BT Group plc
1 Braham Street,
London E1 8EE,
United Kingdom

bt.com

23 February 2024

Mr Jon Higham
Ofcom Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

By email only to IHconsultation@ofcom.org.uk

Dear Jon

BT Group ("BT", comprised of BT, EE and Plusnet brands) welcomes the opportunity to respond to Ofcom's consultation on protecting people from illegal harms online.

BT is the UK's leading provider of fixed and mobile telecommunications and related secure digital products, solutions and services and provides managed telecommunications, security, network and IT infrastructure services to customers across 180 countries. BT is invested in making the internet a safer place for users, including the most vulnerable members of society, offering free technology tools, supporting online safety education and working in partnerships with charities and government.

BT has been, and remains, strongly supportive the aims of the Online Safety Act: a landmark piece of legislation that is intended to protect citizens and consumers from harms online by placing legal duties on platforms and other tech companies to prevent and remove illegal content. It is now critically important that Ofcom robustly implements and enforces the legislation. The Act needs to be followed by effective regulation that does not weaken the intentions of the Act.

In view of the specific areas of the Act which are relevant to BT, we have structured our response as follows rather than responding to each question in the consultation, although we have identified specific questions where relevant. Our comments focus on Volume 6, Annex 9 and Annex 11 of the draft guidance.

Questions 12-13: Application

Whilst we understand Ofcom's intent to take a proportionate approach to regulation to ensure that resources are focused where the risk of harm is greatest, we are of the view that smaller services, particularly those that have identified as having particular or multi-risks, should be required to do more to help ensure that users are sufficiently protected. Some examples of requirements that we consider should be extended to smaller services include:

- **Governance and accountability:**
    - **3C - Written statements of responsibilities for senior members of staff who make decisions related to the management of online safety risks** – this requirement should be extended to smaller services with specific risks, to increase the individual accountability of the named person and other senior individuals, to encourage online

safety risks to be taken seriously and to help set the right culture through "tone from the top".

- **3E - Evidence of new kinds of illegal content on a service, or increases in particular kinds of illegal content, is tracked and reported to the most senior governance body** – it is critical that all services have processes in place to scan for and identify new risks. Should this be absent, services may continue to categorise themselves as low risk, with few and insufficient risk management controls implemented. Reporting of emerging risks to the senior governing body ensures high level accountability for managing online safety risks.

- **3G - Staff involved in the design and operational management of a service are sufficiently trained in a service's approach to compliance** – staff training is required to ensure controls are operating effectively and is integral to embedding a risk management culture across the organisation.

- **Content Moderation:**

  - **4F - Staff working in content moderation must receive training and materials to enable them to identify and take down illegal content** – we consider this to be a basic requirement on organisations to ensure effective operation of their content moderation functions.

- **Enhanced user controls:**

  - **9A - Users can block or mute individual users and be able to be uncontactable by users they do not yet have an on-service connection with (where services have user profiles & functionalities like connection, posting, user communication)** – this appears to be basic functionality to enable users to have better control over their online experiences and reduce the risk of encountering harm online.

  - **9B - Users can disable comments relating to their own posts, including comments from users that are not blocked** – as above.

There is significant differentiation between the requirements placed on large and small services. The high size threshold for "large" firms means that companies which have significant reach are not captured. When regime is operational, there should be a mechanism to ensure that the size threshold and the requirements applicable to different categories of services are reassessed to ensure that the regime is placing sufficient requirements on all services with the greatest risk of harm.

Question 21: Annex 9 Guidance and content communicated "publicly" or "privately"

In respect of measures 14-16 on p4 of the summary document Consultation at a glance: our proposals and who they apply to (ofcom.org.uk), and the relevant footnotes (a)-(c) on pp7-8, it is stated that "Measure does not apply to private communications or end-to-end encrypted communications".
The guidance further clarifies that "These proposals only apply in relation to content communicated publicly on U2U services, where it is technically feasible to implement them. Consistent with the restrictions in the Act, they do not apply to private communications or end-to-end encrypted communications. In Annex 9 to this consultation, we have set out draft guidance which is intended to assist services in deciding whether content has been communicated "publicly" or "privately" for this purpose."

Whilst we accept that scanning is a "proactive technology" and therefore only applies to content communicated publicly, we have concerns at the addition of "or end-to-end encrypted", which does not reflect the wording of the Act. The Act distinguishes between content communicated publicly and content communicated privately. The Ofcom guidance adds "or end-to-end encrypted communications" and appears to treat it in a similar way to that "communicated privately". However the addition of the word "or" seems to suggest that E2EE is not necessarily accepted to be the same as "communicated privately".

We note that both E2EE services and community building services are explicitly recognised in Volume 2 of the draft guidance as high risk with regard to a range of harms including the dissemination of priority illegal content, and therefore require additional mitigations. As more and more traffic is subject to E2EE and this proportion continues to grow, we have concerns about whether this creates a significant gap for large groups of users communicating together and/or at scale via E2EE, and whether it is appropriate to treat such traffic as equivalent to a private communication. This seems to risk creating the "free pass" for E2EE services which was explicitly ruled out by the government during the Bill's passage.

We support a requirement on regulated tech companies to find technical solutions to scanning encrypted content (e.g. client-side scanning) to prevent the sharing of child sexual abuse and exploitation material (CSAM). Such technical solutions have been proven to be both possible and capable of being implemented. Where they have been implemented and subsequently withdrawn this has generally been driven by user feedback, which in our view demonstrates that there is no technical objection to requiring the use of such technology via regulation. This article provides an interesting overview of Apple's choices in this area Inside Apple's Impossible War On Child Exploitation (forbes.com) This issue is particularly relevant in cases where it is the Access Provider itself which applies the encryption (see comments below regarding relevant Access Providers).

Question 53: Access Restriction Orders

BT Group supports Access Restriction Orders as a mechanism to block access to non-compliant regulated services, as a last resort. However we would welcome further detail in the guidance on Ofcom's approach to consultation with relevant access providers before seeking such Orders. This would ensure both that Access Restriction Orders involve the most appropriate access provider, and that technical issues are fully considered in any application for such Orders – noting the Court's obligation to consider the rights and obligations of the relevant parties when making such an Order.

By way of illustration, a key issue is that network providers such as BT have limited ability to block encrypted traffic, such as traffic using DNS-over-https, Private Relay or similar technologies, or encrypted VPNs. BT Group made representations to this effect during the consultation on the Online Safety Bill and during the parliamentary process. We also sought clarity on the scope of the definition of access providers, noting that encryption may be applied by services which would meet the definition of an access provider. During the Bill's passage through the House of Lords, the Government made the following statement to which we would draw Ofcom's attention:

"The amendment in the name of the noble Lord, Lord Allan of Hallam, seeks to clarify what services might be subject to access restriction orders by removing the two examples provided in the Bill: internet access services and application stores. I would like to reassure him that these are simply indicative examples, highlighting two kinds of service on which access restriction requirements may be imposed. It is not an exhaustive list. Orders could be imposed on any services that meet the definition—that is, a person who provides a facility that is able to withdraw, adapt or manipulate it in such a way as to impede access to the regulated service in question. This provides Ofcom with the flexibility to identify where business disruption measures should be targeted, and it future-proofs the Bill by ensuring that the power remains functional and effective as technologies develop."
Online Safety Bill - Hansard - UK Parliament

This statement provided welcome clarification that the definition of "access providers" encompasses a wide class of providers beyond ISPs and app stores, including for example operating systems, VPNs and browsers in addition to the indicative examples provided.

We remain concerned that this is not widely understood by the providers of such services, and that Ofcom guidance should make this clear. Our concern is that otherwise such services will continue to believe that they are out of scope and will continue to adopt technologies which enable users to circumvent blocking orders which are given effect by ISPs or app stores. In order to avoid significant ineffectiveness and/or non-compliance, we would therefore urge Ofcom to clarify and publicise the scope of access providers in respect of which Ofcom may seek Access Restriction Orders in appropriate cases, and provide further guidance on the process it will use to identify such access providers in specific cases.

A final point of clarification for us would be the circumstances in which Ofcom would consider that it would be appropriate for providers to voluntarily assist in the blocking of non-compliant services without an Access Restriction Order, given our obligations with regard to Open Internet Access. This is referred to in paragraph A9.20 of Annex 11 but the legal basis for it and its application in practice is unclear.

Strengthen protections for women and girls

BT welcomes the introduction of new criminal offences in the Act to address online Violence Against Women and Girls, and Ofcom's specific measures relating to Child Sexual Abuse Material (CSAM).
We are strongly supportive of measures to give greater protections for women and girls online and we have previously run public campaigns to highlight the abuse women and girls often face online, via Hope United and with the charity Glitch.

The current consultation on Illegal Harms does not specifically address the safety of the majority of women and girls online. The Act requires Ofcom to provide Guidance to in-scope services on reducing risks of harm to women and girls, which we are expecting Ofcom to consult on in Q2 2025. This timeline for Ofcom to consult on, and then publish, specific Guidance on Violence Against Women and Girls will mean that women and girls will remain exposed to harms for years before service providers are required to implement effective safety measures. In light of the implementation gap, we'd like to see greater consideration of this issue in the current Guidance. In this respect we are aligned with the comments submitted by the Online Safety Act Network osa-network-ofcom-illegal-harms-sign-on-feb-2024.pdf

Public desire for this regime to create a step change in the experience of being online in the UK, and especially to improve safety for children

BT remind Ofcom of the strong body of evidence and research showing that the British public want to see a significant change in their experience of being online and using social media. As evidenced in this research we commissioned from Demos in 2020 Microsoft PowerPoint - Publication- Demos Online Harms Presentation (1) (5) this research showed that the public have a good grasp of the rights trade-offs and finely balanced decisions involved and are willing to make some sacrifices to their own individual online liberties for the sake of the wider community's protection and safety, especially that of children. This research also showed that the public believe technology companies themselves bear the most responsibility for bringing these improvements to safety of their users about.

That Ofcom should use its approach in other areas it regulates to inform its guidance on matters of judgement, such as when content is harmful or abusive

Ofcom's regular research to inform its guidance to broadcasters on offensive language in TV and radio programmes is a great example of how high quality public attitude research can be used to inform regulatory guidance on subjective questions where attitudes change over time. This approach has the advantage of keeping regulation grounded in UK public opinion and this seems a good solution to the issue our Demos research revealed of 'who decides what is harmful?': Public attitudes towards offensive language on TV and Radio: Quick Reference Guide (ofcom.org.uk) It could for example be used as a basis for guidance of what is racist or sexist abuse online that falls short of the threshold of illegality.

We hope this response is helpful to you. Should you have further questions or wish to discuss any of the points raised, please do not hesitate to get in touch.

Yours sincerely

BT Group Regulatory Affairs