

## **Her Majesty's Government – Department for Digital, Culture, Media and Sport—written evidence (FE00012)**

### **House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online**

#### **Introduction**

The Government welcomes the opportunity to provide written evidence to the inquiry of the House of Lords Communications and Digital Committee into freedom of expression online.

The UK is committed to a free, open and secure internet, and will continue to protect freedom of expression online. We recognise the critical importance of freedom of expression, both as a fundamental right in itself and as an essential enabler of the full range of other human rights protected by UK and international law.

We look forward to the findings of the Committee when they are published.

#### **Background: The Online Harms Regulatory Framework and Freedom of Expression**

The Government's written evidence is drawn from the [Full Government Response to the Online Harms White Paper](#), which we published on 15 December 2020. This confirms the government's intention to introduce new Online Safety legislation which will create legal expectations on companies to keep their users safe online. This follows the publication of the [Online Harms White Paper](#) and a three-month consulting period, during which we received over 2,400 consultation responses. We also published the [Initial Government Response](#) to the consultation in February 2020.

The Online Safety Bill intends to make the UK the safest place in the world to go online, while at the same time protecting users' freedom of expression.

Under the new legislative framework, companies in scope will have a duty of care towards their users. The legislation will require companies to prevent the proliferation of illegal content and activity online, and ensure that children who use their services are not exposed to harmful content. It will also hold the largest tech companies to account for what they say they are doing to tackle activity and content that is harmful to adults using their services. They must set out clear terms and conditions, and ensure clear and accessible routes for users to seek redress, including for where they feel content has been removed unfairly.

The online harms regime will apply to platforms who host user generated content, or facilitate interaction between users, as well as search engines.

To meet the duty of care, companies in scope will need to understand the risk of harm to individuals on their services and put in place appropriate systems and processes to improve user safety. Ofcom will oversee and enforce companies' compliance with the duty of care. Companies and the regulator will need to act in line with a set of guiding principles. These include improving user safety, protecting children and ensuring proportionality.

Freedom of expression is at the heart of our approach and safeguards for freedom of expression have been built in throughout the framework. Both Ofcom and in-scope companies will have duties relating to freedom of expression, for which they can be held to account. Freedom of expression will be protected by ensuring that the framework is risk-based and focused on systems and processes. It will not focus on the removal of individual pieces of content.

Regulation will not prevent adults from accessing or posting legal content, nor require companies to remove specific pieces of legal content. We recognise that adults have the right to upload and access content that some may find offensive or upsetting. The largest social media companies will no longer be able to arbitrarily remove harmful content. They will have a legal obligation to enforce their terms and conditions consistently and transparently. Users will have access to effective mechanisms to appeal content that is removed without good reason.

Further, the new laws will have robust and proportionate measures to deal with disinformation that could cause significant physical or psychological harm to an individual, such as anti-vaccination content and falsehoods about Covid-19. Whilst we are committed to taking action to address false narratives online, we will ensure that freedom of expression in the UK is protected and enhanced online. Freedom of expression and the media are essential qualities of any functioning democracy; people must be allowed to discuss and debate issues freely. As such, the UK is dedicated to protecting freedom of expression in line with our democratic values and deplores attempts to restrict freedom of expression through the guise of countering disinformation, including blocking access to the internet, intimidation of journalists or interference in their ability to operate freely, and legislation restricting free expression of opinion

The framework will also include robust protections for journalistic content when shared on in-scope services. We are clear that regulation will protect the vital role of the media in providing people with reliable and accurate information.

---

*The committee sought responses to the following questions to form the written evidence for its report. The committee added that other issues may be discussed provided that their relevance is explained:*

**Is freedom of expression under threat online? If so, how does this impact individuals differently, and why? Are there differences between exercising the freedom of expression online versus offline?**

1. The right to freedom of expression applies online, just as it does offline. Government is committed to ensuring that pluralism is protected online and individuals are able to engage in robust debate online.
2. The internet has, in many ways, transformed our lives for the better. It has revolutionised our ability to connect with each other and created new opportunities for individuals to exercise the right to freedom of expression. However, despite the opportunities that the internet brings, many individuals face obstacles to exercising the right to freedom of expression online.
3. The majority of individuals' online communication is facilitated by online intermediaries and individuals' ability to express themselves online is often governed by private companies. For example, the largest social media platforms set terms and conditions for legal content that go far beyond what is required by the law, even if enforcement is patchy. Users have raised concerns that content may be removed for vague reasons, with limited opportunities for appeal.
4. We also know that many people, particularly those with protected characteristics, are unable to exercise their right to freedom of expression fully, as they do not feel able to use online platforms, often because of experience or fear of online abuse.
5. The right to freedom of expression extends to the right to offend, but does not include a right to say things which are illegal. Accordingly, the criminal law related to speech should apply online in the same way as it applies offline. In February 2018 the previous Prime Minister announced a review by the Law Commission into abusive and offensive online communications, to highlight any gaps in the criminal law which cause problems in tackling this abuse. In June 2019 the Government engaged the Law Commission on a second phase of this review. The Law Commission has consulted on proposed reforms and will issue final recommendations early 2021.

**How should good digital citizenship be promoted? How can education help?**

6. Digital citizenship is an important part of online life and it is vital that it is understood by users. One of the key ways digital citizenship can be promoted to users is through digital media literacy education which can equip users with the knowledge and skills they need to spot dangers online, critically appraise information and take steps to keep themselves and others safe online.
7. The Full Government Response to the Online Harms White Paper confirmed Government's intention to publish a new Online Media Literacy Strategy, which is being developed in broad consultation with stakeholders. The Strategy will ensure a coordinated approach to online media literacy education and awareness for children, young people and adults. Amongst other things, the Strategy will explore the key media literacy skills, and how good digital citizenship can be promoted. The Strategy will be published in Spring 2021.
8. As part of the Government's work on Media Literacy we are conducting a comprehensive mapping exercise to identify what actions are already underway, and to determine the objectives of an online media strategy. This mapping is now underway as part of a wider piece of analysis which will also consider existing research on the levels of media literacy among users, and evaluate the evidence base for media literacy interventions. Initial analysis of the mapping works indicates the UK has a rich media literacy landscape. This includes some initiatives that specifically promote good digital citizenship such as Google's 'Be Internet Citizens' curriculum.

**Is online user-generated content covered adequately by existing law and, if so, is the law adequately enforced? Should 'lawful but harmful' online content also be regulated?**

9. The government is clear that online companies that host user-generated content should take more responsibility for harmful content on their platforms. The Full Government Response to the Online Harms White Paper confirmed the government's intention to introduce a duty of care on companies that host user-generated content or facilitate user interaction.
10. The case for regulatory action is clear. There is extensive evidence of illegal and harmful activity online, threatening our national security, the physical safety of children and individuals' wellbeing. For example:
  - a. Over three quarters of UK adults express a concern about going online,<sup>1</sup> and fewer parents feel the benefits outweigh the risks of

---

<sup>1</sup> ['Internet users' concerns about and experience of potential online harms'](#) Ofcom and ICO, May 2019

their children being online, with the proportion falling from 65% in 2015 to 55% in 2019.<sup>2</sup>

- b. There were more than 69 million images and videos related to child sexual exploitation and abuse referred by US technology companies to the National Center for Missing and Exploited Children in 2019, an increase of more than 50% on the previous year.<sup>3</sup> In 2019, of the over 260,000 reports assessed by the Internet Watch Foundation, 132,730 contained images and/or videos of children being sexually abused (compared to 105,047 in 2018), and 46% of reports involved imagery depicting children who appeared to be 10 years old or younger.<sup>4</sup> Between its launch in January 2015 and March 2019, 8.3 million images have been added to the Child Abuse Image Database.<sup>5</sup> The National Crime Agency estimates at least 300,000 individuals in the UK pose a sexual threat to children.<sup>6</sup>
- c. Terrorist groups use the internet to spread propaganda designed to radicalise, recruit and inspire vulnerable people, and to incite, provide information to enable, and celebrate terrorist attacks. Some companies are taking positive steps to combat online terrorist content. The larger platforms are already taking proactive measures and using automated technology. For instance, Twitter actioned 95,887 unique accounts related to the promotion of terrorism/violent extremism between January and June 2019.<sup>7</sup>
- d. In 2019, according to research conducted by Ofcom and the Information Commissioner's Office, 23% of 12-15 year olds had experienced or seen bullying, abusive behaviour or threats on the internet in the last 12 months.<sup>8</sup> Nearly half of girls admit to holding back their opinion on social media for fear of being criticised.<sup>9</sup> New research is uncovering the scale of hate aimed at people with protected characteristics. Galop, the LGBT+ anti-violence charity's, most recent online hate crime survey highlighted that 8 in 10 respondents had experienced anti-LGBT+ online abuse in the last 5 years.<sup>10</sup> In 2019, the Community Security Trust, a charity that

---

(last viewed in November 2020)

<sup>2</sup> ['Children and parents: Media use and attitudes report 2019'](#) Ofcom, February 2020 (last viewed in November 2020)

<sup>3</sup> National Center for Missing and Exploited Children. Available at: <https://www.missingkids.org/gethelpnow/cybertipline>.

<sup>4</sup> 'The Internet Watch Foundation Annual Report 2019' The Internet Watch Foundation, April 2020 (last viewed in November 2020)

<sup>5</sup> 'Child sexual abuse - Appendix tables' Office for National Statistics, January 2020 (last viewed in November 2020)

<sup>6</sup> 'Law enforcement in coronavirus online safety push as National Crime Agency reveals 300,000 in UK pose sexual threat to children' National Crime Agency, April 2020 (last viewed in November 2020)

<sup>7</sup> 'Rules Enforcement' Twitter, August 2020 (last viewed in November 2020)

<sup>8</sup> 'Internet users' concerns about and experience of potential online harms' Ofcom and ICO, May 2019 (last viewed in November 2020)

<sup>9</sup> 'Reclaiming the Internet for Girls' Plan International (last viewed in November 2020)

protects British Jews from antisemitism, saw a 50% rise in reported anti-Semitic online incidents compared to 2018.

11. The new regulatory framework will increase the responsibility that services have in relation to online harms. In particular, companies will be required to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms, as well as to take appropriate and proportionate action when issues arise. The new regulation will also ensure effective oversight of the take-down of illegal content, and will introduce specific monitoring requirements for tightly defined categories of illegal content.
12. The regulatory framework will establish differentiated expectations on companies in scope with regard to different categories of content and activity on their services: that which is illegal; that which is harmful to children; and that which is legal when accessed by adults but which may be harmful to them. To ensure protections for freedom of expression, regulation will not force companies to remove specific pieces of legal content accessed by adults. Instead the legislation will hold the largest tech companies to account for what they say they are doing to tackle lawful activity and content that is harmful to adults using their services.
13. Under our legislation, a small group of high-risk, high-reach services will be designated as 'Category 1 services', and only providers of these services will additionally be required to take action in respect of content or activity on their services which is legal but harmful to adults. These companies will be required to set clear and accessible terms and conditions which explicitly state how they will handle categories of legal but harmful material, and then enforce these consistently and transparently. Please see the Full Government Response to the Online Harms White Paper consultation for further details on requirements that regulation will place on companies.
14. In addition to online harms regulation, it is important to ensure the criminal law is fit for purpose to deal with harm online. As stated earlier in this return, the government has engaged the Law Commission on a second phase of their review of abusive and offensive online communications. The Law Commission has consulted on proposed reforms and will issue final recommendations early 2021.

### **Should online platforms be under a legal duty to protect freedom of expression?**

---

<sup>10</sup> 'Online Hate Crime Report 2020' Galop (last viewed in November 2020)

15. Currently, private companies that host user generated content online are not bound European Convention on Human Rights (ECHR) obligations to protect their users' right to freedom of expression.
16. However, we recognise the importance of high risk, high reach platforms as public forums where people can engage in robust debate online. The Online Safety Bill therefore seeks to ensure that pluralism is safeguarded online.
17. In-scope services will have a duty to consider safeguards for freedom of expression when implementing their duties under online harms legislation. 'Category 1' companies will also be required to set clear and accessible terms and conditions which explicitly state how they will handle categories of legal but harmful material, and then enforce these consistently and transparently. They will also be required to put in place effective and accessible mechanisms for users to report concerns and seek redress for alleged harmful content or activity online, infringement of rights, or a company's failure to fulfil its duty of care.
18. These measures will prevent companies from arbitrarily removing controversial viewpoints and users will be able to seek redress if they feel content has been removed unfairly. When combined with transparency requirements, this will also increase understanding about what content is taken down and why. In this way, regulation will promote and safeguard pluralism online, while ensuring companies can be held to account for their commitments to uphold freedom of expression.
19. Further, the new regulator, Ofcom, will be required to have due regard to freedom of expression in how they exercise their duties. They will need to make sure the requirements placed on companies do not have an undue chilling effect on an individual's freedom of expression.

**What model of legal liability for content is most appropriate for online platforms?**

20. Under the current liability framework in the UK , 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. This is

in order to provide consistency for the UK's tech sector and to continue to support innovation and growth.

21. The new regulatory framework will increase the responsibility that services have in relation to online harms, while remaining consistent with the existing law on liability for individual items of content that enables platforms to operate. Companies will be required to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms, as well as to take appropriate and proportionate action when issues arise. The new regulatory regime will also ensure effective oversight of the take-down of illegal content, and will introduce specific monitoring requirements for tightly defined categories of illegal content. The position on liability for individual items of content will remain the same as described in paragraph 20.

### **To what extent should users be allowed anonymity online?**

22. Online anonymity is an important principle of a free and open internet. There are many legitimate reasons why an individual would not wish to identify themselves online, for example, whistle-blowers and victims of modern slavery and domestic abuse.
23. However, being anonymous online does not give anyone the right to abuse others. Under the online safety regulation, all companies will need to take swift and effective action against criminal online abuse. Users will be better able to report all types of abuse, and should expect to receive an appropriate response from the platform. This might include removal of harmful content, sanctions against offending users, or changing processes and policies to better protect users.
24. Major platforms will also need to address legal but harmful content for adults, including legal abuse that is prohibited in their Terms and Conditions. The priority categories of legal but harmful content for adults will be set out in secondary legislation and these are likely to include some forms of online abuse. Our approach will make platforms responsible for tackling abuse online, including anonymous abuse, while protecting rights and freedom of expression.
25. Government and law enforcement are taking action to tackle anonymous abuse online. The police also have a range of legal powers to identify individuals who attempt to use anonymity to escape sanctions for illegal online abuse. The Home Office has been working with law enforcement to review whether current powers are sufficient to tackle this abuse where it is illegal.



26. We are also ensuring that the criminal law is fit for purpose to deal with online abuse. The government engaged the Law Commission on a second phase of their review of abusive and offensive online communications. This review considered whether co-ordinated harassment by groups of people online could be more effectively dealt with by the criminal law. The Law Commission has consulted on proposed reforms and will issue final recommendations early 2021.

### **How can technology be used to help protect the freedom of expression?**

27. Under the new legislation, the regulator will have the express power, where alternative measures cannot effectively mitigate harm, to require a company to use automated technology that is highly accurate to identify only illegal child sexual exploitation and abuse content, or terrorist content and activity on their service.
28. Robust safeguards will be included in the online harms legislation to govern when the regulator can require the use of automated technology. The regulator will only be able to require the use of tools that are highly accurate in identifying only illegal content, minimising the inadvertent flagging of legal content ('false positives') for human review.
29. More broadly, modern technologies can help platforms detect online harms at scale, spot illegal content and help enforce a platform's terms and conditions. In most cases, the job of these technologies is to help human moderators uphold their site's published moderation policies - for example, algorithms can be used to trawl thousands of pages of content, and flag to moderators content or behaviour that appears to break terms of service, or could potentially be illegal. Moderators would then investigate the issues further and take a decision in accordance with their published terms of service.
30. This ensures that online platforms keep pace with the scale and pace of change of online harms, whilst making the right decisions that balance freedom of expression with the removal of harmful content.

### **How can platforms create environments that reduce the propensity for online harms?**

#### **How do the design and norms of platforms influence freedom of expression?**

31. It is essential that companies proactively consider the safety consequences of their platform design decisions. An approach that embeds safety at the design stage of an online platform is integral to

tackling online harms, and driving up standards of online safety. For example, by designing a platform to be age appropriate from the outset a company limits the risk of harm occurring to child users rather than reacting to incidences of harm as they occur.

32. The design of an online platform impacts on user safety: poor platform design decisions can increase the risk of online harm occurring while a 'safety by design' approach helps mitigate the risk. The Government recognises the need for action in this space and is taking steps to ensure that online platforms are consciously designed to be safe for users. Retrofitting safety features is possible, but is often more costly, disruptive and risks harming users, than building in user safety from the outset.
33. The Government has committed to publishing a 'Safety by Design' framework that will set out best practice platform design in regards to user safety. The Framework will be published in Spring 2021. The guidance will be voluntary and will help companies better understand the risks associated with platform design and enable them to make safer choices. It will have a particular focus on protecting children and strengthening user's media literacy.
34. There is currently limited evidence on how platform design impacts on freedom of expression. Platform design can impact on a user's access to online content and their critical engagement with what they see online. When used alongside content policies and content recommendation algorithms, platform design may risk affecting a user's freedom of expression. Good platform design can be used to widen the visibility a user has of a range of legal content, improving access to information and a range of viewpoints. Poor platform design - that removes or restricts a user's access to, or ability to share legal content - may risk limiting knowledge and debate.

**How could the transparency of algorithms used to censor or promote content, and the training and accountability of their creators, be improved? Should regulators play a role?**

35. Transparency can play a critical role in ensuring that content removal is well-founded. Improving the transparency and accountability of online service providers will be a key aspect of the new online harms regulatory framework.
36. As part of the framework, Ofcom will have the power to require transparency reports from certain companies about the steps they are taking to keep their users safe. These reports will contain information on

a number of areas, which may include information about the content moderation processes that are in place and how well they are working.

37. As stated above, under our new legislation the largest social media companies will no longer be able to arbitrarily remove controversial content, unless it is prohibited under their terms and conditions. They will have a legal obligation to enforce their terms and conditions relating to harmful content consistently and transparently. Users will have access to effective mechanisms to appeal content that is removed without good reason
38. Greater transparency will help empower users to make informed decisions about their online activity, helping to drive industry accountability and encouraging action from companies.
39. Under the duty of care companies will, where necessary, need to mitigate risks associated with the operation of their algorithms. Ofcom will have a suite of information gathering powers to help it to understand how companies are complying with the Duty of Care, including in relation to their algorithms.

**How can content moderation systems be improved? Are users of online platforms sufficiently able to appeal moderation decisions with which they disagree? What role should regulators play?**

40. Under the new framework, companies will need to consider the impact on users' rights when designing and deploying content moderation systems and processes. This might involve engaging with stakeholders in the development of their content moderation policies, considering the use of appropriate automated tools, and ensuring appropriate training for human moderators.
41. Companies should take reasonable steps to monitor and evaluate the effectiveness of their systems. Certain companies will also need to produce transparency reports, which are likely to include information about their measures to uphold freedom of expression and privacy.
42. At the moment, individuals can often appeal moderation decisions, but processes vary and provision is patchy across the industry. Some companies do not have effective means to address user concerns, and it is not always clear what response, if any, a user will receive.
43. Under the new regulatory framework, all companies in scope will have a specific legal duty to have effective and accessible reporting and redress mechanisms. These mechanisms will need to enable people to raise

concerns that their rights have been infringed, including to appeal moderation decisions. As the independent regulator, Ofcom will set out expectations for these mechanisms in Codes of Practice. The government expects the codes to cover areas such as accessibility (including to children), transparency, communication with users, signposting and appeals.

44. In addition, Ofcom's super-complaints function will ensure there is an avenue to alert the regulator to concerns about systemic issues, including those relating to users' rights.
45. Users will be able to report concerns regarding users' rights, including freedom of expression, to the regulator. Ofcom will not investigate or arbitrate on individual cases. However, receiving user complaints will be an essential part of Ofcom's horizon-scanning, research, supervision and enforcement activity.

**To what extent would strengthening competition regulation of dominant online platforms help to make them more responsive to their users' views about content and its moderation?**

46. The Government has committed to establishing a new pro-competition regime which will focus on addressing harms arising from entrenched market power in digital markets. This regime will empower consumers through greater choice and transparency.
47. A new Digital Markets Unit (DMU), housed in the Competition and Markets Authority (CMA), will be set up to begin to operationalise a new pro-competition regime in early 2021. It will work closely with key regulators, including the new online harms regulator, to ensure that our approach to regulating digital technologies is coherent and effective overall.
48. At the heart of the new pro-competition regime will be a mandatory code of conduct to govern the relationships between dominant firms and different groups of users which rely on their services, promoting fair trading, open choices, trust and transparency.
49. The government has also agreed in principle that the DMU will be able to introduce pro-competition interventions to address the barriers to competition in digital markets, as recommended by the CMA in their recent study into online platforms and digital advertising.
50. The new pro competition regime will drive dynamism and competition across digital markets and the wider economy. It will lead to more

innovative, better quality services and offer users more choice and control over those services. We will be consulting on the design and implementation of the new pro-competition regime in 2021, building on the advice of the Digital Markets Taskforce.

**Are there examples of successful public policy on freedom of expression online in other countries from which the UK could learn? What scope is there for further international collaboration?**

51. International collaboration is important in tackling issues relating to online governance. The government continues to engage with international partners to learn from their experiences and build consensus around shared approaches to tackling online regulation that uphold our democratic values and promote a free, open and secure internet. The government also welcomes international, industry-led, multi-stakeholder initiatives – including initiatives supported by the UN and other multilateral bodies.
52. The UK and the EU have similar objectives in our work on online harms, and continue to share similar values. The EU’s Digital Services Act and the UK’s Online Safety legislation will set out new expectations on companies to ensure they have proportionate systems and processes in place, to mitigate risks and keep their users safe online. The UK’s Online Safety legislation will safeguard freedom of expression and pluralism online, and this is also a priority of the Digital Services Act.

*8 January 2021*