

Response to first OFCOM consultation re Online Safety Bill

---

## Introduction

1. This is a response to OFCOM's first consultation in connection with the Online Safety Bill<sup>1</sup>. The focus of the consultation is on the risk of harm from illegal content, which includes "terrorism content", mitigations concerning illegal content, child access assessment and transparency requirements<sup>2</sup>.
2. This response addresses Question 28 which reads:  
  
**"Q28. Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?"**
3. In summary, improvements could be made by requiring an extra tier of protection for children, who are particularly susceptible to the risk of harm posed by terrorism content.
4. So far as OFCOM's proposed powers under the Bill are concerned, OFCOM could in due course include reference to protecting children from terrorism content in its codes of practice and regulatory guidance.
5. Although not a matter for OFCOM, it is also fair to say that the Online Safety Bill, which is currently paused before Parliament at Report Stage, and whose final content is unknown, could benefit from making an explicit reference to the risk of harm to children from terrorism content. At present, the Bill offers only the same degree of protection for children as for adults.

## Children and Terrorism Content Online

6. There is now a good body of evidence that children are particularly susceptible to being drawn into terrorist offending through encountering terrorism content online. The UN has described children as at particular risk of online recruitment<sup>3</sup>.
7. In 2021, 20 children were arrested for terrorism offences<sup>4</sup>, the highest ever.

---

<sup>1</sup> OFCOM, 'Online Safety Call for Evidence' (6.7.22).

<sup>2</sup> Ibid, para 1.9.

<sup>3</sup> United Nations Office on Drugs and Crime, 'Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System' (2017), at page 13.

<sup>4</sup> Home Office, 'Statistics on the operation of police powers under the Terrorism Act 2000 and subsequent legislation' (year ending December 2021), table A-A.10.

- According to Assistant Commissioner Matt Jukes, 19 of these arrests were linked to extreme right-wing ideology<sup>5</sup>.
- It is almost certain that the great majority, if not all these arrests, related to the child's behaviour online.
- Counter-terrorism arrests generally take place when CT Police assess that there is a risk of harm to the public. These figures therefore relate to the sharp end of police activity and are not to be confused with mere referrals to Prevent.

8. The following details from 2021 are in the public domain:

- (January) a 15-year-old from South Derbyshire appeared in court charged with setting up an online terrorist cell ('British Hand')<sup>6</sup> together with a 16-year from Kent<sup>7</sup>.
- (February) a teenage boy from Cornwall with "personality and developmental issues stemming from his abnormal childhood" was sentenced for online terrorism offences committed as a 13-year-old<sup>8</sup>.
- (February) CT police announced that they had arrested a 16-year-old from Derbyshire and referred to the risk of online radicalisation<sup>9</sup>.
- (May) a 16-year-old boy was arrested for extreme right-wing postings on social media<sup>10</sup>.
- (May) a 16-year-old boy from Swindon was arrested<sup>11</sup>. It related to an investigation into extreme right-wing terrorism coordinated in a private online chat group<sup>12</sup>.
- (June) a 15-year-old girl from Derbyshire appeared in court charged with having a bomb-making video<sup>13</sup>. The case was later dropped after it was found that she had been groomed and sexually exploited<sup>14</sup>.
- (June) a 17-year-old boy from Wiltshire was arrested for terrorism offending after members of the public reported racist comments in online forums<sup>15</sup>.

---

<sup>5</sup> 'Far right mimicking video games to lure middle class children to terrorism', The Guardian (17.3.22). See also Rose, H, AC., "'We are Generation Terror!': Youth-on-youth Radicalisation in Extreme-right Youth Groups', CST and ICSR (2021).

<sup>6</sup> 'South Derbyshire schoolboy charged with terrorism offences', Staffordshire Live (26.1.21).

<sup>7</sup> 'Derbyshire teen who ran terror cell boasted he would "cleanse London" of minorities', Derbyshire Live (5.8.21).

<sup>8</sup> 'UK's youngest terror offender walks free from court after recruiting for neo-Nazi group', Independent (8.2.21).

<sup>9</sup> 'Teenage boy arrested on suspicion of terror offences in Derbyshire', Derbyshire Times (18.2.21).

<sup>10</sup> '16-year-old from Leeds sentenced over right wing terror offence', ITV News (14.3.22).

<sup>11</sup> '16-year-old from Swindon arrested on suspicion of terror offences', ITV News (1.5.21)

<sup>12</sup> 'Extreme Right Wing Terror Group Sentenced to More Than 30 Years Imprisonment', Counterterrorism Policing (23.6.22); the 16-year old was not charged.

<sup>13</sup> 'Derbyshire schoolgirl, 15, in court on six terror charges after allegedly being caught with bomb-making video', iNews (17.6.21)

<sup>14</sup> 'Terrorism charges against Derbyshire schoolgirl are dropped', Derbyshire Live (31.1.22).

<sup>15</sup> 'Terror threat teen wanted to attack mosque and kill 10,000', BBC News (6.1.22).

- (July) a 14-year-old boy from Darlington with “complex vulnerabilities” was arrested having become obsessed with school shootings online<sup>16</sup>.
  - (July) a teenage boy from Gloucestershire was sentenced for online terrorism offences committed as a 15- and 16-year-old. The head of CT Policing South West referred to the “very real risk to the young and vulnerable” caused by online terrorism material<sup>17</sup>.
  - (October) a teenage boy was sentenced to 11 years for attack-planning when a child (related to ‘British Hand’, see above)<sup>18</sup>.
  - (December) a 17-year old from Derbyshire was charged with distributing and possessing terrorist material<sup>19</sup>.
9. During 2021 Counter Terrorism Policing released 54 news items on their website<sup>20</sup>. In 10 of these, the police drew attention to the risk posed to children by online terrorism content and asked for vigilance.
10. OFCOM’s 2021 report, ‘Online Nation’, records that 9% of social video platform users had been exposed to ‘radicalisation or terrorism’ within the last 3 months<sup>21</sup>. Much of children’s social media use is centred on social video<sup>22</sup>.
11. As Independent Reviewer I have drawn attention to the risk that more and more children are being drawn through the internet into terrorist offending, which poses acute dilemmas for law enforcement and society at large<sup>23</sup>.
12. It goes without saying that radicalised children can pose a serious terrorist risk; for them, the consequences of being arrested and prosecuted for terrorism offences have a profound impact on life chances, and their families.

### **Lack of specific protection from terrorism content for children under Bill**

13. Despite the susceptibility of children to terrorism content, the Bill treats adults and children alike in terms of the protection it mandates.
14. Terrorism content is “priority illegal content”<sup>24</sup>. User-to-user services and providers of search services have duties to carry out illegal content risk assessments<sup>25</sup> and to have in place proportionate systems and processes designed, respectively, to prevent or

---

<sup>16</sup> ‘Darlington teenager avoids jail after admitting terror charges’, Northern Echo (21.5.22).

<sup>17</sup> ‘Gloucestershire boy sentenced for terrorism offences’, Gloucestershire Constabulary (29.7.21).

<sup>18</sup> ‘Essex teenage neo-Nazi locked up for 11 years after plotting terrorist acts’, ITV News (19.10.21).

<sup>19</sup> ‘17 Year Old From Derbyshire Charged With Terrorism Offences’, CT Policing (3.2.21).

<sup>20</sup> [www.counterterrorism.police.uk](http://www.counterterrorism.police.uk).

<sup>21</sup> Figure 3.14.

<sup>22</sup> Ibid, page 61.

<sup>23</sup> Hall, J., ‘Keyboard Warriors or International Terrorists?’ (14.7.22),

<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/07/IRTL-Keyboard.pdf>.

<sup>24</sup> Cl.52(7).

<sup>25</sup> Cl.8 and 23.

minimise the risk of individuals encountering it<sup>26</sup>. These illegal content duties apply equally to children and adults.

15. There are special duties concerning children, concerning risk assessments<sup>27</sup> and the protection of children<sup>28</sup>. However, these only apply to “content that is harmful to children” which has a special definition under the Bill.

16. By clause 53 “content that is harmful to children” means<sup>29</sup>:

- “Primary priority content that is harmful to children”. Children must be prevented from encountering this altogether. The government has indicated that this is likely to encompass pornography, self-harm, eating disorders and suicide content;<sup>30</sup>
- “Priority content that is harmful to children”. Companies need to ensure content is age appropriate. The government says this is likely to encompass online abuse, harmful health content, and content depicting or encouraging violence<sup>31</sup>;
- “Content of a kind which presents a material risk of significant harm to an appreciable number of children in the United Kingdom” but expressly excluding illegal content (and therefore terrorism content)<sup>32</sup>.

17. The net effect is that tech companies’ specific duties to assess the risk of harm to children, and to protect children, will not apply to terrorism content because it does not fall within the category of “content that is harmful to children”<sup>33</sup>. Some terrorism content will amount to content depicting or encouraging violence but (a) not all of it will and (b) even then, there is no duty to prevent children from encountering it altogether, only a softer duty based on age-appropriateness.

18. User-to-user services and search services *might* be required to consider the risk of harm to children from terrorism content as part of their illegal content risk assessment duties; and to take additional steps to protect children on the basis that this would be a proportionate response to their illegal content safety duty:

---

<sup>26</sup> Cl.9 and 24.

<sup>27</sup> Cl.10 and 25.

<sup>28</sup> Cl.11 and 26.

<sup>29</sup> Clause 53(4).

<sup>30</sup> Secretary of State for Digital, Culture, Media and Sport, written statement (7.7.22), HCWS194.

<sup>31</sup> Ibid.

<sup>32</sup> Cl.53(5)(a).

<sup>33</sup> It is arguable that one aspect of the children’s risk assessment duty applicable to user-to-user services (cl.10(6)(f)), because it refers not to ‘content that is harmful to children’ but to ‘the different ways in which the service is used, and the impact of such use on the level of risk of harm that might be suffered by children’, might stretch to terrorism content. But this is inconsistent with the remainder of the clause, and there is no equivalent provision for search providers.

- However, this would probably require OFCOM to make specific reference to the particular risk to children as part of its guidance on risk assessments<sup>34</sup> or in its Code of Practice relating to terrorism content<sup>35</sup>.
- Otherwise, tech companies within scope are likely to conclude that their duties in relation to terrorism content are exhausted by compliance with their illegal content duties and do not require specific attention to the position of children.
- Making specific reference to children would be consistent with the general duties of OFCOM contained in section 3 of the Communications Act 2003. Clause 78 of the Bill proposes to amend OFCOM’s general duties to include securing the adequate protection of citizens from harm presented by content on a regulated service, and, in performing this additional function, to “have regard to such of the following as appear to them to be relevant in the circumstances - ...(b) the need for a higher level of protection for children than for adults”.
- But OFCOM appears to have a considerable margin of judgment as to whether to include reference to children in its guidance or the Code of Practice. OFCOM may conclude that since the Bill does not provide additional protection for children from terrorist content, it would not be appropriate to add additional requirements in its Code or guidance.
- The Secretary of State has a power of direction, in certain circumstances, to require OFCOM to modify the contents of the Code of Practice on terrorism content. It remains to be seen whether the Secretary of State would use this power if the regulator decided not to make provision for children in the Code of Practice. In any event, the Secretary of State has no power to direct in relation to risk assessment guidance<sup>36</sup>.

### Why distinguish between adults and children?

19. Removing access to online content interferes with the value of freedom of expression. As defined by the Bill, even with recent improvements<sup>37</sup>, there will be material which a tech company may assess to be terrorism content whose presence on the internet, at least for adults, serves the purposes of truth and informing debate<sup>38</sup>.
20. For example, if a senior army officer appeared in a fundraising video for a proscribed organisation, that could well amount to terrorism content<sup>39</sup>, but its dissemination (at least by recognised news publishers) would be in the public interest.

---

<sup>34</sup> Cl.85

<sup>35</sup> Cl.37.

<sup>36</sup> Cl.40.

<sup>37</sup> New Clause 14 added to Bill at Report stage, HC Vol.718 Col.239 (12.7.22). I drew attention to the original deficiencies in ‘Missing Pieces: A Note on Terrorism Legislation in the Online Safety Bill’ (20.4.22): <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/04/Re-OSB-and-Terrorism-Legislation-3.pdf>.

<sup>38</sup> Hall, J., ‘Rights and Values in Counter-Terrorism Online’ (28.6.22): <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/06/Rights-and-Values-CT-Online.pdf>.

<sup>39</sup> As an offence contrary to section 15 Terrorism Act 2000 (which appears in Schedule 5 of the Bill).

21. The position is different for children, because children are less likely (and, for the very young, unlikely) to appreciate the importance of the content without being detrimentally attracted by the content.
22. Some tech companies' internal standards indicate that they draw a distinction between terrorism content whose dissemination may be beneficial in the interests of freedom of expression, at least for adults. For example, YouTube's 'Violent criminal organisations policy'<sup>40</sup> provides that:
- “If posting content related to terrorism or crime for an educational, documentary, scientific, or artistic purpose, be mindful to provide enough information in the video or audio itself so viewers understand the context. Graphic or controversial footage with sufficient context may be subject to age-restrictions or a warning screen.”<sup>41</sup>
23. It may of course be said that content either is or is not “terrorism content” under the Bill, and therefore it must be removed whether for adults or for children. However, that would be to ignore that:
- Under the amended Bill, a provider is to make “judgements about the status of content”, and in deciding whether content is illegal is required to draw inferences based on the information available to it<sup>42</sup>. Different providers may therefore reach different conclusions.
  - Many of the most powerful tech companies are US-based and animated by First Amendment free speech norms that will inevitably grate against the Bill's goal of suppressing terrorism content.
24. **Example 1:** One of the touchstone issues following the passage of the Bill will be the availability of the violently racist and highly influential terrorist publication 'Siege' by the neo-Nazi James Mason<sup>43</sup>. At present it is readily discoverable online. It is possible that tech companies, including search providers, will treat 'Siege' as “priority illegal content” and take proportionate steps to prevent users encountering it.
25. However, it is also possible that tech companies will argue, after the coming into force of the Bill, that its dissemination is not terrorism content because, among other things, it is a historical document.

---

<sup>40</sup> <https://support.google.com/youtube/answer/9229472?hl=en> (last accessed 27.7.22).

<sup>41</sup> Cf. Instagram's Community Guidelines: <https://help.instagram.com/477434105621119> (last accessed 27.7.22); Reddit's Account and Community Restrictions: <https://www.reddithelp.com/hc/en-us/articles/360043513151> (last accessed 27.7.22).

<sup>42</sup> New Clause 14.

<sup>43</sup> Johnson, B., Feldman, M., 'Siege Culture after Siege: Anatomy of a neo-Nazi Terrorist Doctrine' ICCT (2021); Lee, B., 'Siege Culture and Accelerationism in the UK', CREST (2021). 'Siege' is more important than 'Mein Kampf'; new members of youth terror group must state whether they have read 'Siege' or not: Nabert, A., Brause, C., Bender, B., Robins-Early, N., 'Death Weapons: Inside a Teenage Terrorist Network', Politico (27.7.22).

26. Alternatively, tech companies may argue that, even if one or other documents such as ‘Siege’ do technically amount to terrorism content, nonetheless they are complying with their illegal content duty to use “proportionate systems and processes” because they apply a shared database of hashes to remove other terrorism content which does not include ‘Siege’, and they cannot remove everything objectionable from their services.
27. But even if ‘Siege’ is arguably a historical document that ought to remain available for adults, it does not follow that it should be available for children. And even if providers are prepared to be sanguine about the availability of ‘Siege’ for adults, this disregards the responsibility to avoid exposing children to the risk of harm from terrorism content.
28. It follows that unless the implementation of the Bill provides a clear duty for tech companies to take enhanced and meaningful steps to protect children from terrorism content, then terrorism content such as ‘Siege’ may continue to be accessible to children under the Bill.
29. **Example 2:** Some sites, such as the ‘/pol/’ (meaning politically incorrect) image board on 4Chan and 8Chan, are notorious for hosting hateful content involving fascist and white supremacist fantasies, and have been used to pre-announce mass terrorist killings such as Christchurch, New Zealand<sup>44</sup>.
30. The site 4Chan has the following disclaimer for its ‘/pol/’ imageboard:
- “To access this section of 4chan (the "website"), you understand and agree to the following:
1. The content of this website is for mature audiences only and may not be suitable for minors. If you are a minor or it is illegal for you to access mature images and language, do not proceed.
  2. This website is presented to you AS IS, with no warranty, express or implied. By clicking "I Agree," you agree not to hold 4chan responsible for any damages from your use of the website, and you understand that the content posted is not owned or generated by 4chan, but rather by 4chan's users.
  3. As a condition of using this website, you agree to comply with the "Rules" of 4chan, which are also linked on the home page. Please read the Rules carefully, because they are important.”
31. In researching this response, I easily found a copy of the Buffalo (New York) terrorist attack live-stream on a mainstream platform (not 4Chan or 8Chan). It was sufficient to click that I was over 18. It was not necessary to sign in to view the content.

---

<sup>44</sup> Thorleifsson, C., ‘From cyberfascism to terrorism: On 4chan/pol/ culture and the transnational production of memetic violence’ *Nations and Nationalism*, 28( 1), 286– 301 (2022).

32. This does not appear to provide adequate protection against child users of the site accessing terrorism content. The implementation of the Bill ought to require sites to assess the risk of children accessing terrorism content and take enhanced steps to prevent children from doing so.

### **Conclusions**

33. The Bill does not, regrettably, expressly require user-to-user and search providers to assess the risk that children will encounter terrorism content or carry out enhanced steps to minimise the risk of them doing so.
34. It is potentially open to OFCOM to provide guidance to tech companies, and include detail in its Code of Practice, to remedy these defects.
35. If the Bill remains in its current form, OFCOM should require all platforms to carry out child-centred risk assessments and put in place effective measures to minimise the risk of children encountering terrorism content.

Jonathan Hall QC  
29 July 2022