources of help, as appropriate.

What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

- The Bill does not address all the ways online consumer harms are marketed online, via advertising and posted content. Section 41 Clause 6 of the Bill explicitly excludes the following harms from the scope of the regime:
  - a. the infringement of intellectual property rights;
  - b. the safety or quality of goods; and
  - c. the performance of a service by a person not qualified to perform it.
- Although many illegal activities are not explicitly covered in the Bill, the inclusion of this clause precludes these specific harms from being addressed by the new regulatory regime. Ofcom's existing statutory duties are to both citizens and consumers, but the new regime does not make adequate provision for its regulatory role in consumer protection. Many of these harms are also carried out by or spread by individual users, whether through posts on platforms or advertising. They should not therefore be excluded on the basis of a narrow definition of 'user-generated' harms.
- Major online platforms claim to be tackling these harms and commonly have terms and conditions related to such harms. However, the increased prevalence of these harms indicates that platforms are failing to effectively enforce their own policies.
- We agree with the Treasury Committee Work and Pensions Committee letter[1] to the Prime Minister dated 21 July 2021 that the government should look at this again and seek to ensure that Bill allows for platforms to be made accountable for tackling content which promotes consumer harms – including fraud, scams, pirated content and poor-quality goods or services.

- The Bill's duty of care will cover content and activity that could cause harm to individuals but not harms to society more broadly. The Bill will introduce measures to tackle disinformation and misinformation such as establishing an expert working group, building on Ofcom media literacy duties and measures to improve transparency about how platforms tackle this harm. We note that the recent annual threat update speech in July 2021 by the Director General of MI5, Ken McCallum highlighted misinformation as threat to the State. As a company that currently operates the UK's largest 5G network, misinformation around Covid-19 had a material, real world, impact on the UK's digital infrastructure and the BT staff and subcontractors who work to maintain it. We experienced incidents of arson, attempted arson, and other forms of sabotage on mobile masts delivering services to our customers. Our analysis suggests that many of these incidents were 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 believed that content shared via social media platforms played a significant role in inciting individuals to commit these acts. We would like the Bill to require that in scope platforms when doing a risk assessment under their duty of care, to consider the wider harm of misinformation on their platforms to not just an individual but to the UK economy and wider society.
- We welcome provisions in the Bill for measures to improve transparency about how platforms deal with misinformation as there needs to be greater transparency from platforms as to how they assess the specific reports made in relation to misinformation, but such measures should specify what standard of 'misinformation' must be met for a report to be acted on.

- We welcome that Ofcom will have powers under the new legislation to promote media literacy that will build on existing provision in the Communications Act 2003. We also welcome the government's publication of its Media Literacy Strategy which rightly calls out the lack of long-term stable funding as a key challenge which the government is committed to addressing. However, the Bill does not mention, nor has the government set out elsewhere how Ofcom's enhanced role in improving media literacy will be funded. BT has funded education and awareness campaigns for parents and children over a number of years and along with Sky, Virgin Media and Talk Talk provided over £10M to fund Internet Matters. From our experience adequate and sustainable funding must be provided if media literacy is to be improved in the UK. To achieve this the Bill should include a provision that requires those regulated services that are in scope to help fund Ofcom's enhanced media literacy responsibilities. The costs of improving media literacy should not fall just on taxpayers, and the current landscape of voluntary funding by some commercial organisations is not sustainable once the new regulatory regime is in place – a clear framework is required. There are similar initiatives for the gambling and alcohol industries.

- We note that the Bill specifies that in performing its duty, Ofcom must deliver, commission, or encourage education initiatives aimed at improving media literacy. There are many charities and other organisations doing great things, but the online child safety landscape is highly fragmented with many small players often performing overlapping activities. Future legislation should require Ofcom to provide leadership by carrying out an evidence-based strategic review to identify and back those education and awareness activities that are scalable and can make a real difference such as Internet Matters. This would help to reduce the duplication of activities and resources. Fewer but larger activities would help increase scope, scale and influence which can have a greater impact in the mission to keep children safe online.

Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

- The Bill does provide a significant role for the Secretary of State over the implementation of the Bills provisions by Ofcom (Part 6), from statements of strategic priorities (Clause 109) to directions in special circumstances (Clause 112) or guidance about how Ofcom should exercise its powers (Clause 113). The Secretary of State would also be able to issue a direction to Ofcom to reject a draft Code of conduct for reasons relating to government policy (Clause 33 (1)). However, the government has not made clear why the Secretary of State needs powers of intervention in content matters that do not exist in broadcast or telecoms regulation. Our experience of regulation is that the public and indeed industry are best served when the regulator is independent and not subject to excessive government oversight: decisions are not influenced by short term political pressure which enables better decision-making.

- As mentioned in our response to the above question in relation to the enforcement regime of the Bill, as an ISP we are willing to play our part via, up to and including blocking sites or content via implementing an Access Restriction Order as a last resort – provided the decisions about what to block are made by Ofcom with a clear legal process and right of appeal which would include going to Court. However, we have concerns about the lack of process to challenge the terms of technically unworkable provisions of an Access Restriction Order. We would therefore propose that the Bill needs to introduce a presumption of consultation by Ofcom before an application for an Access Restriction Order is made where reasonably practicable, a requirement of reasonable practicability for the Order to be implemented, a similar requirement on the Court to consider the reasonable practicability of implementing the Order, and a statutory right of appeal/return hearing.

What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

- 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**.** We therefore welcome the government's acknowledgement in its Impact Assessment to work closely with other international partners to address this shared challenge in order to build consensus around shared approaches to internet safety and to learn from other nations' experiences of tackling online harms. We would also welcome government linking the Bill into an international multilateral framework to build upon the recent G7 Technology Ministers' Statement in April 2021 which included G7 Internet Safety Principles.

ENDS

Annex follows:

Annex

How BT is working to make the internet a safer place

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 25 million people by 2025 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.
- Between 2015 and 31 August 2021 BT funded and managed the Barefoot computing programme in partnership with Computing at School (part of BCS, Chartered Institute of IT) to support primary school teachers to deliver the computing curriculum brilliantly. During this time the portfolio of resources increased to over 70 engaging cross curricular lessons/classroom resources, two free workshops and helpful online guides. Around 50 online and offline home learning activities are also available to support learning beyond the classroom. The Barefoot programme has reached over 3 million children through over 85,000 teachers in primary schools across the UK to date.
- In February 2021, through Barefoot, we launched a set of interactive cyber resources in association with the National Crime Agency exploring areas of online ownership and permissions to the law and password protection. 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 and our 'Stop, Think, Do I Consent' resource explores the terms and conditions of a variety of social media organisations, and reflect on the personal information which people consent to 'giving away' when they sign up to such websites.
- In April 2021 BT launched Draw The Line – the first stage of a multi-million pound BT campaign to step up and stand against hate speech and abuse on social media. New YouGov research commissioned by BT revealed the true societal scale of social media abuse e.g. more than one in ten, over five million people, have received online abuse over the last twelve months. BT Sport has spotlighted the issue across the channels and introduced an anti-online abuse policy, deleting, blocking, or reporting hate and abuse on its own channels and being an active bystander. The next stage of our Draw The Line campaign has been our Hope United initiative which was launched ahead of the UEFA European Football Championship to galvanise the nation to make a stand against online hate. Managed by Rio Ferdinand and Karen Carney, Hope United features a squad of footballers who, drawing on their own experience of online hate, feature in BT Tech Tips content, free resources helping to give people the digital skills they need to tackle hate online. These cover areas including recognising hate crime, behaving better online, supporting kids online and being a good team player online. The campaign is empowering people to take action with one in four (24%) of people who saw our social advertising 'now more likely to report offensive behaviour online', and one in six (17%) feel they are now more likely to call out their friends if they see them say something online they don't think is acceptable.
- 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. BT, Sky, Talk Talk and Virgin Media have contributed over £10M of funding to Internet Matters.

- 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.
- Later this year we will be launching a new national initiative to empower and equip the next generation of digital citizens to be their best online selves and stay safe. Working with partners and advisers including Internet Matters, BBC Own It, Childnet and the Anti-Bullying Alliance, we are developing a holistic programme that will support children at the stage of getting their first smartphone on topics such as online hate, digital wellbeing, online safety and media literacy.
- 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 the trade-offs necessary to expand regulation of the online world. The results can be found here.
- 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 Wi-Fi' 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.