Radicalisation websites

About ISPA

The Internet Services Providers' Association (ISPA) UK is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry.

ISPA's membership includes small, medium and large Internet Service Providers (ISPs), cable companies, content providers, web design and hosting companies and a variety of other organisations. ISPA currently has over 200 members, representing more than 98% of the UK Internet access market by volume.

Background to the legal framework

The regulatory framework that underpins the UK internet industry is the eCommerce Directive, which was transposed in 2002 in the UK as the eCommerce Regulations. It attributes different degrees of liability to different types of online intermediaries according to the role they play in the internet eco-system.

Access providers are commonly referred to as ISPs (internet service providers) but are more accurately described as internet access providers. They connect customers to the internet, either through fixed or wireless connectivity. As access providers only pass traffic across a network, they are deemed 'mere conduits' under e-Commerce Regulation 17, and are exempted from liability[1] in recognition of the fact that they play no role in the content of the communications they carry: i.e., they do not determine what it is, they simply carry it from one place to another.

Hosting providers host others' content online, from the websites of large corporations to individual's personal websites or user generated content posted on websites. Under e-Commerce Regulation 19, hosting providers are not liable for the content they host as long as they do not have actual knowledge of unlawful activity or information. However, upon obtaining such knowledge, hosting providers must act expeditiously to remove or disable access to the information, and may become liable if they fail to act. This affords online intermediaries limited liability over the content they host and access they provide.

The 2006 Terrorism Act created several new offences of relevance to online content. Section 1 created an offence of encouragement of terrorism, Section 2 the dissemination of terrorist publications and Section 3 the application of notices to intermediaries in relation to section 1 and 2.

Response to questions

1. **The extent to which you think UK ISPs host material posted by violent extremist groups;**

The majority of 'violent extremist' content is hosted abroad and not in the UK. The Home Office itself has said that the "great majority" of terrorist-related websites of most concern are hosted abroad.[2] Such material is likely to be hosted in countries where legal protections are different than the UK, such as the US where the First Amendment affords greater protection and thus enables content to be more freely hosted.

[1] As mere conduits access providers "shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as result of that transmission." (e-Commerce Regulation 17).
[2] PREVENT Strategy, p.37

Furthermore, UK companies act responsibly and cooperate with law enforcement. Importantly this is backed up by legislation, the 2006 Terrorism Act, which contains the offences of encouragement of terrorism and dissemination of terrorist material. If an ISP failed to remove the content upon receipt of a valid notice under Section 3 of the Act, it would be committing an offence.

2. **Your policy (if you have one) for removing material linked to violent extremist movements upon request from the authorities, or a comment on what the usual practice is amongst ISPs;**

If law enforcement approaches a hosting provider under the Terrorism Act provisions regarding liability for hosting terrorist content, they are compelled to take it down. ISPA worked closely with the Home Office around the legislation and helped provide guidance on the serving of Section 3 notices under the Terrorism Act. Where this is not the case, or where the material is not covered by the Terrorism Act, then it will depend on individual ISP's policies on taking down content.

As the Committee may be aware, government and law enforcement have set up a unit, the Counter Terrorism Internet Referral Unit (CTIRU), which enables members of the public to anonymously report violent extremism. This is then reviewed by the CPS and if it meets the threshold as set out in the legislation and is hosted within the UK, a notice may be sent requesting that the content be removed. As the content reported is analysed using the existing legislation, this takes the burden away from an intermediary.

3. **Any legal or other obstacles you face in removing such material;**

When Section 3 notices of the Act are invoked to remove material then there is no issue; when they're not invoked it becomes more problematic. As in other areas, ISPs are not best placed to determine what constitutes violent extremism and where the line should be drawn. This is particularly true of a sensitive area like radicalisation, with differing views on what may constitute violent extremist. Whilst there may be clear instances of material that breaches the Terrorism Act, in other, more ambiguous cases, our members lack the clarity of over what constitutes 'actual knowledge' and whether the content need be removed.

If material is hosted outside of the UK then an UK intermediary is unable to remove it. To improve this, greater international cooperation could be explored, although what constitutes violent extremist under the law in one country is not necessarily the same elsewhere.

4. **Whether ISPs themselves take pro-active steps to monitor and remove material, and whether it would be reasonable to expect them to do so.**

ISPs generally do not monitor material they host. They often have neither the resources nor expertise and legally are not compelled to do so. Recital 47 of the ECD explicitly states that there is no obligation to monitor.

We find it impractical for ISPs to be expected to proactively monitor material given the sheer volume of content online, and undesirable given the implications for freedom of expression. As Government itself acknowledged in November last year at the London Cyber Conference, it is important that freedom of expression online is maintained. By compelling ISPs to monitor content on contentious areas, there is a potential chilling effect on industry and a risk of making private companies moral arbiters. That said, some online services and communities may choose to have individual policies of removing content and employ moderators to review and remove content.

Instead of proactively monitoring content, the current approach of notice and takedown, which is backed up with a legislative framework, is the most effective and practical solution. This is demonstrated by the low volume of violent extremist content hosted in the UK.