HM Government

Online Harms White Paper

April 2019

CP 57

them very few alternative, safer online services. For example, the 2018 Doteveryone Digital Attitudes[19] report found that almost half of respondents felt they had no choice but to sign up to online services, even where they had concerns.

Tackling online anonymous abuse — Box 6

The internet can be used to harass, bully or intimidate. In many cases of harassment and other forms of abusive communications online, the offender will be unknown to the victim. In some instances, they will have taken technical steps to conceal their identity. Government and law enforcement are taking action to tackle this threat.

- The police have a range of legal powers to identify individuals who attempt to use anonymity to escape sanctions for online abuse, where the activity is illegal. The government will work with law enforcement to review whether the current powers are sufficient to tackle anonymous abuse online.
- We are enhancing law enforcement's ability to tackle anonymous online abuse by investing in training that is designed to improve digital capability across policing. For example, as part of the £4.6 million Police Transformation Fund allocated by the Home Office, the Digital Investigation and Intelligence programme will build police capability to respond to the full range of digital crime types, through investment in technology and training.
- We are also making it easier for the public to report online crimes. Through the Digital Public Contact programme, we will provide the public with a digitally accessible police force with a consistent set of online capabilities to use in engaging and transacting with police services through a single online channel.
- We also expect companies to do substantially more to keep their users safe and counter online abuse, particularly where this is illegal. Companies need to take responsibility for tackling abusive behaviour on their services. More detail is set out in Chapter 3.

Online harms suffered by children and young people

1.17 Being online can be a hugely positive experience for children and young people – see Box 7. Recent research by internet Matters found that seven in ten parents think screen time is essential for their children's learning development and two thirds of parents feel that devices give their children another outlet for creativity, particularly so for children aged 6-10.[20]

1.18 However, the impact of harmful content and activity can be particularly damaging for children, as set out in Box 1 above and Boxes 8-10 below. There is also growing concern about the relationship between social media and the mental health of children and young people. The Children's Commissioner's report published in November 2018 *Who knows what about me* sets out the huge size and growth of children's digital footprint and the associated

19 Doteveryone (2018). People, Power and Technology: The 2018 Digital Attitudes Report. Available at: https://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

20 Internet Matters (2018). Look Both Ways: Practical Parenting in the Age of Screens. Available at: https://www.Internetmatters.org/about-us/screen-time-report-2018/

risks and benefits.[21] Internet Matters reported in February 2019 that vulnerable young people are more likely to suffer online harms and less likely to receive online safety advice and education.[22]

The positive impact of being online for children and young people — Box 7

Most children have a positive experience online, using the internet for social networking and connecting with peers, as well as to access educational resources, information, and entertainment. The internet opens up new opportunities for learning, performance, creativity and expression.

- A literature review by the UK Council for Child Internet Safety (2017) highlights evidence that young people recognise the positive role of the internet in relation to self-expression, developing understanding, bringing people together and respecting and celebrating differences. [23] Research by UNICEF (2017) shows that use of technology is beneficial for children's social relationships, enabling them to enhance existing relationships and build positive friendships online.[24]
- A report by The Royal Society for Public Health in 2017 found that young people reading blogs or watching vlogs on personal health issues helped improve their knowledge and understanding, prompted individuals to access health services, and enabled them to better explain their own health issues or make better choices.[25] They also found that young people are increasingly turning to social media as a means of emotional support to prevent and address mental health issues.
- More recently, research by Ofcom showed that nine in ten social media users aged 12-15 state that this use has made them feel happy or helped them feel closer to their friends. Two thirds of 12-15 year olds who use social media or messaging sites say they send support messages, comments or posts to friends if they are having a difficult time. One in eight support causes or organisations by sharing or commenting on posts.[26]
- In the 2019 UK Safer Internet Centre survey,[27] 70% of young people surveyed said that being online helps them understand what's happening in the world, with 60% noting they have only seen or heard about certain issues or news because they heard about them from the internet. 43% said they have been inspired to take action because of something they saw online, with 48% stating being online makes them feel that their voice or actions matter.

21 Children's Commissioner (2018). Who knows what about me? Available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-knows-what-about-me.pdf
22 Internet Matters (2019). Vulnerable Children in a Digital World. Available at: https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf
23 UKCCIS Evidence Group (2017). Children's online activities, risks and safety. Available at: https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group
24 UNICEF (2017). How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? Available at: https://www.unicef-irc.org/publications/pdf/Children-digital-technology-wellbeing.pdf
25 RSPH (2017). Status of mind: Social media and young people's mental health and wellbeing. Available at: https://www.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf
26 Ofcom (2018). Children and parents: media use and attitudes report 2018. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018
27 UK Safer Internet Centre (2019). Our internet, Our Choice Report. Available at: https://www.saferInternet.org.uk/safer-Internet-day/safer-Internet-day-2019/our-Internet-our-choice-report

Harm: Cyberbullying — Box 8

Threat:

In 2017, one in five children surveyed aged 11-19 reported having experienced cyberbullying in the past year.[28]

- The prevalence of cyberbullying is higher for some groups, such as women, religious minorities, LGBT+, BME and disabled individuals.[29]

Impact:

- Cyberbullying has been shown to have psychological and emotional impact. In a large survey of young people who had been cyberbullied, 41% had developed social anxiety, 37% had developed depression, 26% had suicidal thoughts and 25% had self-harmed.[30]
- These figures are all higher than corresponding statistics for 'offline' bullying, and indicated the increased potential for harm of cyberbullying.

Harm: Self-harm and suicide — Box 9

Threat:

In a survey of young adults, 22.5% reported self-harm and suicide-related internet use, including 8.2% and 7.5% who had actively searched for information about self-harm and suicide respectively.[31]

- Amongst those who had harmed with suicidal intent, 70% reported self-harm and suicide-related internet use.[32]
- The prevalence of using the internet to view related content has also been found to be higher in children than adults. One study of those presenting to hospital following self-harm found that 26% of children had viewed self-harm and suicide content, compared to 8.4% of adults.[33]

28 NHS Digital (2018). Mental Health of Children and Young People in England, 2017. Available at: https://files.digital.nhs.uk/C9/999365/MHCYP%202017%20Behaviours%20Lifestyles%20Identities.pdf
29 Ditch the Label (2017). 'The Annual Bullying Survey 2017'. Available at: https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-2.pdf
30 Ibid.
31 Mars, B et al. (2015). Exposure to, and searching for, information about suicide and self-harm on the internet: Prevalence and predictors in a population based cohort of young adults' Journal of affective disorders,185, 239-45. Available at: https://doi.org/10.1016/j.jad.2015.06.001
32 Ibid.
33 Padmanathan, P. et al. (2018). Suicide and Self-Harm Related internet Use. Crisis. Available at: https://doi.org/10.1027/0227-5910/a000522

Impact:

- The National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH) analysed the characteristics of 595 children and young people (aged under 20) who had died by suicide in the UK between 2014 and 2016.
- The NCISH found that suicide-related internet use (i.e. searching the internet for information on suicide methods) was reported for almost a quarter (23%) of these children and young people.[34]

Harm: Underage sharing of sexual imagery Box 10

Many children and young people take and share sexual images. Creating, possessing, copying or distributing sexual or indecent images of children and young people under the age of 18 is illegal, including those taken and shared by the subject of the image.

- Surveys provide tentative evidence that between 26%[35] and 38%[36] of 14-17 year olds have sent sexual images to a partner, and between 12% and 49% have received a sexual image.[37]
- The proportion of young people sending images varies with age, with one study indicating that 26% of 14 year olds had sent and received sexual images, rising to 48% of 16 year olds.[38]

Impact:

- Sharing sexual images can expose children and young people to bullying, humiliation, objectification and guilt. These images can be shared widely and appear on offender forums or adult pornography sites, or be used to extort further imagery. This puts children and young people in a vulnerable position and at risk of harm. It is a criminal offence to produce, possess or share sexual images of under 18 year olds.
- The National Society for the Prevention of Cruelty to Children (NSPCC) reported that sexting was discussed in 1,392 counselling sessions with children and young people on their helplines that year, representing a 15% increase on the year before.[39]

1.19 The UK Chief Medical Officers (UK CMOs) commissioned independent researchers to carry out a systematic evidence review on the impact of social media use on children and young people's mental health. The review covered important and diverse issues including cyberbullying, online gaming, sleep problems and problematic internet use, which is also known as 'internet addiction'.

34 National Confidential Inquiry into Suicide and Safety in Mental Health (2018). Annual Report: England, Northern Ireland, Scotland, Wales. University of Manchester. Available at: http://documents.manchester.ac.uk/display.aspx?DocID=38469
35 Brook (2017). Digital Romance. Available at: https://www.brook.org.uk/press-releases/digital-romance
36 UKCCIS Evidence Group (2017). Children's online activities, risks and safety. Available at: https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group
37 Ibid.
38 Ibid.
39 Ibid.

1.20 Overall the research did not present evidence of a causal relationship between screen-based activities and mental health problems, but it did find some associations between screen-based activities and negative effects, such as increased risk of anxiety or depression.[40] It is important that parents and carers support their children to have positive experiences online.

1.21 While there is not yet sufficient evidence about the impact of screen time to support detailed guidelines for parents or requirements on companies, we will continue to support research in this area and ensure high quality advice is available to families. We also welcome efforts from the industry to develop tools to help individuals and families understand and manage how much time they spend online – more information on these is in Box 33.

Emerging challenge: Screen time — Box 11

Screen time and its impact on children is an issue of growing concern. Research by Internet Matters found that nearly half of parents (47%) are concerned about the amount of time their child spends online and 88% take measures to limit their child's use of devices.[41]

- The UK CMOs recently conducted a systematic evidence review on children and young people's screen and social media use. The CMO subsequently produced advice for parents and carers to encourage them to discuss boundaries with children around online behaviours and time spent using screens, and to lead by example.
- For example, the UK CMOs advised that:
  - Sleep matters. Getting enough good quality sleep is very important. Leave phones outside the bedroom when it is bedtime.
  - Sharing sensibly. Talk about sharing photos and information online and how photos and words are sometimes manipulated. Parents and carers should never assume that children are happy for their photos to be shared. For everyone – when in doubt, don't upload!
  - Education matters. Make sure you and your children are aware of, and abide by, their school's policy on screen time.
  - Keep moving! Everyone should take a break after a couple of hours sitting or lying down using a screen. It's good to get up and move about a bit. #sitlessmovemore
  - Safety when out and about. Advise children to put their screens away while crossing the road or doing an activity that needs their full attention.
  - Talking helps. Talk with children about using screens and what they are watching. A change in behaviour can be a sign they are distressed – make sure they know they can always speak to you or another responsible adult if they feel uncomfortable with screen or social media use.

40 Department of Health and Social Care (2019). United Kingdom Chief Medical Officers' commentary on Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews. Available at: https://www.gov.uk/government/publications/uk-cmo-commentary-on-screen-time-and-social-media-map-of-reviews

41 Internet Matters (2018). Look Both Ways: Practical Parenting in the Age of Screens. Available at: https://www.Internetmatters.org/about-us/screen-time-report-2018/

- Family time together. Screen-free meal times are a good idea – you can enjoy face-to-face conversation, with adults giving their full attention to children.
- Use helpful phone features. Some devices and platforms have special features – try using these features to keep track of how much time you (and with their permission, your children) spend looking at screens or on social media.

Future action – building our understanding:

Given the amount of time many children spend online, and the level of parental concern on this issue, we urgently need to build a better understanding.

- While we do not expect the regulator to set requirements around screen time, both government and the regulator will continue to support research in this area to inform future action in this space.
- We need to develop a better understanding of not just of the impact of screen time as a whole, but also between different types of screen time and children's development and wellbeing.
- As part of this, we also expect companies to support the developing evidence base around screen time, for example by providing access to anonymised data to researchers as recommended by the CMOs
- If the emerging evidence base demonstrates a strong link between different elements of screen time and damage to children's wellbeing or development, companies will be expected to take appropriate action to fulfil their duty of care.

Threats to our way of life

1.22 The UK's reputation and influence across the globe is founded upon our values and principles. Our society is built on confidence in public institutions, trust in electoral processes, a robust, lively and plural media, and hard-won democratic freedoms that allow different voices, views and opinions to freely and peacefully contribute to public discourse.

1.23 Inaccurate information, regardless of intent, can be harmful – for example the spread of inaccurate anti-vaccination messaging online poses a risk to public health. The government is particularly worried about disinformation (information which is created or disseminated with the deliberate intent to mislead; this could be to cause harm, or for personal, political or financial gain).

1.24 Disinformation threatens these values and principles, and can threaten public safety, undermine national security, fracture community cohesion and reduce trust.

1.25 These concerns have been well set out in the wide-ranging inquiry led by the Digital, Culture, Media and Sport (DCMS) Select Committee report on fake news and disinformation, published on 18 February 2019. This White Paper has benefited greatly from this analysis and takes forward a number of the recommendations. The government will be responding to the DCMS Select Committee report in full in due course. We also note the recent papers from the Electoral Commission and Information Commissioner's Office on this and wider issues, and are considering these closely.

Table 1: Online harms in scope

Harms with a clear definition	Harms with a less clear definition	Underage exposure to legal content
• Child sexual exploitation and abuse. • Terrorist content and activity. • Organised immigration crime. • Modern slavery. • Extreme pornography. • Revenge pornography. • Harassment and cyberstalking. • Hate crime. • Encouraging or assisting suicide. • Incitement of violence. • Sale of illegal goods/ services, such as drugs and weapons (on the open internet). • Content illegally uploaded from prisons. • Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).	• Cyberbullying and trolling. • Extremist content and activity. • Coercive behaviour. • Intimidation. • Disinformation. • Violent content. • Advocacy of self-harm. • Promotion of Female Genital Mutilation (FGM).	• Children accessing pornography. • Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time).

2.3 There is already an effective response to some categories of harmful content or activity online. These will be excluded from the scope of the new regulatory framework to avoid duplication of existing government activity.

2.4 The following harms will be excluded from scope:

- All harms to organisations, such as companies, as opposed to harms suffered by individuals. This excludes harms relating to most aspects of competition law, most cases of intellectual property violation, and the organisational response to many cases of fraudulent activity. The government is leading separate initiatives to tackle these issues. For example, the Joint Fraud Taskforce is leading an ambitious programme of work to tackle fraud, including online fraud, through partnership between banks, law enforcement and government.
- All harms suffered by individuals that result directly from a breach of the data protection legislation, including distress arising from intrusion, harm from unfair processing, and any financial losses. Box 16 explains how the UK's legal framework provides protection against online harms linked to data breaches.

- All harms suffered by individuals resulting directly from a breach of cyber security or hacking. These harms are addressed through the government's National Cyber Security Strategy.
- All harms suffered by individuals on the dark web rather than the open internet. These harms are addressed in the government's Serious and Organised Crime Strategy. A law enforcement response to criminality on the dark web is considered the most effective response to the threat. As set out in the strategy, the government continues to invest in specialist law enforcement skills and capability.

Stronger regulation of personal data online Box 16

The UK already enjoys high standards of data protection law, that were modernised in 2018 with the introduction of the GDPR and the Data Protection Act 2018. The government chose to go further than other countries, by providing stronger powers to apply to the investigation and enforcement of specific online threats.

Key protections for online harms involving personal data include:

- An obligation to provide clear and accessible privacy information, tailored for children when they are the users of online services.
- A legal obligation to accountability, making companies responsible for placing data protection at the centre of the design of online services in a way that mitigates the risk to users' information. This also includes a requirement to undertake data protection impact assessments, and have them approved by the ICO where high risks persist.
- A right to erasure of personal data online, with stronger provisions where data has been gathered from a child user.
- An age-appropriate design code, which gives the design standards we will expect providers of online services and apps used by children to meet when they process their data.
- A power to inspect algorithms in situ, to understand their use of personal data and whether this leads to bias or other detriment.
- A power to require information to be handed over to the ICO wherever it is held, including on cloud servers.

Shortcomings of the current regulatory landscape

2.5 Currently there is a range of UK regulations aimed at specific online harms or services in scope of the White Paper, but this creates a fragmented regulatory environment which is insufficient to meet the full breadth of the challenges we face. The current regulatory framework includes:

- GDPR and the Data Protection Act enforced by the ICO. This includes collection and use of personal data, including when online. The GDPR also has extraterritorial scope and can be enforced against companies outside the UK who offer services to UK users.[55]

55 The Information Commissioner's Office. Available at: https://ico.org.uk/

- The Electoral Commission's oversight of the activity of political parties, and other campaigners, including activity on social media.[56]
- Forthcoming age verification requirements for online pornography.[57]
- The Equality and Human Rights Commission's oversight of the Equality Act 2010 and Freedom of Expression.[58]
- Ofcom's existing oversight of video-on-demand services.[59]
- The revised EU Audiovisual Media Services Directive, which will introduce new high-level requirements for video sharing platforms such as YouTube.[60]
- The Gambling Commission's licensing and regulation of online gambling.[61] DCMS has been working with the Commission to tighten advertising rules on gambling and launched GAMSTOP, the online self-exclusion scheme. Additional age-verification requirements are expected to come take effect in from May this year[62].
- The Competition and Markets Authority's (CMA) enforcement of consumer protection law online. See Box 17 for further details.

Consumer enforcement by the Competition and Markets Authority Box 17

Businesses risk breaching consumer protection law where their online behaviour misleads consumers or treats them unfairly. The CMA has undertaken a range of recent enforcement activity examining potentially unfair or misleading online behaviour, including:

- Online gambling – the CMA worked with the Gambling Commission to sanction unfair online 'bonus' promotions by major gambling firms. The CMA was concerned that players' money could effectively be trapped under the terms of these promotions, or that they could be caught out by unclear or imbalanced promotion rules. Changes were agreed with a number of firms, including William Hill and Ladbrokes.
- Online reviews and endorsements – the CMA has an ongoing programme of work to tackle fake or misleading online reviews and endorsements. Most recently, 16 celebrities, reality stars and social media influencers committed to always be clear

56 The Political Parties, Elections and Referendums Act 2000 (PPERA) provides the Electoral Commission with the powers and functions to regulate political finance in the UK. Electoral law is also enforced by the police, who lead on the Representation of the People Act offences. The Electoral Commission has powers to investigate breaches of the rules to funding and spending for election and referendum campaigns, which includes digital campaigning.

57 The Digital Economy Act 2017 provides for the regulation of providers of online commercial pornography to ensure that pornographic material is not normally accessible by those under 18, and that content which is deemed to be extreme pornographic material is not made available to any user. The BBFC is the designated regulator. These requirements will come into force shortly.

58 The Equality and Human Rights Commission. Equality Act 2010. Available at: https://www.equalityhumanrights.com/en/equality-act/equality-act-2010

59 The EU's Audiovisual Media Services Directive 2010 provides Ofcom with the power to regulate editorial content (programming) on UK 'video-on-demand' services – overseeing compliance on content requirements that cover protecting under 18s, preventing incitement to hate, and commercial references in programmes.

60 The EU's revised Audiovisual Media Services Directive (2018) will place requirements on 'video sharing platforms' to take 'appropriate measures' to protect minors from harmful content, protect the general public from illegal content and content that incites violence and/or hatred, and will introduce basic requirements around advertising. A regulator is still being selected, and these requirements are scheduled to come into force by September 2020.

61 The Gambling Act 2005 provides the Gambling Commission with powers to license and regulate all forms of gambling, including online gambling.

62 From May 2019, the Gambling Commission will bring in changes that mean that age and identity must be verified before consumers can deposit money and gamble, and will require age verification before customers can access free-to-play demo games.

in their social media posts where they have been paid to post content online. The CMA is now examining the responsibility of social media platforms to ensure that paid-for content is always properly disclosed.

- Secondary tickets – as a result of action by the CMA, including court proceedings against Viagogo, consumers will always receive essential information before they purchase a ticket from online resale platforms, in particular if there is a risk that the consumer will not be able to get into the event or venue. The court order secured against Viagogo also requires that 'pressure selling' messages are removed from their website.
- Online hotel booking – the CMA recently agreed changes with companies in the Booking.com and Expedia corporate groups in relation to potentially misleading online practices. These include new requirements to be clear about the role that commission plays in the order of search results and that any claims about the limited availability of hotel rooms are accurate and do not risk misleading consumers.

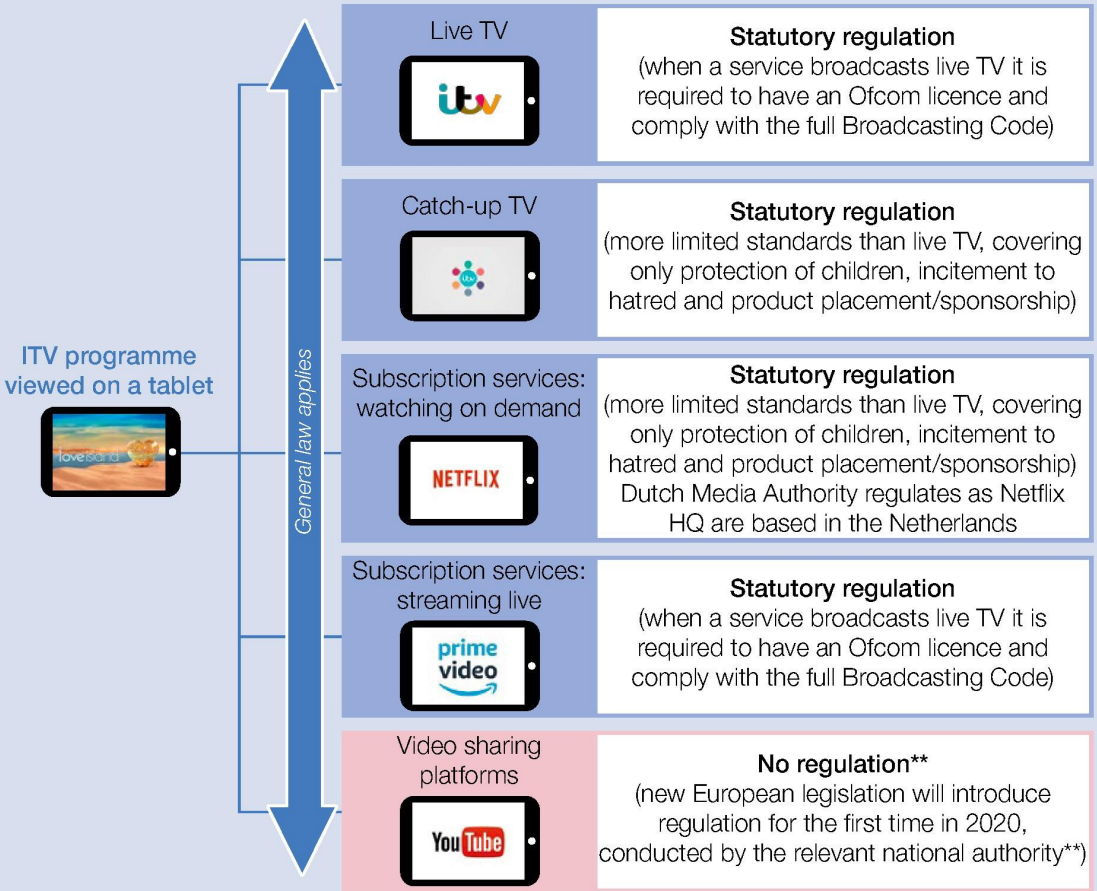
2.6 Under the current liability regime, which is derived from the EU's e-Commerce Directive, platforms are protected from legal liability for any illegal content they 'host' (rather than create) until they have either actual knowledge of it or are aware of facts or circumstances from which it would have been apparent that it was unlawful, and have failed to act 'expeditiously' to remove or disable access to it. In other words, they are not liable for a piece of user-generated illegal content until they have received a notification of its existence, or if their technology has identified such content, and have subsequently failed to remove it from their services in good time.

2.7 For illegal harms, it is also important to make sure that criminal law applies online in the same way as it applies offline. In February 2018 the Prime Minister announced a review by the Law Commission of the law in relation to abusive and offensive online communications, to highlight any gaps in the criminal law which cause problems in tackling this abuse. In its scoping report last year, the Law Commission concluded that behaviour is broadly criminalised to the same extent online as offline and recommended a clarification of existing communication offences. The government is now finalising the details of the second phase of the Law Commission work.

2.8 For legal harms, the same piece of content can be subject to different regulatory standards depending on the platform on which it appears. Ofcom's report Addressing Harmful Content Online sets out how the same programme would be regulated to differing degrees depending on whether it is broadcast on TV, viewed on-demand, or on an online video sharing platform (see Box 18). This means that there are significant gaps in consumer protection.[63]

63 Ofcom (2018). Addressing Harmful Online Content. Available at: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/online-policy-research/addressing-harmful-online-content

Regulation of the same content on different services Box 18



Source: Addressing Harmful Content Online, Ofcom 2018.

Voluntary approaches

2.9 Beyond this range of regulatory requirements, the government's Internet Safety Strategy Green Paper, published in 2017, focused on a voluntary approach to countering harmful behaviour and content online. The green paper recognised that government alone cannot keep citizens safe from online harms, and sought to work in close partnership with industry to put in place specific technical solutions to make social media platforms safer.

2.10 Voluntary initiatives between government, industry and civil society are promising in some areas, and the leading companies have taken a number of steps to improve their platforms, for example as set out in Boxes 19-21. We are clear that the progress made on terrorism and CSEA through this voluntary cooperation with the industry must continue, alongside the development of a new regulatory framework.

Existing initiatives to tackle online harms: Global Internet Forum to Counter Terrorism — Box 19

Following the Westminster terrorist attack in March 2017, the government convened a roundtable with major industry players, including Facebook, Twitter, Google and Microsoft to see what more could be done to tackle terrorist content online. This led to these companies setting up the Global Internet Forum to Counter Terrorism (GIFCT) in June 2017.

The GIFCT is leading the cross-industry response to reduce the availability of terrorist content on the internet so that there are no safe spaces for terrorists online. Key objectives for the Forum are to increase the use of automation and machine learning technology to detect and remove terrorist content – ultimately preventing terrorist content being made available to users in the first place – and supporting smaller, less well-resourced companies to tackle these threats on their own platforms.

The Forum has taken some positive steps since its establishment, but there is still much more to do. The government wants to see an ambitious and tangible plan for delivery. Our aims for the GIFCT in 2019 are for the Forum to:

- Expand its membership, securing a greater range and quantity of companies to sign up as members of the Forum.
- Devote greater efforts to targeted interventions with priority platforms, including through the development and sharing of automated technology.
- Put in place a clear programme of activity, providing metrics against which success can be measured.
- Provide greater visibility to drive this agenda forward, including companies having a clearer public voice on the issue.

Existing initiatives to tackle online harms: UK Council for Internet Safety — Box 20

The UK Council for Internet Safety (UKCIS) is a new collaborative forum through which government, the tech community and civil society work together to ensure the UK is the safest place in the world to be online.

Expanding the scope of the former UK Council for Child Internet Safety (UKCCIS), UKCIS works to tackle online harms such as hate crime, extremism and violence against women and girls, in addition to maintaining a focus on the needs of children.

Priority areas of delivery for UKCIS over the next year include:

- Producing a landscape review of research around adult online harms, and regular concise summaries of emerging research.
- Updated guidance to schools on sexting, and evaluation of online safety provision, and for Initial Teacher Training providers to help them upskill new teachers in online safety.

- Promoting the Connected World framework, which describes the digital knowledge and skills that children should have the opportunity to develop at different stages of their lives.
- A digital resilience framework and toolkit to help families, educators, policymakers, frontline service workers and the industry better support users online, across a wide range of harms.

Existing initiatives to tackle online harms: WePROTECT Global Alliance **Box 21**

The WePROTECT Global Alliance (WPGA) was established in recognition that CSEA is a global crime requiring a global response.

The UK government played a key role in establishing WPGA and is its sole financial donor. WPGA aims to protect more children, apprehend more perpetrators of abuse and make the internet free from child sexual exploitation. Eighty-five countries are members of WPGA, along with 20 global technology companies and 25 leading non-governmental organisations.

The success of the UK government funded WPGA is that it has brought together government, law enforcement, industry and civil society to take a stand against online child sexual exploitation.

2.11 In the Government Response to the Internet Safety Strategy Green Paper consultation, we noted that only a relatively small group of the larger companies are engaged with the government's work on online safety, even though online harms can and do occur across many websites. There is also a wide variation in the extent, efficacy and pace of actions by companies to tackle online harms. Some companies rely on user moderation to oversee reported violations of their terms and conditions, such as Reddit; others employ teams of moderators or deploy technology to monitor content, such as Facebook.

2.12 Many companies claim to hold a strong track record on online safety but there is limited transparency about how they implement or enforce their policies, and there is a persistent mismatch with users' experiences – 70% of Britons believe that social media companies do not do enough to prevent illegal or unethical behaviours on their platforms.[64] 60% of respondents to our Internet Safety Strategy Green Paper consultation had witnessed inappropriate or harmful behaviour online; only 41% thought their reported concerns were taken seriously by social media companies.[65]

2.13 At present many online companies rely on using their terms and conditions as the basis by which to judge complaints. In practice however, companies' terms and conditions are often difficult for users to understand, and safety policies are not consistent across different

64 Edelman (2018). Edelman Trust Barometer – UK Findings. Available at: https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2018/

65 HM Government (2018). Government Response to the Internet Safety Strategy Green Paper. May 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf

platforms, with take-down times, description of harms and reporting processes varying. A series of investigations have highlighted the risk of serious shortcomings in the training, working conditions and support provided for content moderators.[66]

2.14 There is no mechanism to hold companies to account when they fail to tackle breaches. There is no formal, wide-reaching industry forum to improve coordination on terms and conditions. The absence of clear standards for what companies should do to tackle harms on their services makes it difficult for users to understand or uphold their rights.

2.15 The government believes that voluntary efforts have not led to adequate or consistent steps to protect British citizens online. As highlighted above, users' own experiences confirm a sense of vulnerability online.

An international approach

2.16 The threat posed by harmful and illegal content and activity online is a global one, and many of our international partners are also developing new regulatory approaches to tackle online harms. Box 22 sets out what some other countries are doing in this area.

International approaches to countering online harms — Box 22

Germany adopted its Network Enforcement Act ('NetzDG') in 2017. This law requires online platforms with more than two million registered users in Germany to remove 'manifestly unlawful' content, which contravenes specific elements of the German criminal code, such as holocaust denial and hate speech, within 24 hours of receiving a notification or complaint, and to remove all other 'unlawful' content within seven days of notification. Non-compliance risks a fine of up to €50 million. This law also seeks to increase platform responsibility through imposing greater transparency and significant reporting obligations.

Australia established an eSafety Commissioner through its Enhancing Online Safety for Children Act in 2015. The eSafety Commissioner is responsible for promoting online safety for all Australians. As well as offering a complaints service for young people who experience serious cyber bullying, its remit includes identifying and removing illegal online content and tackling image-based abuse.

The European Commission, led by DG JUST, published in September 2018 a proposal on preventing the dissemination of terrorist content online – Member States agreed a Council version of the text in December 2018. The aim of the proposal is to ensure a consistent approach across industry to the removal of online terrorist content by Hosting Service Providers, for example social media platforms and video sharing sites. There are similarities in the approach taken to the framework proposed in this White Paper – as currently drafted it looks to take a proportionate approach to setting requirements, introduce duties of care on companies, and implementing a transparency framework.

Over 2018, the EU Commission, led by DG CNECT, also published its Action Plan against Disinformation. The Commission collaborated with companies including Facebook, Google and Twitter to produce a code of practice against disinformation. This resulted in commitments to improve the transparency of political advertising, prevent the misuse

66 The Verge (2019). The Trauma Floor. Available at: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona