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

Ofcom Online Safety Team
Ofcom
Riverside House
2A Southward Bridge Road
London SE1 9HA

By email to IHconsultations@ofcom.org.uk

23 August 2024

BT Group Submission on Online Safety

Dear Sir/Madam,

BT welcomes Ofcom's work on online safety, which is as an important part of building a safer internet for all. Having assessed Ofcom's proposals, we would like to comment on a range of areas, which could benefit from Ofcom's consideration.

Ofcom should issue clearer guidance on the meaning of the restriction on proactive measures in respect of content communicated privately:

- We understand that the OSA exempts content communicated privately from Ofcom's powers to require proactive measures, including by way of a Code of Practice (s 136, s 232, Schedule 4). However, we believe that some stakeholders are interpreting the lack of proactive requirement to mean that they should not use proactive measures, which is not our understanding of the Act. Our understanding is that a service may choose to use proactive measures on private messaging services to fulfil the duties that apply to all user-to-user services including private messaging services (e.g. to prevent access to and remove priority illegal content). Our understanding of the legal position is simply that Ofcom cannot direct regulated user-to-user services to use proactive measures in relation to content communicated privately (although can direct a regulated service to use accredited technology in relation to CSAE material whether communicated publicly or privately under s 121).
- Ofcom may also want to make it clearer that regulated user-to-user services that offer private messaging (and E2EE technology) may be able to fulfil their obligations to find and remove illegal content by using proactive measures on their service, at the point that content such as images are added to it and before they are attached to and sent as a private message. For example, our view is that some social media platforms could make progress towards compliance in respect of

CSAE material by using processes similar to those they already have in place for commercial purposes, to gather metadata on user behaviour and the images and links users are bringing into the service. Client-side scanning can also be used to compare images uploaded to messaging services from a device against, for example, IWF and NETMEC hash lists before the images are sent in a message. Our view is that it is important to draw the distinction between the private message itself and the service providing it, so that such services are not effectively treated as out of scope.

Ofcom should be clear that 'private messages' and 'E2EE' are not synonymous in the law:

- The OSA only applies the exemption from proactive measures to privately-communicated content. The use of the language "private communications or end-to-end-encrypted communications" in the guidance footnotes above introduces a category of exempted E2EE communications which is not in the Act – and the guidance footnotes appear to recognise that E2EE communications are a different category by including them separately. E2EE communications are not, as far as we are aware, listed as a category in the Annex 9 "Guidance on content communicated 'publicly' or 'privately' under the OSA".
- As more and more of the internet moves to E2EE, we have concerns that E2EE encrypted communications amongst groups of users should not necessarily be treated as synonymous with "private" communications and to treat them as such will lead to significant areas of online activity which are out of reach of the proactive protections which the OSA provides. The government was clear in its comments during the Bill's passage that there was no intent to exempt E2EE services, but by treating all E2EE communications as outside the scope of proactive measures, we are concerned that there will be little meaningful impact on illegal content carried on such services, which are identified in the guidance as particularly high risk.
- For example, all E2EE communications are currently exempted in the draft guidance from requirements to scan for known CSAE hashes. In addition to our concerns about whether E2EE communications should benefit from the same exemptions as private communications, we are concerned as to whether this is intended to (or will be interpreted to) prevent the use of technologies such as client-side scanning which can scan for such hash matches on upload to the service and before they are technically subject to E2EE.
- We are also unclear as to why E2EE communications should benefit from exemption from default settings designed to protect children from grooming, many of which do not appear to relate to content communicated privately but more to user account settings.

- Our understanding is that the law was carefully balanced to address concerns over privacy protections but that the legal duties around safety, especially protection of children, apply to all regulated user-to-user services, whether the content is private or public, or with or without E2EE. Ofcom's draft guidance in this area can be read (and is being interpreted) as introducing blanket exemptions, which we believe misinterprets the intent of the legislation, and risks a lengthy enforcement effort to deliver a key priority of the Act, namely the protection of children from abuse over these services.

Lastly, we suggest it would be helpful if Ofcom, the Government, issue guidance on how privacy interacts with other rights in domestic law.

- International services especially may benefit from a clear reminder that the Article right to privacy, family life, home and correspondence is a qualified right and it is lawful to interfere with this where in accordance with the law and necessary in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- This gives a clear legal basis to interfere with individual privacy rights both on the basis of the prevention of criminal activity such as CSAE currently enabled by online platforms and messaging services, and the protection rights and freedoms of the child victims themselves.
- In our view, some international services, both due to cultural norms and commercial interests, give a disproportionate importance to the privacy rights of service users when set against the harms enabled by their services. This includes the gross infringement of the victims' own privacy rights inherent in CSAE activity, which generally seems to be accorded a lesser focus than the privacy rights of such users. We suggest that setting this balancing of rights out clearly may help these services understand the UK legal obligations they now operate under and support better and more widespread compliance sooner. We are concerned that without this Ofcom may find itself having to have these arguments on a case-by-case basis during enforcement and legal proceedings.

Yours sincerely,

BT Group