Christchurch Call Advisory Network Submission to Ofcom Consultation On Protecting people from illegal harms online

23 February 2024

Thank you for the opportunity to provide a response to Ofcom's consultation on Protecting people from illegal harms online. The Christchurch Call Advisory Network (CCAN) is the civil society arm of the Christchurch Call community. CCAN's mission is to provide expert advice on implementing the commitments in the Call in a manner consistent with a free, open, and secure Internet and with international human rights law.

The Call objectives overlap significantly with various facets of the Online Safety Act, and CCAN members have a wide variety of relevant expertise. As Ofcom notes in Volume 1.11, "Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR)." CCAN has put together a concise response that highlights our collective knowledge in these areas, and in human rights and technology more broadly, specifically focusing on Ofcom's approach to moderation of terrorist and violent extremist content online.

Ofcom's assessment of the causes and impacts of online harms: Preserving a free, open, and secure Internet

CCAN maintains that there is a danger in simplistically framing encryption as a risk factor, given the potential use of encryption by terrorists, violent extremists and other actors intending to cause harm to others. CCAN agrees with the report that encryption is not inherently a risk and advocate that end to end encryption enables safe communication for people all around the world, from ordinary users to vulnerable populations, which is essential to both freedom of expression and privacy— two fundamental rights Ofcom has noted that are particularly relevant to the Online Safety Act.

Encryption is a technical feature that is vital for Internet security for two reasons: (1) it ensures the confidentiality and integrity of the data (for example in financial transactions) and (2) it reduces the vulnerabilities to ordinary Internet users. Establishing that service providers enable access is a technical matter that is not feasible due to how end-to-end encryption is implemented. Therefore, framing end to end encryption as a "service" increases risk that can potentially hamper the Christchurch Call commitment to upholding the principle of free, open

and secure Internet. Encryption is not a service that platforms and Internet actors are offering (like video streaming) but it is a technical feature essential for preserving the integrity and confidentiality of data on the Internet, due to a mathematical function, thus it is not and should not be treated as an additional "service". CCAN members Internet Society and Electronic Frontier Foundation (EFF) have written on the UK Online Safety Act and its effect on encryption which can be accessed here, and here.

Framing end-to-end encryption as a risk factor implies that there are actions that providers can take to mitigate this risk. At the same time, the Online Safety Act clearly states that Ofcom does not have the power to require the use of proactive content moderation technologies within encrypted environments, except for Child Sexual Exploitation and Abuse (CSEA) material.

Ofcom's framing of encryption as a risk factor places indirect pressure on providers that would effectively circumvent exceptions for E2EE laid out in the Online Safety Act, implicitly pushing service providers not to roll-out encryption on their services. CCAN members are strongly against this type of indirect pressure.

User access and account removal: Upholding freedom of expression
Ofcom suggests that "Accounts should be removed if there are reasonable grounds to infer they are run by or on behalf of a terrorist group or organisation proscribed by the UK Government." Such a categorical approach, is based on a much lower standard of evidence ("reasonable grounds to infer") than it would have been required under UK Criminal law. It also does not take into account the serious harms to freedom of expression, including access to information and important evidence of crimes including human rights violations, that such removals can cause.

Designated terrorist organizations are sometimes state-sponsored, part of elected governments, or have the resources to form quasi governments. Not all of their activities and accounts engage with terrorist activities, while some engage with providing public services and announcements. In certain circumstances, some designated terrorist organizations have governmental power obliging the local population to join compulsory military service, for example. Association with such accounts might not even be voluntary.

Removing suspected terrorist accounts without due diligence and without considering the impact on freedom of expression and on third parties' access to information hampers the UK's ability to uphold the following call commitment: "Respect, and for Governments to protect, human rights, including by avoiding directly or indirectly contributing to adverse human rights impacts through business activities and addressing such impacts where they occur."

Furthermore, despite Ofcom's acknowledgement in A2.4 that "it is not an offense to portray terrorism (for example in a video clip from a film or TV show) or to report on terrorism (for

example as news or current affairs)," categorical and low-evidence approaches to suspending accounts and removing content often leads to removal of reporting, and even condemnation, especially when combined with automated content moderation.

Instead of the proposed approach, the decision to remove accounts, and the access to all the information provided by such accounts, should be based on the type of content information such accounts are disseminating, rather than the fact accounts are on a list. Here is where CCAN very much agrees with Ofcom that: "Services should consider the purpose and meaning of content when making illegal content judgements, having regard to the whole context in which it appears. Ofcom would take into account a user's right to freedom of expression in enforcing the safety duty." (A.2.4, p.19)

However, A.2.18, allows for a broader interpretation: "Content which does none of the above, but which relates somehow to a proscribed organisation, may still be illegal content.". Considering accounts held by proscribed terrorist organizations as of higher risk sounds legitimate. However, in practice since the companies are usually very risk averse, there are limited attempts to contextualize illegal content and prefer not to allow for any kind of proscribed organization to have an account (a practice called 'collateral censorship').

In other words, Ofcom departs from positive obligations under UK law to determine criminal conduct, and gives a blank check to service providers to apply standards that breach basic legal standards to preserve human rights. This delegation of powers to the private sector under lowered standards could ultimately lead the courts to declare takedown decisions illegal under UK law. It is worth noting that the lack of transparency around removal notices made under ToS by the UK police have already been critiqued from a human rights perspective, including by the Oversight Board for Meta in a case[1] where it considered a request to remove a "drill rap" video under the company's terms of service rather than through a legal order.

Destruction of evidence

Removal and takedowns of certain types of content can result in harm including destruction of evidence, such evidence can be critical for law enforcement and/or international bodies like the International Criminal Court or investigations being carried out by the United Nations. This is further highlighted by CCAN members in this report for the Global Internet Forum to Counter Terrorism (GIFCT) and this whitepaper. Such removals would hinder the UK's ability to uphold the Call commitment to: "Ensure appropriate cooperation with and among law enforcement agencies for the purposes of investigating and prosecuting illegal online activity in regard to detected and/or removed terrorist and violent extremist content, in a manner consistent with rule

[1] Oversight Board, 2022-007-IG-MR, https://www.oversightboard.com/decision/IG-PT5WRTLW

of law and human rights protections." CCAN suggests Ofcom works to create an evidence preservation mechanism when such content does need to be removed for legal reasons. CCAN maintains that Ofcom should use a more holistic approach (if allowed by law) and consider the context and content by undertaking a human rights impact assessment to ascertain that informational content does not become inaccessible.

Information gathering and supervision: Ensuring Transparency

One "best practice" making the Christchurch Call innovative is the government and online service provider commitment to "Recognise the important role of civil society in supporting work on the issues and commitments in the Call." CCAN urges Ofcom to work with civil society to implement the Online Safety Act. CCAN understands that Ofcom has research, media literacy, and engagement functions and believes these can all be used to work with CCAN, as well as with individual civil society organizations, academics, and in particular groups representing impacted communities.This kind of relationship provides a dual function: (1.) CCAN as a Civil Society Organization provides technical advice and (2.) it is iterative, for example, it enables Ofcom to address potential pitfalls that correspond to preserving human rights, open, free and secure Internet.

"The statutory information gathering powers conferred on Ofcom by the Act give us the legal tools to obtain information in support of our online safety functions. These powers will help us to address the information asymmetry that exists between Ofcom and regulated services." (28.2). CCAN reminds Ofcom that this information asymmetry is even more drastic for civil society, and particularly for users and affected communities, and urges Ofcom to use its supervisory function and information notices in a transparent manner. These provisions of the Online Safety Act could enable Ofcom to share key information relevant to the impact of online service providers on human rights, for example providing transparency into companies' uses of the GIFCT database and number of takedowns done under terms of service rather than in response to legal orders.

However, used improperly or without sufficient public reporting, information notices could be used to circumvent legal protections in place for user privacy, or simply in a way that does not take into account the limitations of small, medium, and large companies. They could also further disadvantage civil society and users, who are already at a disadvantage in an uneven playing field when it comes to information asymmetry. Ofcom's supervisory functions more broadly could have the effect of creating opaque, bilateral relationships between government and companies, cutting out essential civil society input and hampering the UK's ability to carry out the Call Commitment of "Recognis[ing] the important role of civil society in supporting work on the issues and commitments in the Call, including through: Offering expert advice on implementing the commitments in this Call in a manner consistent with a free, open and secure

Internet and with international human rights law; [and] Working, including with governments and online service providers, to increase transparency." Finally, if used too extensively, some of the enforcement provisions could encourage companies to take sweeping measures to comply with the Online Safety Act that do not sufficiently consider the impact on users' rights.

We believe that Ofcom could also play a role in preserving researchers' data access. Such preservation could help with Civil Society Organizations consultation. Providing data access can surface issues Ofcom may not have noticed previously and then can act on in its regulatory capacity.

In sum, CCAN urges Ofcom to ensure it adheres to a free, open and secure Internet that is human rights compliant. CCAN strongly implores Ofcom to use its information gathering and supervisory powers in a transparent way that upholds the UK's Christchurch Call commitment to a free, open, and secure Internet.

Thank you for the opportunity to provide CANN's perspective at this stage of the Online Safety Act. CCAN encourages Ofcom to have continuous engagements with civil society organizations throughout its consultative phase and as it transitions to policy.

Sincerely,
Christchurch Call Advisory Network
Christchurchcall.network

Recommendations

1. We suggest Ofcom works to create an evidence preservation mechanism when such content does need to be removed for legal reasons. Such a mechanism should have strong privacy and legal protections for access alongside methods for international mechanisms to access preserved evidence. CCAN members would be willing to consult with the UK Government on such an initiative.

2. We urge Ofcom to work with civil society to implement the Online Safety Act. CCAN understands that Ofcom has research, media literacy, and engagement functions and believes these can all be used to work with CCAN, as well as with individual civil society organizations, academics, and in particular groups representing impacted communities.

3. CCAN suggest a more formalized role between companies and civil society that can contribute to meaningful engagement. Ofcom overwhelmingly relies on tech-companies and does not direct tech-companies to work with civil society. One of the Christchurch

Call commitments is to: “work with civil society to promote community-led efforts to counter violent extremism in all its forms, including through the development and promotion of positive alternatives and counter-messaging.” It is not clear whether Ofcom has plans to direct tech-companies to work with civil society.

4. CCAN advise Ofcom not to consider “encryption” as a risk.

5. CCAN suggest that Ofcom uses a more holistic approach (if allowed by law) and consider the context and content and undertake human rights impact assessment to ascertain that nonviolent, informational content does not become inaccessible. Such a mechanism must still protect privacy.

6. We recommend a stronger, proactive approach to addressing emerging threats as opposed to putting in place reactive measures. This must be done together with the tech sector and intersecting subject-matter experts and organizations. CCAN members would be willing to consult with the UK Government on such initiatives.