Tech Against Terrorism—written evidence (FEO0036)

House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online

Introduction

Tech Against Terrorism is an initiative established in 2017 supported by the United Nations Counter Terrorism Executive Directorate (UN CTED) and implemented by the UK-based Online Harms Foundation. Tech Against Terrorism supports the global technology sector in responding to terrorist use of the internet whilst respecting human rights, and works to promote public- private partnerships to mitigate this threat. Tech Against Terrorism's research shows that terrorist groups - both jihadist and far-right terrorists - consistently exploit smaller tech platforms when disseminating propaganda. Tech Against Terrorism's mission is to support smaller tech companies in tackling this threat whilst respecting human rights and to provide companies with practical tools to facilitate this process. As a public-private partnership, the initiative is supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of Spain, Switzerland, the Republic of Korea, and Canada. We were recommended as an industry partner in the Government's Interim code of practice on terrorist content and activity online[1] published in December 2020.

Summary

The Government's Online Harms legislation addresses many online harms, however chief among them are the harms posed by terrorist use of the internet. We therefore believe our insights may be an important place from which to draw lessons.

Throughout our research of counter-terrorism measures adopted by governments across the globe, we have noticed worrying trends towards subverting freedom of expression and the rule of law.

Our arguments in this response may be summarised as follows:

- **Accountability** – the Government needs to provide more leadership and strategic thinking in protecting freedom of expression rather than placing the onus on private companies.

- **Rule of Law** – counterterrorism and online harms measures need to be based on the rule of law and pay due regard for human rights, in particular freedom of expression.

---

1 https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-terrorist-content-and-activity-online-accessible-version

- **Proportionality** – the Government should remain vigilant that their regulatory measures do not disproportionately burden smaller tech platforms.

Q1. Is freedom of expression under threat online? If so, how does this impact individuals differently, and why? Are there differences between exercising the freedom of expression online versus offline?

1. Online freedom of expression is under threat from multiple angles. Regulation measures, such as content moderation and algorithms, have been shown to risk disproportionately affect minority groups. In some spaces, harassment and intimidation are rife, affecting users' willingness to express themselves freely online.

2. Our greatest concern is poor regulation. Whilst we appreciate the government's willingness to address online harms, including terrorist use of the internet, a majority of global regulation, including the proposed Online Harms scheme, poses potential threats to freedom of expression online. Several laws, including the Online Harms Bill, also propose removal of content that is legal but "harmful", which we believe is a serious risk that may undermine the rule of law. As shown in Tech Against Terrorism's Online Regulation Series,[2] several (including non-democratic) countries are introducing mechanisms that will effectively ban speech that is legal offline in the online sphere. It is questionable whether this is an approach the UK should take cues from.

3. Furthermore, we remain sceptical as to whether the state regulation that we have seen will be effective in terms of actually serving its intended purpose. We have identified five unintended consequences of state over-regulation of social media on terrorist use of the internet:

    a. **Increased migration of online terrorist ecosystems to smaller platforms** – as terrorists are pushed off larger social media platforms – who are more capable of removing specific content and users as regulation may demand – smaller platforms become overwhelmed by an influx of criminal actors. Furthermore, when regulation introduces financial penalties for failure to comply, this risks disproportionately targeting smaller platforms, who will effectively be punished for their lack of capacity. Whilst we encourage all companies to contribute to tackling terrorist use of the internet, we cannot expect smaller and micro-platforms to have the capacity to comply with the same blanket regulation (e.g. tight content removal deadlines) as large platforms.

    b. **Emboldening non-democratic governments' censorship of political dissent** – when democracies like the UK enforce regulation that risks undermining fundamental human rights such as freedom of

[2] https://www.techagainstterrorism.org/2020/12/22/the-online-regulation-series-summary/

expression, authoritarian regimes are often quick to adopt the same calculus to suppress political opposition.

c. **Increased outsourcing adjudication of content legality to private companies rather than the legal system** – several governments still rely on companies to adjudicate on content's illegality and have made this a key requirement of the law, despite academics warning that such lack of judicial oversight is incompatible with IHR law.

d. **Further radicalisation of people vulnerable to terrorist exploitation** – many of whom complain of feeling 'silenced' or 'censored' if posts that are not actually illegal are removed. The same is true for those vulnerable to disinformation, who may see the removal of posts about, say the perceived 'dangers' of vaccination, as proof of a deep state conspiracy to silence dissenting voices.

4. Whilst we are not opposed to regulation per se, we implore governments to place the rule of law, fundamental freedoms, and appropriate support mechanisms at the centre of any regulatory effort.

Q3. Is online user-generated content covered adequately by existing law and, if so, is the law adequately enforced? Should 'lawful but harmful' online content also be regulated?

5. Current regulation of online user-generated content is unnecessarily harsh: we would highlight the penalties for merely clicking terrorist content online under Section 3(2)(c) of the Counterterrorism and Border Security Act 2019.

6. There is also significant uncertainty over the enforcement of current regulation, e.g. how other aspects of UK counter-terrorism law applies to online content, an area which is only now being examined by the Law Commission's project on Reform of Communications Offences[3] and should have been consulted on before proceeding with the Online Harms legislation. Such uncertainty has led to overly cautious moderation by social media platforms.

7. Any regulation of online speech must act in a manner that is consistent with the rule of law and international human rights protections. We note that metrics which monitor the balance of users' right to freedom of expression and duty to moderate are rarely divulged by governments. We have worked with various platforms on enhancing their transparency reporting, yet this remains a difficult task given governments do not seem to share the same commitment to transparency as they expect from industry.

---

3 https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/

8. Therefore, if governments would like to see more action on content that is currently not illegal but harmful, it should legislate against such content rather than encourage companies to take action on online activity via extra-legal means.

9. Whilst we would stress that – in the counterterrorism area – no platform is perfect in its response (due to the complex challenge this constitutes), we would add that a majority of tech companies (including very small platforms) already have policies and practices in place that go well beyond what it is legally required for them to do.

10. It is paramount that governments do not use their influence to encourage companies to take action on online activity via extra-legal means, as this would severely undermine the rule of law and risk effectively prohibiting freedom of speech.

Q4. Should online platforms be under a legal duty to protect freedom of expression?

11. Combating terrorism has to be the responsibility of governments rather than private companies. Whilst tech companies can and should tackle terrorism online, we risk undermining the rule of law and democratic accountability by placing the onus of countering terrorism on tech companies rather than governments.

12. Governments must also be careful that legislation designed to protect users from terrorist use of the internet does not violate fundamental freedoms, whereby legal speech might be removed via extra-legal means.

13. As things stand, platforms are already stepping up, often assuming a duty of care under an ambiguous legal framework in order to avoid serious financial penalties. The fear of these penalties is a major factor in restricted freedom of expression online.

14. There should be legal clarity to clarify the duties of government. We make the following recommendations that would help tackle harmful content – especially terrorist content – online:

    a) **Help provide definitional clarity around terrorism** – For example, via designations or other measures grounded in the rule of law, to prevent a situation in which private companies define the term. The UK to some extent leads internationally in this regard – having designated three far-right terrorist groups – whereas such designation is entirely lacking in almost every other country.

    b) **Introduce transparency reporting on Government measures to target harmful content online, including terrorism –** We note that metrics which monitor the balance of users' right to freedom of

expression and duty to moderate are rarely divulged by governments. We have worked with various platforms on enhancing their transparency reporting, yet this remains a difficult task given governments do not seem to share the same commitment to transparency as they expect from industry.

c) **Improve leadership on providing strategic thinking** – Particularly around how terrorist use of the internet is tackled in a manner that addresses root causes, accounts for the exploitation of the tech ecosystem rather than a smaller number of individual companies, and respects human rights, freedom of expression, and the rule of law.

15. We encourage civil society to continue to stay engaged in these debates and to support companies in identifying harmful content and in thinking through how measures can be developed in a human rights compliant manner.

Q5. What model of legal liability for content is most appropriate for online platforms?

16. Platforms should not be liable for third party user-generated content. Delegating the responsibility of removing certain types of content to platforms creates serious liability issues for small platforms in particular.

17. Many platforms exist only as hosts or mere conduits; forcing them to undertake moderation and content checks would open them to scrutiny and potential liability for third party content.

18. We are concerned that 'safe harbour' defences are under immense pressure across many jurisdictions, e.g. reforms to the EU's Electronic Commerce Directive under the new Digital Services Act, and the United States' Section 230 of the Communications Decency Act (CDA).

19. In order to preserve the freedoms that the internet enables, and the competition that drives innovation and new forms of expression and communication, we must be cautious of the risks that misguided modification of current legal liability schemes may pose.

Q6. To what extent should users be allowed anonymity online?

20. Anonymity online is a cornerstone of the freedom of the internet, and platforms should be free to make decisions about the anonymity of users themselves. Terrorist and extremist use of the internet would not be affected by an anonymity ban: some extremists are perfectly happy to post illegal or harmful content under their own name.

21. From our experience with use of the internet under authoritarian regimes, we are concerned that rights to privacy and rights to personal security come under serious threat when full transparency of users becomes a legal

requirement, and it is very likely that such a ban would disproportionately negatively affect minority groups and set a destructive precedent for non-democratic nations.

Q7. How can technology be used to help protect the freedom of expression?

22. Technology has been used by industry to manage many of the problems identified in an absence of government leadership and guidance. Protecting freedom of expression often means enabling companies to better protect their users from harmful content, which is why we have supported the Global Internet Forum to Counter Terrorism, a voluntary industry forum (including Twitter, Microsoft, Google and Facebook) set up in June 2017.

23. Since 2019, we have been developing the Terrorist Content Analytics Platform (TCAP), a secure online platform that automates the detection and analysis of verified terrorist content on smaller internet platforms. This will represent the world's first and largest structured dataset of verified terrorist content.

    a. The TCAP will support smaller tech companies in improving content moderation decisions. Often the smallest platforms have limited resources to do this on their own. The platform will also facilitate secure academic research and analysis of terrorist use of the internet using the latest methodologies from advanced analytics and data science. This will help increase understanding of the threat and identify ways to improve the global response.

    b. The TCAP will augment efforts to use artificial intelligence (AI) and machine learning to detect terrorist content at scale. The platform will be available for use by vetted tech companies and academics, and will include oversight mechanisms to ensure content accuracy.

    c. In 2020, we consulted with experts from tech companies, academia, and civil society to seek further input. The outcome of this consultation was a decision to extend the remit of TCAP so that it includes content from far-right violent extremists groups. We hope to launch a beta version of the platform in Autumn 2020.

Q8. How do the design and norms of platforms influence the freedom of expression? How can platforms create environments that reduce the propensity for online harms?

24. Currently, the norms of platforms have been determined by the absence of government guidance. Without designation lists or other legal clarity on what constitutes terrorist content, platforms have had to make this distinction themselves, which raises serious questions about the rule of law.

Clarity from the government would greatly assist in protecting online spaces as open forums.

25. The internet should also be a diverse space; therefore, any regulation should be sensitive to differences in user expectations on different platforms. For example, some platforms are discussion forums, which might want to permit footage of terrorist attacks if presented with context; other platforms, such as image portfolios like Pinterest or youth forums like The Student Room, are either not discussion-based or directed at specific discussions, and will therefore more likely seek to remove even the slightest mention of terrorism (even if that might not be technically ideal from a freedom of expression persepctive).

26. It is important that platforms have a right to enforce different content standards – provided that they are guided by a legal basis set via appropriate legal channels – as this preserves the fundamental diversity of the internet, Although all platforms should act responsibly, it's not appropriate to enforce content norms via extra-legal means. If governments don't want specific content online, they need to make specific content illegal via the appropriate legal processes.

Q12. Are there examples of successful public policy on freedom of expression online in other countries from which the UK could learn? What scope is there for further international collaboration?

27. Several government online strategies are short-term and respond to immediate threats rather than the systems that sustain criminal activity online, e.g. we advise smaller social media platforms who are regularly overwhelmed by migrations of criminal and violent extremist actors banned from larger social media platforms.

28. We need to build systems-based or network-based responses: responses that consider the international and interjurisdictional aspects of cybercrime and the entire online ecosystem.

29. An informed and collaborative relationship with the tech sector is therefore crucial for governments. We regularly brief parliamentarians on the latest counter-terror tools and initiatives. Stronger collaboration between parliamentarians and civil society organisations such as TAT would help governments and the tech sector achieve common purpose.

30. The United States has long leant on its First Amendment right to freedom of speech when it comes to online regulation and content moderation. This means internet platforms are largely in control of their own content policies and codes of conduct. In addition, Section 230 of the Communication Decency Act 1996 establishes immunity from legal liability for tech platforms: effectively meaning they are treated like a noticeboard where people can post their views as individuals, rather than a publisher

responsible for the content their 'authors' (users) produce. The Trump Administration administered an executive order directing independent rules-making agencies to consider regulations that narrow the scope of Section 230 and investigate companies engaging in "unfair or deceptive" content moderation practices. The move shook the online regulation framework and resulted in a wave of proposed bills and Section 230 amendments from both government and civil society. A change in Section 230 would have a big impact globally with most platforms being founded and operated from within the US. To date it is unclear where the incoming Biden administration stands on its progression.

31. In Europe, Germany's[4] regulatory framework has to some extent helped set the standard for the European, and possibly global, regulatory landscape. Germany has an extensive framework for regulating online content, particularly with regards to hate speech and violent extremist and terrorist material.[5] The NetzDG is one of the most extensive regulations of online content in the world, requiring tech companies to comply with several stringent requirements including regular reporting.

32. We see the German blueprint for regulation mirrored in other regions, some with questionable records on human rights, who may be using the German example to justify their own measures designed to stifle freedom of speech and political dissent. Whilst there is criticism[6] from several political directions against this scheme, there is also consensus that removing liability protections would have severe consequences for the internet and online speech, encouraging platforms to over-censor in order to protect themselves from liability.

33. In September 2018, the EU Commission introduced a proposed "regulation on preventing the dissemination of terrorist content online". The proposal suggests three main instruments to regulate online terrorist content:

    a. Swift removals: companies would be obliged to remove content within one hour of having received a removal order from a "competent authority" (which each Member State will be able to appoint). Failure to meet the one-hour deadline could result in penalty fees of up 4% of the company's global annual turnover.

    b. Content referral: the competent authority will also be able to refer content to companies, similar to the role currently played by the EU IRU, for removal against company Terms of Service.

    c. Proactive measures: companies would be required to take "proactive measures" to prevent terrorist content from being uploaded on their platforms – for example by using automated tools.

---

4 https://www.techagainstterrorism.org/2020/10/21/the-online-regulation-series-germany/
5 https://globalreports.columbia.edu/books/speech-police/
6 https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

34. The Commission's proposal drew criticism from academics,[7] experts, and civil society groups.[8] Further, the proposed regulation was criticised by three separate UN Special Rapporteurs,[9] the Council of Europe,[10] and the EU's own Fundamental Rights Agency,[11] which said that the proposal is in possible violation of the EU Charter for Fundamental Rights.[12]

35. Whilst the regulation clarifies that its definition of "terrorist content" is based on the Terrorism Directive, there have been concerns[13] that companies – due to the risk of fines – might remove content shared for journalistic and academic purposes. There has also been criticism raised against the referral mechanism, since this allows for tech company Terms of Service, as opposed to the rule of law, to dictate what content gets removed for counterterrorism purposes. Content moderation expert Daphne Keller has called this the "rule of ToS."[14]

36. At Tech Against Terrorism, we have cautioned[15] against the EU proposal's potential negative impact on smaller tech companies, and warned against the potential fragmentation that it risks leading to. We also encourage the EU to provide more clarity as to what evidence base motivates the one-hour removal deadline.

15 January 2021

---

7 https://cdt.org/wp-content/uploads/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf

8 https://www.article19.org/resources/joint-letter-on-european-commission-regulation-on-online-terrorist-content/

9 https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234

10 https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/misuse-of-anti-terror-legislation-threatens-freedom-of-expression

11 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf

12 https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

13 https://cpj.org/2020/03/eu-online-terrorist-content-legislation-press-freedom/

14 http://cyberlaw.stanford.edu/blog/2019/03/eus-terrorist-content-regulation-expanding-rule-platform-terms-service-and-exporting

15 https://www.voxpol.eu/the-eus-terrorist-content-regulation-concerns-about-effectiveness-and-impact-on-smaller-tech-platforms/