Tech Against Terrorism
Submission to the consultation process for Australia's Online Safety Bill

Submitted on 11 February 2021

1. Recommendations

Based on our reading of the draft Online Safety Bill, we recommend that the Government of Australia:

1. Avoids introducing measures that risk undermining of the rule of law, for example by removing legal content or contributing to extra-legal norm-setting
2. Clarifies:
    a. What safeguards are or will be put in place to avoid removal of legal content
    b. What redress mechanisms are or will be put in place in case of erroneous removal, in particular with regards to app removal and link deletion orders
    c. Definitions around key terms such as 'serious harm' to avoid the risk of reliance of subjective interpretation – such subjectivity is difficult for tech companies to operationalise
3. Introduces segmented levels of responsibility for tech companies dependent on size and avoids financial penalties for smaller or micro-platforms
4. Provides evidence as to why a 24-hour removal deadline is required
5. Provides information on the steps taken to ensure that the e-Safety Commissioner's office carries out its activities with the fullest respect for freedom of expression and human rights
6. Uses existing legal instruments which are more likely to positively contribute to countering terrorist use of the internet, including via improving designation of (particularly far-right) terrorist groups

2. Observations

2.a. Positive aspects of the Online Safety Bill

There are several positive aspects worth highlighting in the Bill. Firstly, we commend the fact that the main body in charge of coordinating and encouraging action from tech companies, the e-Safety Commissioner, has a clear legal standing. This ensures that several of the instruments provided (such as removal orders) are carried out in accordance with the rule of law. Whilst we have some concerns around the process regarding the industry standards setting mentioned in the Bill, we strongly support any work that help raise tech sector standards and capacity to take action on illegal – and particularly terrorist – content and activity. This is why we since 2017 have worked to help increase tech sector capacity to tackle terrorist use of the internet in a manner that respects human rights, for example via our Mentorship Programme[1] and the Tech Against Terrorism Pledge.[2] We encourage and invite the Government of Australia to examine best practices learned from these processes. Further, we see some potential in the Act to create legal mechanisms for action on terrorist operated

[1] https://www.techagainstterrorism.org/membership/tech-against-terrorism-mentorship/

[2] https://www.techagainstterrorism.org/membership/pledge/

websites (TOWs), sites which are run by terrorist groups in order to archive and store terrorist propaganda.[3] Lastly, we support the fact that the Government seeks to approach the issue of online safety in a manner that focusses on improving the systems and processes that underpin content moderation, and not only on content itself.

2.b. Areas of concern

Rule of law

1) We are concerned that the Bill will lead to extensive takedown of legal (but 'harmful') speech. Worryingly, this is part of a global regulatory trend where (democratic and non-democratic) countries are introducing mechanisms that risk undermining the rule of law, which we documented in our Online Regulation Series.[4] For example, whilst cyber bullying and abuse are issues that we would like tech companies to help counter for ethical reasons, compelling them to do so under threat of potential liability and financial penalties risks undermining the rule of law. Whilst some aspects of bullying and abuse have anchoring in Australian criminal code, the definitions provided in the Act suggest that the law will potentially lead to removal of large amounts of legal speech. In a democracy, we cannot make speech that is legal offline illegal in the online space. If harms need countering online, they should be prohibited in law before creating legislation aiming to remove such content from the internet.
2) We have some concerns regarding the extra-legality of the development of industry codes in Article 140 (2) as well as in Article 143. We do not think it is appropriate for the tech sector to develop codes that can subsequently be introduced into law with legal liability and subsequent financial penalties. Whilst improved industry codes should be encouraged, it is important that legislation is determined by democratically accountable institutions. Similarly, for the basic online safety expectations detailed in Part 4 of the draft Bill, we ask the Government to clarify whether Article 45 (4) means that the basic online safety expectations will contribute to an extra-legal process by which companies will be held legally liable for failure to comply with the standard.
3) We further encourage the Government to clarify the statement found in Section 95 (blocking request) and 99 (blocking notice) stating that the e-Commissioner is under no obligation to observe requirements of procedural fairness. The Government should ensure that this does not lead to any requests and notices being issued to tech companies via extra-legal channels.
4) With regards to terrorist use of the internet and related harms, there is a lack of reference to existing legal frameworks and how they will support the implementation of the Bill. We therefore encourage more clarity on how the Bill relates to existing hate speech and terrorism legislation in Australia, as well as to the designation of terrorist groups.
5) We would challenge the assumption that it is the tech industry's responsibility to keep Australian citizens safe, including from (but not limited to) terrorism. Whilst all tech companies should play a role in responding to terrorist and violent extremist use of their services (in addition to other harms), this is primarily the responsibility of governments. It

[3] We are currently tracking 36 TOWs but suspect this number is not comprehensive. TOWs play an increasingly important role in the terrorist and violent extremist online eco-system and facilitates storing of content, materials which can be linked via beacon platforms.

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

is vital that counterterrorism efforts both online and offline are led by democratically accountable institutions and not private tech companies.

Freedom of expression

6) We are concerned that there are no clear references to safeguards to prevent erroneous removal of content as a result of blocking or removal requests. This is particularly serious for link deletion and app removal requests, as these are severe steps with a potentially detrimental impact to freedom of information if carried out erroneously. Furthermore, there is no reference to redress mechanisms in the Bill. We encourage the Government to specify what exact measures will be put in place to prevent adverse impact on freedom of speech.
7) There are a number of imprecise definitions that we believe risk having negative impact on freedom of expression. The definitions provided for child cyber bullying and cyber abuse seem to build on a perceived 'common sense' approach as opposed to legal concepts, and are therefore at risk of being assessed subjectively. Not only will this risk leading to removal of legal content, but it will also be difficult to operationalise for tech companies. Causing 'serious harm to a person's mental health', which is how cyber abuse is defined, could – due to is subjectivity – imply a wide range of legal and commonplace speech that could be expressed without any intent to do harm. For this reason, there is a risk that this law could be used to silent legitimate expression, for example public criticism of individuals.
8) We have some concerns around the Abhorrent Violent Material (AVM) scheme. Whilst the scope of the law is clear, we worry that imprecise definitions of 'terrorist act' and calls for companies to remove content 'expeditiously' could encourage tech platforms to remove content that is shared with the purpose of documenting terrorist offences and war crimes that can serve as crucial evidence in court proceedings.[5] We appreciate the necessity to restrict access to content that risks becoming viral in the immediate aftermath of a terrorist attack. However, due to the drastic measures that the Bill allows for, the Government should ensure that there are sufficient safeguards in place in case of wrongful blocking and that appropriate redress mechanisms are identified.

Smaller tech companies and tech sector capacity

9) We are concerned that the draft Bill does not explicitly refer to smaller tech companies. Based on our work in supporting smaller tech companies to tackle terrorist use of the internet over the past four years, we are aware that smaller tech companies often do not have the capacity to take swift action due to limited staff numbers or subject matter expertise on various harm areas. Since it is well-established, and has been for a long time, that terrorists predominantly exploit smaller platforms for exactly this reason,[6] it is disappointing to not see this reflected in the Act.
10) Specifically, we worry that instruments such as the removal and blocking deadlines of 24 hours (which are punishable by steep fines) will severely harm competition and innovation.

[5] See Human Rights Watch's report "Video Unavailable: Social Media Platforms Remove Evidence of War Crimes": https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes

[6] https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/

Furthermore, since many smaller companies might not be able to take action within the timeframe or have the financial means to pay the fines, the legislation will likely be ineffective in terms of achieving its stated aim.

11) We encourage the Government to provide further clarity as to whether the Act will apply to tech companies of all sizes and recommend that obligations are segmented according to company size. An example of recent draft regulation where this has been done is the EU's Digital Services Act,[7] where smaller platforms are exempted from some of the transparency reporting requirements.

12) Lastly, we would contest the notion that the presence of illegal and harmful content online is the result of tech company commitment (or perceived lack thereof). There is widespread expert consensus that content moderation at scale for vary large platforms is virtually impossible to do perfectly. For smaller companies, the lack of capacity and resources is a well-documented challenge. For all companies, there are complex decision-making processes related to all kinds of harm areas that often require a high degree of nuance and contextual understanding. We therefore should not expect that companies can address exploitation of their services by simply creating more algorithms or working harder. Terrorism is an especially complex issue for which there are a plethora of (overwhelmingly offline) root causes. Whilst it is arguably outside of the scope of this Act to address these points, we do encourage the Government to keep this in mind ahead of the introduction of this and other laws pertaining to online speech.

Effectiveness in countering terrorist use of the internet

13) Whilst this Bill has several positive aspects, we assess that it will not be effective in terms of countering terrorist use of the internet. The reason for his is two-fold. Firstly, we worry that the Bill seems directed towards larger tech companies. Whilst it is reasonable to expect larger tech companies to improve their response to terrorist use of their services, as noted above the most important strategic threat is currently on smaller platforms. The measures introduced in the draft will not help or necessarily encourage smaller companies to improve their capacity. Secondly, we believe that governments can achieve much more to tackle terrorist use of the internet by focusing on other legal instruments instead of complex regulation of online speech. One is designation. Here, governments can help tech companies by clearly indicating which groups are illegal and therefore subject to removal from platforms. In our experience, this creates clarity for tech companies and improves overall tech sector efforts to remove terrorist content, even from occasionally hostile platforms who otherwise would choose to keep such content online.[8] Such designation is particularly lacking with far-right groups. We therefore encourage Australia to improve its designation of far-right terrorist groups. To us, this approach is preferable to allowing democratically unaccountable tech companies set the standard for permissible speech online.

14) Furthermore, we note that the Act does not explicitly refer to terrorist propaganda and other activity outside of the definitions of 'terrorist act' provided in the AVM scheme. Due to the complex and diverse threat that terrorist use of the internet constitutes, we

[7] https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[8] One example is Gab, who deleted a page run by UK-designated group Scottish Dawn after a report from Tech Against Terrorism referring to its illegal status.

encourage the Government to clarify if other types of terrorist exploitation will also be covered by the Bill.

About Tech Against Terrorism

Tech Against Terrorism is an initiative supported by the United Nations Counter Terrorism Executive Directorate (UN CTED) in April 2017. We support the global technology sector in responding to terrorist use of the internet whilst respecting human rights, and we work to promote public-private partnerships to mitigate this threat. Our research shows that terrorist groups - both jihadist and far-right terrorists – consistently exploit smaller tech platforms when disseminating propaganda. At Tech Against Terrorism, our 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. We are currently building the Terrorist Content Analytics Platform (TCAP), which supports tech companies in swiftly taking action on terrorist content located on their sites. As a public-private partnership, the initiative has been supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of Spain, Switzerland, the Republic of Korea, and Canada.