



**COUNTER
TERRORISM
POLICING**



**METROPOLITAN
POLICE**

Dame Melanie Dawes DCB
Chief Executive of Ofcom

Matt Jukes QPM
Assistant Commissioner
Specialist Operations
New Scotland Yard
Richmond Terrace
Victoria Embankment
London
SW1A 2JL

Louisa Rolfe OBE
Assistant Commissioner
Frontline Policing
New Scotland Yard
Richmond Terrace
Victoria Embankment
London
SW1A 2JL

Ref: ACSO/31/24
4th April 2024

Dear Dame Melanie

Thank you for the opportunity to respond to your proposals in the Illegal Harms consultation. We are responding jointly on behalf of the Metropolitan Police Service and Counter Terrorism Policing.

The scope of the consultation is considerable and it reflects the experience and concerns that law enforcement has moderating online harmful content. We know that harmful content has the potential to create more powerful radicalising tools and materials that appeal to young people in particular.

The range and diversity of the content is almost as significant as the scale. We have spoken frequently about the impact the online world and the way in which we consume information is having on the ever-evolving threat of terrorism and serious organised crime. There is no doubt that our increasing dependence on digital spaces and networks is also having a profound effect on how extreme views may be formed, and how individuals become radicalised. Whilst innovative work within policing can help tackle the proliferation of harmful content, it is vital that technology companies also play their part. UK policing is already engaged in identifying and removing, then investigating those responsible for the proliferation of illegal and harmful online content.

At a working level, there has been extensive dialogue between our organisations and we are satisfied that our engagement has ensured that the consultation covered the areas of most concern to Counter Terrorism Policing and to wider policing. We note that you articulate a significant evidence base for your findings which correctly reflects our analysis of the online space.

This response concerns the Online Safety Act 2023 as passed by Parliament, and the role of Ofcom in regulation according to the legislation. In so doing, we have no doubt you will gain insights into the efficacy of the legislation. We see a good deal of potentially harmful content in our case work that will not be captured under the scope of the Act and therefore sit beyond your regulation. We would welcome the opportunity to determine how we can work with Ofcom to explore and capture the evidence of the limitations of this Act and the constraints of Ofcom's remit and resources, so that a future Government can continue to set its ambitions for legislation and regulation in the assertive, world-leading way that the threat environment requires.

Whilst the Act is an important tool in regulating the safety of online users in relation to user-generated content, it will only be successful if Ofcom is able properly to enforce its new duties. It is vital that technology companies play their part in tackling the proliferation of harmful content. We look to Ofcom to oversee and enforce the regime robustly and with rigour.

The UK's Counter-Terrorism Internet Referral Unit (CTIRU) works with internet service providers and tech companies to have extremist content removed. Where material is considered in breach of UK terrorism laws, the CTIRU will seek its removal, either by working with the internet service providers or hosting companies. The CTIRU will also alert police forces to online terrorist offences, to enable action against individuals who are engaged in the promotion, glorification, or encouragement of terrorist acts online. From the referrals, the CTIRU establishes if the content and purpose of posting breaches UK TACT legislation, other UK legislation or poses a safeguarding or significant risk or threat to the UK.

Since 2015, the CTIRU has facilitated the removal of over 300,000 pieces of content. In 2022, the UK CTIRU undertook more than 2,500 assessments of extremist or terrorist content, leading to around 5,000 pieces of content being removed.

Since the October 7th 2023 Hamas attacks in Israel and the escalation of the conflict, we have seen examples of where digitally manipulated content relating to the conflict's domestic implications have been shared online, with huge audiences. There has been a significant surge in referrals to the CTIRU about online content relating to the Israel-Hamas conflict. Materials requested by the CTIRU for removal include podcasts, sermons and memes as well as horrific footage from international events repurposed specifically for social media. Referrals also include screenshots of private conversations, direct messages and WhatsApp groups, all of which Counter-Terrorism Policing are assessing and triaging to the relevant part of policing.

Your draft Codes of Practice provide appropriate guidance for online platforms to moderate terrorist content. The Illegal Content Judgements Guidance provides a comprehensive and detailed analysis of the terrorism online. In focussing your Guidance on content that breaches TACT, online platforms should find it easier proactively to remove such content.

However, we are also seeing a rise of deep fake and AI generated content. Despite this sitting outside of current legislation we call on Ofcom to advise providers to manage the proliferation of harmful aspects of this technology.

We recognise the position asserted by you in relation to proscription and hash matching for terrorist content. It is clear that platforms should have a positive obligation to provide content from proscribed organisations. Counter Terrorism Policing maintain both hash set and URL databases for content that may indicate an extremist mindset or refers to material that may indicate an extremist mindset. We recognise the challenge in developing a dataset for provision to platforms and are willing to support Ofcom and the technology sector as you develop your own systems.

Counter Terrorism Policing has adopted the recommendation made by the Independent Reviewer of Legislation in his 2021 Annual Report of the Terrorism Acts. We are working with the Crown Prosecution Service to provide a formal list of content whose possession or dissemination has led to convictions in the United Kingdom under section 2 Terrorism Act 2006 or section 58 Terrorism Act 2000 in order to assist tech companies with content moderation decisions.

Serious Organised Crime (SOC) syndicates increasingly leverage online platforms to facilitate illicit activities, including but not limited to human trafficking, drug trafficking, financial crime and cyber-

enabled offences. These criminal enterprises thrive in the anonymity and accessibility afforded by the digital realm. The new measures will have the potential to reduce online-enabled SOC but it will need robust enforcement by you. There is still significant work to be done by platforms to identify and remove content relating to knife and drug sales.

We are keen to work closely with you to ensure that the new measures do not inadvertently hinder law enforcement's ability to monitor and combat criminal activities occurring in the online space. Collaboration between us, you and online platforms to develop effective mechanisms for identifying and removing illegal content without impeding ongoing criminal investigations is vital.

The implementation of the Online Safety Act provides a unique opportunity to tackle a vast range of online harm, but it will require significant enforcement and vigorous monitoring. We look forward to meeting you to discuss further these important issues.

Yours sincerely



Matt Jukes
Assistant Commissioner Specialist Operations
National Lead for CT Policing



Louisa Rolfe
Assistant Commissioner
Frontline Policing