

## INDEPENDENT REVIEWER OF TERRORISM LEGISLATION

---

### Response to second OFCOM consultation re Online Safety Act 2023

---

1. This is my response to OFCOM's second consultation in connection with the Online Safety Act 2023<sup>1</sup>.
2. The focus of OFCOM's consultation is protecting children from harm online. It comprises an impressive set of documents with some hair-raising revelations about the content to which children are routinely exposed<sup>2</sup>.
3. However, terrorism content is not identified as presenting a particular risk to children. In my response to OFCOM's first consultation on illegal content, I sought to explain why this is a blind spot<sup>3</sup>.
4. OFCOM's response to the first consultation exercise is awaited.

#### **The Risk of Falling Between Two Stools**

5. Some of priority harmful content considered in the second consultation<sup>4</sup> overlaps with terrorism content.
6. This priority content (hereafter 'relevant priority content') is:
  - Content which is abusive and which targets any of the following characteristics— (a) race, (b) religion, (c) sex, (d) sexual orientation, (e) disability, or (f) gender reassignment.
  - Content which incites hatred against people— (a) of a particular race, religion, sex, or sexual orientation, (b) who have a disability, or (c) who have the characteristic of gender reassignment.
  - Content which encourages, promotes, or provides instructions for an act of serious violence against a person.

---

<sup>1</sup> OFCOM, 'Consultation: Protecting children from harms online' (8.5.24).

<sup>2</sup> 'Volume 3: The causes and impacts of online harms to children'.

<sup>3</sup> Response dated 22.1.24, available at <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2024/01/240122-IRTL-OFCOM-response.pdf>.

<sup>4</sup> Section 62(2)-(4) Online Safety Act 2023; OFCOM consultation, supra, Table 3.1.

7. This type of content is reasonably self-explanatory. It may be easier for providers to make decisions about this type of material, than to make difficult judgments about whether content is, or is not, terrorism content and therefore illegal. Although OFCOM's draft Illegal Contents Judgment Guidance<sup>5</sup> is impressive, I do not envy domestic or (more likely) overseas providers trying to work out whether the Terrorism Acts are being contravened.
8. In addition:
- the mandated risk assessment duties that apply to children may require a more granular assessment risk than applies to illegal content. For example, the children's risk assessment duty requires consideration of features that enable content to play automatically<sup>6</sup>, which is not required in the illegal content risk assessment duty<sup>7</sup>.
  - There is merit in placing greater obligations on providers to remove terrorism or priority harmful content for children, who are particularly susceptible, than for adults, who are better able to make up their own minds.
9. It is therefore important that children are effectively protected against relevant priority content, as well as terrorism content.
10. Despite this, OFCOM's "Risk Profiles for Content Harmful to Children"<sup>8</sup>, on which providers will be expected to draw when complying with their child-related duties, is deficient.
- Specific risks for discussion forums (Table A1.1, para 1c) do not refer to relevant priority content, only to suicide, self-harm and eating disorder. Discussion forums such as 8Chan/8Kun are notorious for hateful violent content.
  - Livestreaming (ibid, para 4a) refers to suicide and self-harm, but not relevant priority content. Yet livestreamed massacres, such as the Christ Church killings, are a key vector for radicalisation.
  - Re-posting or forwarding content (ibid, para 4e) against does not identify relevant priority content as a type of risk associated with this service. Forwarding violent and hateful material is a key risk with these services.
11. Moreover, this guidance is inconsistent with OFCOM's research in the first consultation<sup>9</sup>, in which it said in relation to terrorism offences:

"A wide range of types of U2U services are known to be used by terrorist actors. **Social media services** are particularly relevant to perpetration of this harm because of their reach and popularity. Terrorist content is also often identified on **file- storage and file-sharing services**. **Gaming services** have also been

---

<sup>5</sup> Consultation (9.11.23) 'Annex 10: Online Safety Guidance on Judgement for Illegal Content'.

<sup>6</sup> Section 11(6)(f) Online Safety Act 2023.

<sup>7</sup> Section 9.

<sup>8</sup> Annex 1 to draft Children's Risk Assessment Guidance (8.5.24).

<sup>9</sup> Consultation (9.11.23) 'Volume 2: The causes and impacts of online harm', at 6B.

used by terrorists as recruitment and training tools, while **marketplaces and listing services** can be used to raise and collect funds. These types of service have therefore been included in the risk profiles.

Other services are also used to organise, recruit, fundraise and disseminate terrorism content. These include **video-sharing services, discussion forums and chat rooms, messaging services, fundraising services, and payment services**.

Our evidence suggests that services which facilitate the creation of online communities of like-minded individuals, such as in discussion forums or chat rooms, may increase the risks of harm related to terrorism. They can enable potential perpetrators and organised communities to encourage each other to share terrorism content, which may lead to an increase in the risks of harm from terrorism.”

12. This analysis was in the context of terrorism content generally as it affects all users, and therefore including children.
13. I urge OFCOM to spell out more fully the risks of children encountering relevant priority content. This is to avoid the risk posed by terrorism content to children being neither adequately catered for under the illegal content regime (first consultation) or the child protection regime (second consultation).

JONATHAN HALL KC

12 JUNE 2024