Dear Ofcom Consultation Team,

I am writing to strongly object to the proposed framework underpinning Ofcom's Technology Notice powers within the Online Safety Act. While tackling terrorism and child sexual exploitation and abuse (CSEA) content is an undeniably critical objective, the methods proposed in this consultation raise serious concerns regarding privacy, free speech, technological feasibility, and proportionality.

1. Threat to Encryption and Privacy

The powers being discussed risk undermining end-to-end encryption, which is essential for protecting personal privacy, business confidentiality, and national security. By requiring providers to implement specific content-scanning technologies, Ofcom risks forcing platforms to introduce backdoors or client-side scanning—essentially compromising the very security mechanisms that protect law-abiding users from cyber threats, identity theft, and state surveillance.

Leading cybersecurity experts, tech companies, and even government agencies have consistently warned against such measures. Breaking encryption to scan messages for illegal content also creates vulnerabilities that bad actors—terrorists, criminals, and hostile states—could exploit. This would make all users, including children, less safe online, not more.

2. Inaccuracy and Overreach of Detection Technologies

Mandating content identification technologies based on minimum standards of accuracy raises critical concerns. Automated detection systems, including AI-based tools, are notoriously error-prone, often failing to distinguish between legitimate content (such as news reports, educational material, and lawful discussions) and illegal material.

For example:

AI-driven moderation tools have high false-positive rates, frequently misidentifying content and leading to wrongful removal of lawful speech.

Context matters, and automated systems cannot reliably determine intent—leading to legitimate conversations being flagged as terrorism-related or harmful when they are not.

Bad actors will adapt—those who produce and share illegal content will find ways to evade detection, while ordinary users may be wrongly flagged.

Setting arbitrary "minimum standards of accuracy" does not fix these fundamental flaws and may lead to widespread over-removal of lawful content to minimize risk.

3. Disproportionate Powers and Lack of Safeguards

The consultation suggests that Ofcom will have the power to compel platforms to use specific technologies for detecting illegal content. This is an extraordinary power that risks turning Ofcom into an unaccountable arbiter of online speech and surveillance. There are no clear safeguards ensuring that such orders will be issued only when strictly necessary, nor any strong oversight mechanisms to prevent misuse.

Where is the transparency? There is no clear process for public scrutiny of these orders.

Where is the appeal process? If a provider is wrongly forced to implement ineffective or harmful technology, how can they challenge it?

Who holds Ofcom accountable? Regulators should not have unchecked power over how private platforms moderate content.

4. Harm to UK Businesses and Digital Economy

These powers place an enormous burden on online platforms, especially smaller UK-based businesses that do not have the resources to develop or implement sophisticated monitoring systems. This will create a barrier to innovation, pushing startups out of the UK or discouraging them from entering the market altogether.

Larger companies may even withdraw encrypted services from the UK, as companies like WhatsApp and Signal have already indicated, and Apple has already done. This leaves UK users with fewer secure options, harming both privacy and business interests.

Conclusion: Withdraw or Rethink This Approach

While tackling terrorism and CSEA content is vital, this proposal is deeply flawed and carries unacceptable risks. Ofcom should:

1. Explicitly protect end-to-end encryption rather than undermining it.

2. Reject mandatory content-scanning technologies that are unreliable and disproportionate.

3. Ensure strong safeguards, transparency, and an appeals process for any Technology Notices issued.

4. Consult cybersecurity experts and civil rights organizations to find effective but rights-respecting solutions.

I urge Ofcom to reconsider this framework and pursue more proportionate, evidence-based approaches that do not jeopardize privacy, free speech, or the UK’s digital economy.

I look forward to your response.

Yours sincerely,
Name Withheld 1