Home Office

Voluntary Guidance For Internet Infrastructure Providers On Preventing Terrorism Online

Contents

Introduction

Terrorist groups and individuals have long exploited the internet to share propaganda, recruit and inspire others, and facilitate attacks.

All elements of the internet eco-system have important roles to play in effectively reducing the availability and accessibility of terrorism content, mitigating the risk of radicalisation, and reducing the harm that it poses to society. Internet infrastructure providers provide the essential services that enable the internet to function and be accessible to users. They therefore have a key role to play in preventing terrorism online.

Infrastructure providers can, and should, also take steps to prevent the sharing and dissemination of Child Sexual Abuse Material (CSAM). This document is published alongside Voluntary Guidance for Infrastructure Providers on Tackling Online Child Sexual Exploitation and Abuse.

What is terrorism content?

Online terrorism content is any content which, by uploading it or otherwise making it available to others online, a person is committing an offence under UK terrorism laws. Terrorism content online can take many forms, including but not limited to statements, imagery (including still images and others such as GIFs), videos (both live and pre-recorded), voice recordings and documentation such as leaflets, papers and posters.[1] Schedule 5 of the Online Safety Act provides a comprehensive overview of related terrorism offences[2].

We are also concerned about Terrorist Operated Websites (TOW), which are websites set up by terrorists for recruitment purposes and to store and disseminate terrorist content. These websites are used by terrorists to maintain a consistent online presence and to avoid the moderation policies of social media platforms. Terrorist operated websites make use of a variety of internet infrastructure services to be accessible and available to users; they are easy to register, relatively stable and can quickly reappear following disruption, including by using techniques such as Top-Level Domain hopping.

How this guidance relates to other UK Government initiatives

This guidance is separate but complementary to the Online Safety Act 2023. Internet infrastructure providers are out of scope of the mandatory safety duties in the Online Safety Act, but could be required, by court order, to withdraw services from non-compliant regulated services as part of the business disruption measures set out within the Online Safety Act.

This guidance also builds on the Interim Code of Practice on Terrorist Content and Activity Online published by the Home Office in December 2020. Ofcom, as the new regulator for online safety in the UK, will publish its own Code of Practice for terrorism content. This will supersede the Interim Code published in 2020.

[1] Interim Code of Practice on Terrorist Content and Activity Online published by the Home Office in December 2020

[2] Schedule 5 of the Online Safety Act

How to use this guidance

The scope of this guidance is limited to the infrastructure layer of the internet. The responsibilities of user-to-user services to prevent terrorism on their services are separately set out in the Online Safety Act.

We have not set a fixed definition of 'infrastructure providers', but this term broadly refers to internet services that enable individual users to access websites, apps and other online content. We have suggested a non-exhaustive list, including web-hosting providers, Content Distribution Network (CDN) providers, registries, registrars, anonymising services, Internet Service Providers (ISPs), Mobile Network Operators (MNOs), browsers and app stores. We recognise that some companies will provide services across several of these categories. All infrastructure providers regardless of location are in scope of this guidance.

While not all the actions in this guidance will be relevant to all infrastructure providers, the guidance should provide a guiding framework when making decisions about how best to play a role in tackling terrorism online. While there is no legal obligation to act in accordance with this guidance, we encourage all infrastructure providers to consider this guidance carefully, reflect on how it applies to their services, and take all relevant and appropriate steps to help prevent terrorism online. This guidance is not meant to be static and will likely evolve over time. We welcome feedback on the guidance and suggestions of further examples of best practice.

The UK is committed to protecting fundamental rights, including freedom of expression and privacy, as well as to a free, open and secure internet. To ensure protections for freedom of expression, this guidance seeks to address only unlawful terrorism-related content and websites. Infrastructure providers should ensure any application of this guidance relating to their services is done so in a manner that promotes and protects human rights.

Companies will need to continue to respect laws in the countries in which they operate over and above this guidance, which should not affect companies' approach to existing or future legislation, and any other existing legal obligations.

Actions for infrastructure provider companies to consider are set out in the sections below. Companies should consider actions for all infrastructure providers in Section 1, and then may also wish to consider the appropriate service-specific actions in Section 2.

Section 1:
Actions For All Infrastructure Providers

Under the United Kingdom's Terrorism Act 2006, an individual or a company, including internet infrastructure providers, may become liable for disseminating unlawful terrorism content if they are notified of such content by the police. Internet infrastructure providers are required to follow their legal obligations and act upon the police notice in such circumstances.

The offence of disseminating terrorist content under section 2 of the Terrorism Act 2006 does not necessarily require intention and may be committed recklessly (e.g. in circumstances where someone has been reckless as to whether an effect of their conduct amounts to the provision of assistance in the commission or preparation of encouragement to terrorism). The offence extends to circumstances in which a service is provided which, as a result of that service, enables others to access a terrorist publication. It also applies to the transmission of a terrorism publication.

By contrast, there is no legal obligation to act in accordance with this guidance, but we encourage all providers to consider the guidance and to take proactive steps to achieve the following outcomes:

1. **Services and products are safeguarded against exploitation for terrorism-related purposes.** Where applicable, providers should assess the risk of their services being exploited for terrorism-related purposes and should put in place adequate safety mitigations.

2. **The accessibility and operability of terrorist operated websites is reduced.** The relevant provider(s) should take steps to reduce the accessibility and operability of a terrorist operated website exploiting their internet infrastructure service(s), including by reducing the ability of a terrorist operated website to recover full operability following disruption of service. The means to do this will differ depending on the nature of the infrastructure provider, but all providers should consider what steps they can reasonably and practically take.

3. **The accessibility and availability of terrorism content online is reduced.** Where applicable, infrastructure providers should consider utilising available tools appropriate to their specific architecture to identify terrorism content and take steps to reduce its accessibility and availability.

Actions that may help infrastructure providers achieve the above outcomes are set out below:

1. Safety by design

Incorporate safety considerations into the design of products and services. Where applicable, infrastructure providers should assess the risk of their services being exploited for terrorism-related purposes and consider adequate safety mitigations. Providers may also wish to take steps to ensure their customers cannot use their services to bypass safety features on other services.

As technologies, such as Artificial Intelligence (AI) and machine learning, develop at pace many mitigations could be, and in some cases already are, implemented using AI. AI should not be relied on as a sole decision maker but rather should be used to support human decision-making. Where applicable, providers should consider how to integrate this technology safely and responsibly into their services. Any AI abilities should be kept up to date and should consider the rules for what AI can generate, in addition to being aware of bad users' attempts to bypass those rules.

2. Terms of Service

Ensure and appropriately enforce Terms of Service that prohibit terrorist use. All infrastructure providers should make clear in their Terms of Service that use of their services for terrorism-related purposes is prohibited. Providers may additionally wish to make clear that customers utilising their services should also seek to prohibit terrorism content and activity on their own services. Terms of service should be clear, easy to navigate and easily accessible.

Infrastructure providers should consider what processes they can put in place to ensure and encourage customers to adhere to their Terms of Service. In the instance of a breach of terms relating to terrorism, infrastructure providers should consider appropriate enforcement action. Consequences for Terms of Service violations should serve as a meaningful deterrent. To enable enforcement, infrastructure providers should consider implementing effective 'Know Your Customer' checks proportionate to the risks faced by the service, to ensure that customers are identifiable and contactable in the event of a Terms of Service breach.

3. Identification and reporting mechanisms

Establish mechanisms to proactively identify and receive reports of terrorist exploitation. All infrastructure providers should consider what steps they can reasonably and practically take to identify and prevent terrorist use of their services. Infrastructure providers should ensure that they have in place effective and easy-to-use processes to ensure that they can receive reports of terrorism-related exploitation of their services from individual users, civil society, and trusted flaggers. Companies should ensure that reports are responded to in a timely and clear way, and that there is a function to appeal or dispute outcomes. In addition, companies should have the resources and manpower to quickly and effectively triage and action the reports that they receive. Infrastructure providers may also wish to operate a trusted flagger programme to be alerted to known terrorist operated websites or terrorism content from trusted sources. Where applicable, we would particularly encourage infrastructure providers to make use of Tech Against Terrorism's Terrorist Content Analytics Platform, which provides alerts to companies, as well as their Knowledge Sharing Platform, which contains a comprehensive list of proscribed terrorist organisations, including associated imagery and logos, as well as a list of known terrorist operated websites.

4. Cooperation with law enforcement

Quickly report imminent threats to life, or of serious physical injury, to the police. Companies wishing to follow best practice should voluntarily report to UK law enforcement any suspicion of an imminent threat to life or serious physical injury (with a clear UK connection) that may be detected or flagged to them. This is in addition to complying with legal obligations relating to referrals of unlawful terrorism-related content by the UK police.

5. Transparency

Publish transparency reports on tackling terrorism online. Where applicable, infrastructure providers should consider publishing transparency reports and sharing relevant data on (1) terms of service enforcement relating to terrorism, and (2) efforts to safeguard service provision from exploitation for terrorism-related purposes. This will help to build public confidence in the steps being taken by infrastructure providers and may also contribute to building greater understanding of the terrorism threat online.

6. Multi-stakeholder engagement

Work with others to share understanding and approaches for safeguarding against terrorist exploitation. Infrastructure providers should look to engage and work with other infrastructure providers as well as a range of cross-sector stakeholders, including other companies, governments and civil society organisations, to share relevant expertise and best practice. Providers may want to work with global initiatives such as the Global Internet Forum to Counter Terrorism, the Christchurch Call to Action or with organisations such as Tech Against Terrorism. Companies are encouraged to maintain relationships with governments and law enforcement agencies in countries where they operate. This will help to identify key challenges, develop a shared understanding of the threat landscape, and share best practice.

Section 2:
Service-Specific Actions

This section provides suggestions of best practice that specific types of providers can take to safeguard their services, reduce the accessibility and operability or terrorist operated websites, and reduce the accessibility and availability of terrorism content. This section is not designed to be prescriptive or to provide an exhaustive list of actions, but instead it should be illustrative of the types of actions that infrastructure providers can take. Some infrastructure providers may offer multiple types of service. In this guidance, we have grouped providers as follows:

- Internet Service Providers and Mobile Network Operators
- Content Distribution Network providers
- Anonymising services
- Domain Name System registration services
- Web-Hosting Providers
- Browsers
- App stores

1. Internet Service Providers (ISP) and Mobile Network Operators (MNO)

You may wish to consider:

- Using appropriate filtering tools/ lists to prevent access to known URLs of terrorist operated websites or terrorism content.
- Displaying splash pages when users try to access URLs containing known terrorism content.
- Where possible, taking reasonable steps to retain relevant data when voluntarily reporting to law enforcement whilst remaining compliant with other legal obligations for data protection.

2. Content Distribution Network providers

You may wish to consider:

- Using appropriate tools to identify whether Content Distribution Network services are being exploited for the purpose of facilitating access to known terrorist operated websites or terrorism content.
- Taking proportionate enforcement action upon a breach of terms of service relating to terrorism, including by removing services from terrorist operated websites or repository sites directing users to terrorism content on other sites.
- Where possible, taking reasonable steps to retain relevant data when voluntarily reporting to law enforcement whilst remaining compliant with other legal obligations for data protection.

3. Anonymising services (e.g. VPNs or proxies)

You may wish to consider:

- Where possible, using appropriate tools to identify and block access to known URLs containing terrorism content.
- Using URL filter lists to prevent access to URLs containing terrorism content.
- Taking steps to ensure customers cannot use services to bypass safety features on other services.

4. Domain Name System registration services (e.g. registries and registrars)

You may wish to consider:

- Removing or suspending domains that direct users towards terrorism content.
- Where feasible, taking steps to prevent top level domain hopping by terrorist operated websites, including by exploring opportunities for greater information sharing between registries.
- Where possible, taking reasonable steps to retain relevant data when voluntarily reporting to law enforcement whilst remaining compliant with other legal obligations including those relating to data protection.

5. Web-Hosting Providers

You may wish to consider:

- Using appropriate tools to identify whether hosting services are being exploited for the purpose of facilitating access to known terrorist operated websites or terrorism content.
- Taking appropriate enforcement action upon a breach of terms of service relating to terrorism, including by removing services from terrorist-operated websites.
- Where possible, taking reasonable steps to retain relevant data when voluntarily reporting to law enforcement whilst remaining compliant with other legal obligations including those relating to data protection.

6. Browsers

You may wish to consider:

- Using appropriate filtering tools/lists to prevent access to known URLs of terrorist operated websites or containing terrorism content.
- Displaying splash pages when users try to access URLs containing known terrorism content.
- Preventing auto-complete for searches associated with terrorism content.

- Where possible, taking reasonable steps to retain relevant data when voluntarily reporting to law enforcement whilst remaining compliant with other legal obligations including those relating to data protection.
- Where AI tools are embedded into browsers, ensuring that these tools prevent the generation or amplification of unlawful terrorism content.
- Taking steps to ensure customers cannot use browser services to bypass safety features on other services.

7. App Stores

You may wish to consider:

- Adopting the UK Government's Code of practice for app store operators and app developers
- Ensuring that there is a robust review and update process for new apps before they are made available on app stores.
- Including policies for app developers that prohibit apps from being developed for terrorism-related purposes.
- Requiring all apps that host third-party content to have moderation tools in place that can be used to report, block and remove terrorism content.
- Offering training for app developers on safety by design to prevent unlawful terrorism content on apps.

Next Steps

This guidance is a first step in setting out the UK Government's expectations and proposals for what infrastructure providers may consider doing to limit the risks of terrorist exploitation of internet infrastructure services. We hope that this can provide the basis for ongoing discussion, including about best practice efforts to prevent terrorism online. To get in touch, please contact the Preventing Radicalisation Online team in the Home Office at online.policy.unit@homeoffice.gov.uk

Definitions

- **Proscribed Group:** This is a terrorist group or organisation banned under UK law. Further detail about proscription in the UK and a list of UK proscribed groups can be found here.
- **Terrorist Operated Website:** A Terrorist Operated Website (TOW) is a website that is owned or operated by or in support of a proscribed terrorist group.
- **Top-Level Domain (TLD):** Domains at the top of the domain name hierarchy. For example .com, .org and .info are examples of generic Top-Level Domains (gTLDs). The term also covers country code Top-Level Domains (ccTLDs) like .uk for UK or .us for US and sponsored Top-Level Domains (sTLDs) like .mobi or .xxx[3]

[3] Glossary Of Terms - Internet Watch Foundation (iwf.org.uk)

- **Top-Level Domain hopping:** Top-Level Domain hopping is where a website containing certain illegal material is taken down, but then reappears with the exact same second level domain name under a different Top-Level Domain.
- **Trusted Flagger:** An organisation that is considered to be a trusted source with expertise for identifying and reporting content or behaviour that is illegal or violating a service's terms and conditions.