

Online safety law to be strengthened to stamp out illegal content

- List includes online drug and weapons dealing, people smuggling, revenge porn, fraud, promoting suicide and inciting or controlling prostitution for gain
- New criminal offences will be added to the bill to tackle domestic violence and threats to rape and kill
- Flagship UK laws to protect people online are being toughened up with new criminal offences and extra measures to force social media companies to stamp out the most harmful illegal content and criminal activity on their sites quicker.

Digital Secretary Nadine Dorries today announced extra priority illegal offences to be written on the face of the bill include revenge porn, hate crime, fraud, the sale of illegal drugs or weapons, the promotion or facilitation of suicide, people smuggling and sexual exploitation. Terrorism and child sexual abuse are already included.

Previously the firms would have been forced to take such content down after it had been reported to them by users but now they must be proactive and prevent people being exposed in the first place.

It will clamp down on pimps and human traffickers, extremist groups encouraging violence and racial hate against minorities, suicide chatrooms and the spread of private sexual images of women without their consent.

Naming these offences on the face of the bill removes the need for them to be set out in secondary legislation later and Ofcom can take faster enforcement action against tech firms which fail to remove the named illegal content.

Ofcom will be able to issue fines of up to 10 per cent of annual worldwide turnover to non-compliant sites or block them from being accessible in the UK.

Three new criminal offences, recommended by the Law Commission, will also be added to the Bill to make sure criminal law is fit for the internet age.

Digital Secretary Nadine Dorries said:

This government said it would legislate to make the UK the safest place in the world to be online while enshrining free speech, and that's exactly what we are going to do. Our world leading bill will protect children from online abuse and harms, protecting the most

vulnerable from accessing harmful content, and ensuring there is no safe space for terrorists to hide online.

We are listening to MPs, charities and campaigners who have wanted us to strengthen the legislation, and today's changes mean we will be able to bring the full weight of the law against those who use the internet as a weapon to ruin people's lives and do so quicker and more effectively.

Home Secretary Priti Patel said:

The internet cannot be a safe haven for despicable criminals to exploit and abuse people online.

Companies must continue to take responsibility for stopping harmful material on their platforms. These new measures will make it easier and quicker to crack down on offenders and hold social media companies to account.

The new communications offences will strengthen protections from harmful online behaviours such as coercive and controlling behaviour by domestic abusers; threats to rape, kill and inflict physical violence; and deliberately sharing dangerous disinformation about hoax Covid-19 treatments.

The government is also considering the Law Commission's recommendations for specific offences to be created relating to cyberflashing, encouraging self-harm and epilepsy trolling.

To proactively tackle the priority offences, firms will need to make sure the features, functionalities and algorithms of their services are designed to prevent their users encountering them and minimise the length of time this content is available. This could be achieved by automated or human content moderation, banning illegal search terms, spotting suspicious users and having effective systems in place to prevent banned users opening new accounts.

New harmful online communications offences:

Ministers asked the Law Commission to review the criminal law relating to abusive and offensive online communications in the Malicious Communications Act 1988 and the Communications Act 2003.

The Commission found these laws have not kept pace with the rise of smartphones and social media. It concluded they were ill-suited to address online harm because they overlap and are often unclear for internet users, tech companies and law enforcement agencies.

It found the current law over-criminalises and captures 'indecent' images shared between two consenting adults – known as sexting – where no harm is caused. It also under-criminalises – resulting in harmful communications

without appropriate criminal sanction. In particular, abusive communications posted in a public forum, such as posts on a publicly accessible social media page, may slip through the net because they have no intended recipient. It also found the current offences are sufficiently broad in scope that they could constitute a disproportionate interference in the right to freedom of expression.

In July the Law Commission recommended more coherent offences. The Digital Secretary today confirms new offences will be created and legislated for in the Online Safety Bill.

The new offences will capture a wider range of harms in different types of private and public online communication methods. These include harmful and abusive emails, social media posts and WhatsApp messages, as well as 'pile-on' harassment where many people target abuse at an individual such as in website comment sections. None of the offences will apply to regulated media such as print and online journalism, TV, radio and film.

The offences are:

A 'genuinely threatening' communications offence, where communications are sent or posted to convey a threat of serious harm.

This offence is designed to better capture online threats to rape, kill and inflict physical violence or cause people serious financial harm. It addresses limitations with the existing laws which capture 'menacing' aspects of the threatening communication but not genuine and serious threatening behaviour.

It will offer better protection for public figures such as MPs, celebrities or footballers who receive extremely harmful messages threatening their safety. It will address coercive and controlling online behaviour and stalking, including, in the context of domestic abuse, threats related to a partner's finances or threats concerning physical harm.

A harm-based communications offence to capture communications sent to cause harm without a reasonable excuse.

This offence will make it easier to prosecute online abusers by abandoning the requirement under the old offences for content to fit within proscribed yet ambiguous categories such as "grossly offensive," "obscene" or "indecent". Instead it is based on the intended psychological harm, amounting to at least serious distress, to the person who receives the communication, rather than requiring proof that harm was caused. The new offences will address the technical limitations of the old offences and ensure that harmful communications posted to a likely audience are captured.

The new offence will consider the context in which the communication was sent. This will better address forms of violence against women and girls, such as communications which may not seem obviously harmful but when looked at in light of a pattern of abuse could cause serious distress. For example, in the instance where a survivor of domestic abuse has fled to a secret

location and the abuser sends the individual a picture of their front door or street sign.

It will better protect people's right to free expression online. Communications that are offensive but not harmful and communications sent with no intention to cause harm, such as consensual communication between adults, will not be captured. It will have to be proven in court that a defendant sent a communication without any reasonable excuse and did so intending to cause serious distress or worse, with exemptions for communication which contributes to a matter of public interest.

An offence for when a person sends a communication they know to be false with the intention to cause non-trivial emotional, psychological or physical harm.

Although there is an existing offence in the Communications Act that captures knowingly false communications, this new offence raises the current threshold of criminality. It covers false communications deliberately sent to inflict harm, such as hoax bomb threats, as opposed to misinformation where people are unaware what they are sending is false or genuinely believe it to be true. For example, if an individual posted on social media encouraging people to inject antiseptic to cure themselves of coronavirus, a court would have to prove that the individual knew this was not true before posting it.

The maximum sentences for each offence will differ. If someone is found guilty of a harm based offence they could go to prison for up to two years, up to 51 weeks for the false communication offence and up to five years for the threatening communications offence. The maximum sentence was six months under the Communications Act and two years under the Malicious Communications Act.

Professor Penney Lewis, Commissioner for Criminal Law, said:

The criminal law should target those who specifically intend to cause harm, while allowing people to share contested and controversial ideas in good faith. Our recommendations create a more nuanced set of criminal offences, which better protect victims of genuinely harmful communications as well as better protecting freedom of expression.

I am delighted that the Government has accepted these recommended offences.

ENDS

Notes to Editors:

Extending the list of priority offences in the Online Safety Bill

The draft Online Safety Bill in its current form already places a duty of care on internet companies which host user-generated content, such as social media and video-sharing platforms, as well as search engines, to limit the

spread of illegal content on these services. It requires them to put in place systems and processes to remove illegal content as soon as they become aware of it but take additional proactive measures with regards to the most harmful 'priority' forms of online illegal content.

The priority illegal offences currently listed in the draft bill are terrorism and child sexual abuse and exploitation, with powers for the DCMS Secretary of State to designate further priority offences with Parliament's approval via secondary legislation once the bill becomes law. In addition to terrorism and child sexual exploitation and abuse, the further priority offences to be written onto the face of the bill includes illegal behaviour which has been outlawed in the offline world for years but also newer illegal activity which has emerged alongside the ability to target individuals or communicate en masse online.

This list has been developed using the following criteria: (i) the prevalence of such content on regulated services, (ii) the risk of harm being caused to UK users by such content and (iii) the severity of that harm.

The offences will fall in the following categories:

- Encouraging or assisting suicide
- Offences relating to sexual images i.e. revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences – harassment and stalking
- Drug-related offences
- Weapons / firearms offences
- Fraud and financial crime
- Money laundering
- Controlling, causing or inciting prostitutes for gain
- Organised immigration offences

The Law Commission's review of harmful online communications

In 2019 the Law Commission began a review of the law relating to abusive and offensive communications. This review, sponsored by the Department for Digital, Culture, Media and Sport, considered whether criminal offences in England and Wales sufficiently captured harmful communications online. In particular, it considered: Section 1 of the Malicious Communications Act 1988 which criminalises the sending of communications that are indecent, grossly offensive, a threat, or false to another person, where the sender's purpose is to cause 'distress or anxiety'.

Section 127(1) of the Communications Act 2003 which criminalises the sending, via a 'public electronic communications network', of a message which is 'grossly offensive or of an indecent, obscene or menacing character,'.

Section 127(2) of the Communications Act 2003 which criminalises sending a message which is known to be false for the purpose of causing 'annoyance, inconvenience, or needless anxiety' to another.

The Commission published the final report of its review of harmful online communications and the role of the criminal law in combatting that behaviour, 'Modernising Communication Offences,' in July 2021. The government has today published its interim response to the Law Commission's report and confirmed it will take forward recommendations for three new offences – a harm-based offence, a false communications offence and a threatening communications offence.

The draft Online Safety Bill is focussed on the regulation of online platforms, while the new criminal offences apply to individuals. The new offences complement the regulatory regime and will help to achieve the bill's aim of making the UK a safer place to be online.