CHRISTCHURCH CALL

TO ELIMINATE TERRORIST & VIOLENT EXTREMIST CONTENT ONLINE

Supporting smaller platforms

Introduction

The Christchurch Call (the Call) was established in 2019 as a commitment by governments and Online Service Providers (OSPs) to eliminate Terrorist and Violent Extremist Content (TVEC) online. The Call rests on the conviction that a free, open, and secure internet offers extraordinary benefits to society and that respect for freedom of expression is fundamental; however, no one has the right to create and share TVEC online. The Call has since grown to over 120 governments, OSPs, partners, and civil society organisations, all working together towards the elimination of TVEC on the internet.

From the beginning, Call Leaders have recognised the important role that smaller OSPs play in preventing the proliferation of TVEC, particularly during crisis incidents. In 2019, they noted the awareness and capacity challenges that smaller OSPs face and, in response, supporters committed to empowering smaller OSPs as they build capacity to remove TVEC.[1] Since 2019, the Christchurch Call has catalysed this support, with the Call Community building upon existing and new resources and tools that have revolutionised the support available to smaller OSPs that need assistance.

However, gaps remain that still challenge the ability of smaller OSPs to eliminate TVEC from their services. In the wake of global regulatory change, smaller OSPs are experiencing an increasing shortage of awareness and capacity to engage with the now-wide range of available resources and tools, and they often are unable to participate in effective crisis response mechanisms. Terrorists and violent extremists are exploiting these gaps to propagate their content as widely as possible.

Responding to these challenges, at their 2022 Summit Call Leaders committed to "ensuring shared industry tools remain at the leading edge of technology and are effective in responding to adversarial tactics and shifts". [2] This report seeks to analyse these challenges, map the current supports available to smaller OSPs, and consider what needs to be done to address identified gaps. It is based on desktop research and consultation with the Call Community and smaller OSPs between May and September 2023.

Definition of smaller OSPs

For the purposes this report, an OSP is the provider of any online service that facilitates the access to, input, or upload of user-generated content. This definition generally excludes static websites without this functionality but can include those with comment sections (such as news sites), as well as file search engines, storage (including hosting), file sharing, social media, gaming, video, messaging, and some other services.

Referring to some OSPs as "smaller" can be misleading. Some have just a few dozen users whereas others can have millions. Some can have very few staff relative to users, while others can be better resourced. It is also not particularly useful from an analytical perspective. Consultations highlighted

the diverse ways OSPs can be categorised, and how they categorise themselves, with reference to dimensions including Monthly Active Users (MAU), revenue, number of staff, number of dedicated trust and safety staff, nature of the service, and community culture. These different dimensions influence both the risk that a service will be exposed to TVEC and the OSP's awareness, capacity, and willingness to address it.

For this report, a smaller OSP is any provider that lacks the awareness and/or capacity to eliminate TVEC on their service.[*]

Threat environment

It remains unclear how many smaller OSPs operate, out of the approximately 201 million active websites online.[3] OFCOM estimates that approximately 100,000 services will be within the scope of the UK Online Safety Bill[4], although the number of these that are currently experiencing terrorist and violent extremist exploitation, and to what extent, is under-researched at this time.

The online ecosystem is also volatile, with services continually starting-up and shutting-down across the web, and decentralisation providing new portability of presence for users while creating new moderation risks.[5 & 6] The geography and user base of these services is equally unclear, although is certainly in the hundreds of millions (potentially well over a billion), given the collective MAU of many services.

Amongst this dynamic and vibrant internet ecosystem, terrorists and violent extremists are increasingly exploiting smaller services to share TVEC. This is not a new issue: the United States Department of Homeland Security first identified[7] in 2010 that jihadist organisations were utilising a multi-platform approach to sharing TVEC. Numerous academics[8, 9, 10, 11 & 12] (as collated by Watkin[13]) and others[14, 15 & 16] have subsequently noted the tactics that terrorists and violent extremists use to propagate their content as widely as possible. This behaviour typically involves 'outlinking' (also called 'dead-dropping' or 'signposting') from beacon platforms (typically the largest OSPs, where content is quickly removed) to content stores (typically smaller OSPs) where the content resides and where rapid and effective content moderation is less likely to exist, aided by circumventors (such as VPNs) to avoid detection.[17 & 18] The consequence of this behaviour is an increased exploitation of the awareness, capacity, and willingness of smaller OSPs, which also carries implications for the largest OSPs.

Smaller OPS are also exploited in crisis incidents, such as the 2022 Buffalo, NY, attack where the shooter exploited several smaller services to both plan and broadcast his attack.[19] TVEC from this attack and the Christchurch massacre are continuously quickly removed by the largest OSPs but remains readily available on some smaller services where extremists exploit a lack of detection capabilities to re-post, discuss and share it and similar material.[20 & 21] 'Alt-tech' platforms represent a subset of smaller OSPs dedicated to extreme or fringe content, usually with a lack of content moderation; these OSPs provide opportunities for terrorist and violent extremist exploitation, with little intervention.[22, 23 & 24]

[*] Willingness is also a key consideration, and unmoderated and alt-tech services are a priority outlined in the 2022 Christchurch Call Leaders' Summit, however unwillingness raises a different set of issues and possible interventions, which the Call Community is to explore in depth in the Free, Open and Secure Internet Principle Working Group.

Landscape mapping

Regulatory change

Recent and upcoming government laws will require increased content moderation, risk assessments, transparency, and more from OSPs. For example, the European Union *Terrorist Content Online Regulation* requires compliance with removal orders within one hour, transparency reporting, and other measures such as preserving removed content and having an appeals and complaints mechanism,[25] Australia's *Online Safety Act* includes a risk assessment requirement,[26] Singapore's *Online Safety Act* includes the need to comply with blocking directions,[27] and the United Kingdom's *Online Safety Bill* will require OSPs to proactively remove illegal content[28]; all of which include in scope smaller OSPs in some capacity. Evidently, regulators recognise that TVEC and other forms of illegal/harmful content can reside and be shared on smaller services, so regulatory responses must include them to be effective. This new regulatory burden may hinder innovation and competition because of the strenuous resources required to implement compliance measures. Most laws are designed to minimise effects on smaller OSPs, and some have also put in place specific supports (see below), but in a global ecosystem with a growing number of regulatory frameworks with their own compliance burdens, it is increasingly difficult for many smaller OSPs to possess the awareness and capacity necessary to adhere to all of them.

Existing resources and tools

There are numerous resources and tools available in the Call Community to support smaller OSPs counter terrorist and violent extremist exploitation of their services. Briefly, these include:

- **Tech Against Terrorism** (TAT), whose efforts to support smaller OSPs include a membership program and Knowledge Sharing Platform that provide access to practice guides on defining terrorist content, transparency reporting benchmarks, global legislation (through the Online Regulation Series) and terrorist symbols and terms.
- The **Terrorist Content Analytics Platform** (TCAP), developed by TAT with the support of the Canadian Government, which alerts participating smaller OSPs of URLs on their services that contain TVEC. Soon, the TCAP will also hash URLs for the GIFCT's Hash Sharing Database and archive content for audit and research purposes.[29]
- **TAT Europe**, the arm of TAT funded by the European Commission to uplift the capacities of smaller OSPs to comply with the Terrorist Content Online Regulation.
- The **Global Internet Forum to Counter Terrorism** (GIFCT), whose membership provides access to cross-service information sharing, crisis response including the Hash Sharing Database, working groups, and workshops.
- **Hasher-Matcher-Actioner**, an open-source tool developed by Meta to assist smaller OSPs develop in-house capacity to label, hash and match harmful content.
- An upcoming tool from **Google Jigsaw** and TAT that will provide content moderation workflow capabilities to smaller OSPs that currently rely on manual moderation.
- The maturing commercial **safety tech industry**, comprising over 350 vendors that provide automated, behavioural-based detection of online harms, intelligence and threat awareness, age-assurance, regulatory compliance support, and more.[30 & 31]

These tools, particularly those from TAT and the safety tech industry, have lowered the costs for smaller OSPs looking to eliminate TVEC from their services and have begun to fill the gap in

resources and tools that existed in 2019. Nonetheless, a variety of challenges still face smaller OSPs, as will be presented below.

Gap analysis

Ideally, OSPs regardless of size should have the awareness, capacity, and willingness to eliminate TVEC from their services, while respecting human rights and playing their part in a free, open, and secure internet. Despite advancements in the tools and resources, there are remaining gaps in awareness and capacity that impact the ability of smaller OSPs to fully participate in online counter-terrorism efforts, which this section will explore.

As noted earlier, there are likely hundreds of thousands of smaller OSPs operating around the world, many of which could potentially be at risk from terrorist and violent extremist exploitation. It is important to note at the outset that many smaller OSPs likely have the awareness, capacity, and willingness to eliminate TVEC, even if they are not formally involved in multistakeholder or industry-led efforts. The Christchurch Call recognises that resources and tools should be available and accessible to all smaller OSPs that need or could benefit from them, regardless of their membership of specific initiatives.

Current gaps:

Awareness: The extent to which the majority of smaller OSPs are aware of the existing resources and tools available to them is unclear and there is limited research to rigorously evaluate this point. Anecdotally, however, we know from our consultations that levels of awareness are highly variable. Some are aware; others are not at all.

Capacity: Obtaining awareness of available resources and tools and then implementing them as an effective response to TVEC requires capacity, which is often lacking within smaller OSPs. Recently, cuts to trust and safety teams within smaller OSPs have further restricted their capacity to address specific risks on their services. A common theme heard in our consultations with smaller OSPs was their need to prioritise other kinds of illegal content, based on greater prevalence and/or harmfulness.

Given the significant changes – regulatory, technological, and commercial – that have impacted the OSP and TVEC landscape in the time since the launch of the Christchurch Call in 2019, the awareness and capacity of smaller OSPs remains in flux. Regulatory frameworks are still evolving, but combined with education and support programmes, they will meaningfully impact both the awareness and the cost-benefit analysis of acting against TVEC where it is a risk (i.e., capacity and willingness). At the same time, the efforts of Call supporters like TAT, Meta, Google and others, and the flourishing safety tech sector, means there are new resources and tools available to address the diverse needs of smaller OSPs, and these are increasingly affordable to acquire and implement. It will take some time for the full effects of these changes to materialise, and the consequent impact of TVEC on smaller OSPs to be fully understood.

In the meantime, the Call Community should continue to support smaller OSPs to improve awareness and build capacity to address TVEC – issues we know they face – with a focus on:

- **Increasing awareness amongst smaller OSPs of existing resources and tools to eliminate TVEC.** While there are now numerous resources and tools available to smaller OSPs, a complex regulatory landscape and competing online harm priorities mean that only some

smaller OSPs have a full understanding of what TVEC is, why it is important to eliminate it, why they are required to, and what exists to help them to do. *The Call Community should undertake communication efforts, perhaps bundled with the campaigns of regulators who are aiming to increase compliance with their laws, by presenting existing resources and tools as a tangible way OSPs can demonstrate their online safety efforts.*

- **Identifying, encouraging, and supporting smaller OSPs to avail themselves of these resources and tools.** While initiatives such as the GIFCT deliver valuable support and industry information sharing capabilities, strenuous membership criteria mean that these sorts of resources are an option for only the most motivated of smaller OSPs. Lower-barrier options, such as those from regulators, TAT, and the commercial safety tech market, are best-suited for smaller OSPs who are lacking in capacity. *The Call Community should use its knowledge of which smaller OSPs are at the greatest risk of exploitation and use all available levers to improve their uptake of existing resources and tools.*

- **Integrating smaller OSPs into effective crisis response.** One smaller OSP we consulted said that a terrorist crisis incident on their service is what "keeps me awake at night", but crisis integration for smaller OSPs is currently limited to the GIFCT, whose membership criteria is beyond the capacity of most. TAT is currently developing a new tiered alerting framework and incident response policy for the TCAP, linked to existing crisis response protocols. Should TAT obtain funding to make the TCAP's crisis functions available 24/7, it would create a globally available, low-barrier entry for smaller OSPs wishing to quickly become part of the crisis response network. *The Call Community should consider support for the TCAP and other effective crisis response solutions as a priority to aide with the integration of smaller OSPs into effective crisis response.*

- **Ensuring that solutions are transparent and respect human rights.** As obligations to eliminate TVEC increase for smaller OSPs, an increased take-up of resources and tools is encouraged (as above), but with this comes the potential for risks for human rights. We heard some concerns about privacy and freedom of speech implications of commercial safety tech, although some vendors offer assurances and mitigations for both. There are resources available, such as the TAT Transparency Guidelines and Human Rights Toolkit, that aim to uplift OSP awareness of human rights. *The Call Community should consider how it can raise awareness and incentivise demand and supply for transparent, human-rights-respecting solutions for smaller OSPs.*

- **Considering the impact of new and emerging technologies.** New tech such as generative artificial intelligence, decentralised services, blockchain and immersive technologies are sometimes presented as the next generation of the internet. Start-up and smaller OSPs lead the charge in the adoption of new tech, and often face the burden of designing and implementing content moderation in entirely new ways. For example, research[32 & 33] points to the challenges decentralisation provides to eliminating TVEC. Generative AI poses its own challenges, but also presents opportunities for the automated detection of TVEC, particularly by the commercial safety tech sector. *The Call Community is already actively considering the impact of new tech and should actively consider the unique challenges faced by smaller OSPs.*

The role of willingness, as it relates to smaller OSPs, is also an important gap given the rise of alt-tech and far-right services. This topic will be explored in depth in the Call's Free, Open and Secure Internet Principle Working Group.

Conclusion

The Call Community has catalysed the resources and tools available to smaller OSPs since 2019, with Call supporters and partners investing to ensure that services of any size can eliminate TVEC. However, challenges remain, and the Call Community should focus on supporting the awareness and capacity of smaller OSPs to engage with and effectively use these resources and tools, including supporting smaller OSPs to participate in crisis response. The Call can fill these gaps by building on the efforts already underway in the Community, with consideration paid to human rights and the impact of new tech, to support a free, open, and secure internet.

Thanks

Parts of this report are based on a doctoral dissertation[34] by Amy-Louise Watkin, in which she proposes a framework to regulate terrorist content online. In her framework, Dr. Watkin suggests that the awareness, capacity, and willingness of OSPs are the key obstacles to successful intervention against TVEC. We thank Dr. Watkin for her research and the time she spent providing advice to us on this topic.

We also thank all Call supporters and partners and the OSPs that participated in the consultation for this report. A particular thanks goes to the smaller OSPs who invested time speaking to us despite their limited time and staff.

Endnotes

[1] Christchurch Call. (2019). *The Christchurch Call to Action: To eliminate terrorist and violent extremist content online*.
[2] Christchurch Call. (2022, September 20). *Co-chair statement: Christchurch Call Leaders' Summit* [Press release].
[3] Siteefy. (2023). *How many websites are there in the world?*
[4] National Audit Office. (2023). *Preparedness for online safety regulation*.
[5] Kominers, S. D., & Wu, L. (2023, July 13). Threads foreshows a big – and surprising – shift in social media. *Harvard Business Review*.
[6] Abbing, R. R., Diehm, C., & Warreth, S. (2023). Decentralised social media. *Internet Policy Review*, *12*(1), 1-11. doi: 10.14763/2023.1.1681
[7] Department of Homeland Security. (2010). *Terrorist use of social networking Facebook case study*. Public Intelligence.
[8] Shehabat, A., & Mitew, T. (2018). Black-boxing the Black flag: Anonymous sharing platforms and ISIS content distribution tactics. *Perspectives on Terrorism*, *12*(1), 81-99.
[9] Weirman, S., & Alexander, A. (2020). Hyperlinked sympathizers: URLs and the Islamic State. *Studies in Conflict & Terrorism*, *43*(3), 239-257. doi: 10.1080/1057610X.2018.1457204
[10] Conway, M., Khawaja, Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2019). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict & Terrorism*, *42*(1-2), 141-160. doi: 10.1080/1057610X.2018.1513984
[11] Nouri, L., Lorenzo-Dus, N., & Watkin, A. (2021). Impacts of radical right groups' movements across social media platforms: A case study of changes to Britain First's visual strategy in its removal from Facebook to Gab. *Studies on Conflict & Terrorism*. doi: 10.1080/1057610X.2020.1866737
[12] Urman, A., & Katz, S. (2020). What they do in the shadows: Examining the far-right networks on Telegram. *Information, Communication & Society*, *25*(7), 904-923. doi: 10.1080/1369118X.2020.1803946
[13] Watkin, A. (2021). *Regulating terrorist content on tech platforms: A proposed framework based on social regulation* [Doctoral dissertation, Swansea University]. Cronfa.
[14] Tech Against Terrorism. (2019). *Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content – April 2019*.

[15] Institute for Strategic Dialogue. (2022). *Detours and diversions: Online strategies for the dissemination of right-wing extremist content*.
[16] Romaniuk, S. N., Fabe, A. P. H., & Nandy, D. (2023*). Terrorist platform migration: The move to smaller, less regulated online spaces*. Global Network on Extremism & Technology.
[17] Bradley, A., & Shadnia, D. (2022). *Examining online terrorist migration to terrorist and violent extremist-owned domains*. George Washington University Program on Extremism.
[18] Weimann, G., & Vellante, A. (2021). The dead drops of online terrorism: How jihadists use anonymous online platforms. *Perspectives on Terrorism*, *15*(4), 39-53.
[19] Office of the New York State Attorney General Latitia James. (2022). *Investigative report on the role of online platforms in the tragic mass shooting in Buffalo on May 14, 2022*.
[20] Ehsan, R., & Stott, P. (2020). *Far-right terrorist manifestos: A critical analysis*. Centre on Radicalisation & Terrorism.
[21] Ware, J. (2020). *Testament to murder: The violent far-right's increasing use of terrorist manifestos*. International Centre for Counter-Terrorism.
[22] Fielitz, M., & Thurston, N. (2018). *Post-digital cultures of the far right: Online actions and offline consequences in Europe and the US*. Transcript.
[23] Johnson, H., Volk, K., Serafin, R., Grajeda, C., & Baggili, I. (2022). Alt-tech social forensics: Forensic analysis of alternative social networking applications. *Forensic Science International: Digital Investigation*, *42*(1), 1-13. doi: 10.1016/j.fsidi.2022.301406
[24] Jasser, G., McSwiney, J., Pertwee, E., & Zannettou, S. (2023). 'Welcome to #GabFam': Far-right virtual community on Gab. *New Media & Society*, *25*(7), 1728-1745. doi: 10.1177/14614448211024546
[25] Tech Against Terrorism Europe. (2023). *European regulation on Terrorist Content Online (TCO)*.
[26] Online Safety.org.au. (2023). *Industry codes*.
[27] Bird & Bird. (2022). *Singapore introduces new law for online safety*.
[28] UK Government. (2023). *A guide to the Online Safety Bill*.
[29] Tech Against Terrorism. (2023, May 5). *Terrorist Content Analytics Platform launches in Canada* [Press release].
[30] PUBLIC. (2023). *The international state of safety tech*.
[31] Bernard, T. (2023, July 24). The evolving trust and safety vendor ecosystem. *Tech Policy Press*.
[32] Institute for Strategic Dialogue. (2023*). The hydra on the web: Challenges associated with extremist use of the fediverse – a case study of PeerTube*.
[33] Institute for Strategic Dialogue. (2023). *Inside the digital labyrinth: Right-wing extremist strategies of decentralisation on the internet and possible countermeasures*.
[34] Watkin, A. (2021). *Regulating terrorist content on tech platforms: A proposed framework based on social regulation* [Doctoral dissertation, Swansea University]. Cronfa.