Internet safety laws strengthened to fight Russian and hostile state disinformation

- Social media platforms will have to proactively look for and remove disinformation from foreign state actors which harms the UK
- Firms failing to tackle online interference by rogue states face huge fines or being blocked

Social media platforms will have to proactively tackle Russian and other state-sponsored disinformation aimed at undermining the UK under changes ministers are making to new internet safety laws.

Many people are concerned about the threat that malicious state-linked disinformation poses to UK society and democracy, particularly following Russia's brutal invasion of Ukraine.

The government will table an amendment to link the National Security Bill with the Online Safety Bill – strengthening this landmark and pioneering internet legislation to make the UK the safest place in the world to go online. A new Foreign Interference Offence created by the National Security Bill will be added to the list of priority offences in the Online Safety Bill.

It means social media platforms, search engines and other apps and websites allowing people to post their own content will have a legal duty to take proactive, preventative action to identify and minimise people's exposure to state-sponsored or state-linked disinformation aimed at interfering with the UK.

This includes tackling material from fake accounts set up by individuals or groups acting on behalf of foreign states to influence democratic or legal processes, such as elections and court proceedings, or spread hacked information to undermine democratic institutions.

Digital Secretary Nadine Dorries said:

> The invasion of Ukraine has yet again shown how readily Russia can and will weaponise social media to spread disinformation and lies about its barbaric actions, often targeting the very victims of its aggression. We cannot allow foreign states or their puppets to use the internet to conduct hostile online warfare unimpeded.
>
> That's why we are strengthening our new internet safety protections to make sure social media firms identify and root out state-backed disinformation.

Security Minister Damian Hinds said:

> Online information operations are now a core part of state threats activity. The aim can be variously to spread untruths, confuse, undermine confidence in democracy, or sow division in society.
>
> Disinformation is often seeded by multiple fake personas, with the aim of getting real users, unwittingly, then to ‘share’ it. We need the big online platforms to do more to identify and disrupt this sort of coordinated inauthentic behaviour. That is what this proposed change in the law is about.

Platforms will need to do risk assessments for content which is illegal under the Foreign Interference Offence and put in place proportionate systems and processes to mitigate the possibility of users encountering this content.

This could include measures such as making it more difficult to create large scale fake accounts or tackling the use of bots in malicious disinformation campaigns. When moderating their sites, the firms will need to make judgments about the intended effect of content or behaviour which they have reasonable grounds to believe is state-sponsored disinformation and whether it amounts to misrepresentation.

These judgements could be based on patterns of behaviours and tactics used, or aided by relevant knowledge of the political and geopolitical context, for example narratives from state-backed media being amplified online.

To help platforms in carrying out this duty, companies will also be able to draw on the regulator Ofcom’s codes of practice. Ofcom will have the power to fine companies failing to act up to ten per cent of their annual global turnover, force them to improve their practices and block non-compliant sites.

Foreign Interference Offence

Under the National Security Bill, which is due in Parliament for Committee Stage next week, a new offence of foreign interference is established to deter and disrupt state threats activity including state-linked disinformation which undermines the UK.

It will make it illegal for a person to engage in conduct for, on behalf of or with intent to benefit a foreign power in a way which interferes in UK rights, discredits our democratic intuitions, manipulates people’s participation in them and undermines the safety or interests of the UK.

The offence includes conduct that involves making false or misleading misrepresentations, including using information which is true but presented in a misleading way or misrepresenting a person’s identity

Online Safety Bill as drafted

As it is currently drafted, the Online Safety Bill will already force companies to take action on state-sponsored disinformation which is illegal and where there is harm to individuals – for example if it contains a threat to kill. Companies whose services are likely to be accessed by children will need to protect underage users from harmful misinformation and disinformation.

Additionally, Category 1 companies will need to address misinformation and disinformation which is harmful and could be accessed by adults – such as dangerous anti-vaccine theories or fake coronavirus cures. They will need to set out clearly whether this content is allowed in their terms of service, and enforce this consistently.

The Bill has strong protections for people's rights to freedom of expression. Clause 19 provides specific safeguards against the over-removal of content and requires platforms to have due regard for users' right to free expression. Companies will also have a duty to ensure they have effective and accessible reporting and redress mechanisms so that users can easily challenge wrongful content takedown decisions.

ENDS

Notes to Editor

- As the list of priority offences in Schedule 7 of the Online Safety Bill cannot include offences that are not yet law, the amendment has been tabled to the National Security Bill to ensure that once the Online Safety Bill gains Royal Assent, it contains the most up to date version of the Foreign Interference Offence.
- The list of priority offences, which can be further updated by regulations, already includes:
  terrorism, child sexual abuse and exploitation, assisting suicide, threats to kill, public order offences, harassment and stalking, hate crime, the sale of illegal drugs and weapons, people trafficking offences, exploiting prostitutes for gain, extreme pornography, revenge pornography, proceeds of crime offences, and fraud offences.
- More information on the Home Office's National Security Bill.