Government Response to Lords Select Committee on Communications Report, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf

Introduction

The Government is grateful for the Committee's inquiry into internet regulation and welcomes the Committee's report "Regulating in a Digital World" and its recommendations.

We recognise that, as well as opportunities, the internet has brought new challenges and risks. We are clear that Government must lead the way in tackling these challenges.

The Committee's recommendations are closely aligned with the Government's approach. Our recently-updated Digital Charter sets out an ambitious programme of work to ensure that the internet and digital technologies are safe and secure, developed and used responsibly - with users' interests at their heart - and deliver the best outcomes for consumers through well-functioning markets.

In some cases we will shift expectations of behaviour; in some we will need to agree new standards; and in others we will update our laws. Where regulation is necessary, we will ensure it is well-targeted, proportionate and delivers a stable and predictable business environment for innovation to thrive. We will develop our approach in collaboration with industry and international partners and ensure it is coherent and easy to understand for citizens as well as businesses. Through this work we will protect citizens, increase public trust in new technologies, and create the best possible basis on which the digital economy and society can thrive.

To make the UK the safest place in the world to be online, the Department for Digital, Culture, Media and Sport and the Home Office recently published the Online Harms White Paper, setting out our plans for world leading legislation. The Government recognises that illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet. The prevalence of the most serious illegal content and activity, which threatens our national security or the physical safety of children, is unacceptable.

Other online behaviours or content, even if they may not be illegal in all circumstances, can also cause serious harm. Online platforms can be a tool for abuse and bullying, and they can be used to undermine our democratic values and debate. The impact of harmful content and activity can be particularly damaging for children, and there are growing concerns about the potential impact on their mental health and wellbeing.

To address these harms, the Government is establishing a new statutory duty of care to make companies take more responsibility for the safety of their users online and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator, which will implement, oversee and enforce the new regulatory framework.

New regulation will be risk-based and proportionate across the broad range of businesses and other organisations in scope, designed to support innovation and a thriving digital economy.

Our proposals will also help companies to ensure the safety of users whilst promoting freedom of expression and other norms that underpin our democratic society.
For example, the Government strongly supports press freedom and editorial independence. A vibrant, independent, plural and free press that is able to hold the powerful to account is essential to our democracy. This is why journalistic or editorial content will not be affected by the regulatory framework we are putting in place.

We are clear that digital technology and the internet must work for everyone - for citizens, businesses and society as a whole. This means new technologies must be deployed ethically, as well as safely and securely. The UK already benefits from well established and robustly enforced personal data laws, as well as wider regulations that guide how digital technology technologies can be used. We have also established the Centre for Data Ethics and Innovation - a new advisory body which will provide independent, expert advice on the measures needed to enable and ensure safe, ethical and innovative uses of AI and data-driven technologies.

The challenges from digital technologies cut across all sectors of society and the economy, and our work reflects this. We commissioned an independent review of competition in the digital economy, undertaken by an expert panel in digital competition led by Professor Jason Furman. We also commissioned the independent Cairncross Review, which considers how the news industry in the UK can become more sustainable as it transitions from print to digital. We will continue to consider a full range of possible solutions, including domestic legal changes where necessary, to ensure the internet works for everyone.

The Government's response to the recommendations in the Committee's report are set out below.

Principles for regulation

1. The 10 principles set out in this report should guide the development and implementation of regulation online and be used to set expectations of digital services. These principles will help the industry, regulators, the Government and users work towards a common goal of making the internet a better, more respectful environment which is beneficial to all. They will help ensure that rights are protected online just as they are offline. If rights are infringed, those responsible should be held accountable in a fair and transparent way. With these principles the internet would remain open to innovation and creativity while a new culture of ethical behaviour would be embedded into the design of services. (Paragraph 68)

   Response:

   We are firmly committed to ensuring that the internet and new technologies are not only safe and secure, but also that they are developed and used responsibly and ethically, with users' interests at their heart.

   The Digital Charter sets out Government's approach to protecting citizens, increase public trust in new technologies, and create the best possible basis on which the digital economy and society can thrive. The Charter outlines the principles underpinning this work, which are closely aligned with those set out in this report.

These principles are:

- *the internet should be free, open and accessible*
- *people should understand the rules that apply to them when they are online*
- *personal data should be respected and used appropriately*
- *protections should be in place to help keep people safe online, especially children*
- *the same rights that people have offline must be protected online*
- *the social and economic benefits brought by new technologies should be fairly shared.*

As set out in the Online Harms White Paper, the Government will establish a new statutory duty of care to make companies take more responsibility for the safety of their users online and tackle harm caused by content or activity on their services. Compliance with this duty of care will be overseen and enforced by an independent regulator. It will have sufficient resources and the right expertise and capability to perform its role effectively.

Ethical technology

2. As organisations, including financial and health services providers, increasingly perceive individuals as the aggregation of data gathered about them (sometimes called their 'data selves'), it is essential that data be accurate, up-to-date and processed fairly and lawfully, especially when processed by algorithm. While the GDPR and the Data Protection Act 2018 provide valuable safeguards, including subject access rights to ensure that data are accurate and up to date and the right to opt out from purely automated processing, there are weaknesses in the regime. For example, a subject access request does not give subjects automatic access to behavioural data generated about them because it is deemed to be the property of the company that acquired it. (Paragraph 80)

3. Users of internet services should have the right to receive a processing transparency report on request. In a model similar to a subject access report under the GDPR users should have the right to request a data transparency report from data controllers showing not only what data they hold on the data subject (which is currently the case under the GDPR) but also what data they generate on them (behavioural data) and any behavioural data obtained from third parties, including details of when and how they are obtained. (Paragraph 81)

Response:

The Government takes both the protection of personal data and the right to privacy extremely seriously. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), alongside the increased powers for the ICO to gather evidence, inspect artificial intelligence (AI) and levy significant fines on those who break the law, update our data protection laws fit for the digital age.

The Data Protection Act 2018, which applies the EU's GDPR standards, ensures data transparency amongst all those who process personal data. Under the GDPR, companies "must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject." These transparency obligations begin at the data collection stage and apply "throughout the life cycle of processing".

By personal data we mean any information relating to an identified or identifiable natural person ('data subject'). The data subject may be identified by reference to an identifier such as their name or an online identifier. The GDPR also has provisions on profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Article 22 of the GDPR define additional rules to protect individuals where automated decision making is taking place that has legal or similarly significant effects on them.

However, the increased use of data and AI is giving rise to complex, fast-moving and far-reaching ethical and economic issues that cannot be addressed by data protection laws alone. Increasingly sophisticated algorithms can glean powerful insights, which can be deployed in ways that influence the decisions we make and the services we receive. It is essential that we understand, and respond to, barriers to the ethical deployment of AI. That is why the Government has set up the Centre for Data Ethics and Innovation. The Centre will provide independent, impartial and expert advice on the ethical and innovative deployment of data and AI.

The Centre published its Work Programme in March 2019, including two major reviews, on the issue of algorithmic bias, across a number of sectors, and online targeting, investigating how data is used to shape people's online environments via the personalisation and targeting of messages, content and services online. The Centre recently announced Calls for Evidence for both of these reviews.

4. Data controllers and data processors should be required to publish an annual data transparency statement detailing which forms of behavioural data they generate or purchase from third parties, how they are stored and for how long, and how they are used and transferred. (Paragraph 82)

Response:

The GDPR places obligations on organisations to process people's data lawfully, fairly and transparently. This includes making it clear to people how their data will be used, who it will be shared with, for how long it will be held and when it will be erased. This information, along with individuals' rights under the Data Protection Act 2018, should be set out clearly in a privacy notice.

5. Digital service providers (such as hardware manufacturers, operators of digital platforms, including social media platforms and entertainment platforms, and games developers) should keep a record of time spent using their service which may be easily accessed and reviewed by users, with periodic reminders of prolonged or extended use through pop-up notices or similar. An industry standard on reasonable use should

be developed to inform an understanding of what constitutes prolonged use. This standard should guide design so that services mitigate the risk of encouraging compulsive behaviour. (Paragraph 88)

Response:

As set out in the Online Harms White Paper, both Government and the regulator will continue to support research in this area to inform future action on screen time.

While there is not yet sufficient evidence of a causal link between screen-based activities and negative effects 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, and some services have already introduced such features.

In June 2018, Apple launched updates to its mobile operating system that help customers reduce interruptions and manage screen time for themselves and their families. Similarly, Google's Family Link app allows parents to view how long their children spend on different apps, approve or block apps their children want to download, or recommend specific apps, as well as set limits on screen time, and remotely lock a child's device for a break. In addition, some gaming consoles, such as Xbox One, Playstation4 and Nintendo Switch have tools which allow parents to control access to content and place limits on screen time.

We need to develop a better understanding not just of the impact of screen time as a whole, but also of the link 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 Chief Medical Officer, Professor Dame Sally Davies. 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.

6. The Information Commissioner's Office should set out rules for the use of algorithms based on the principles set out in chapter 2. The ICO should be empowered to conduct impact-based audits where risks associated with using algorithms are greatest and to require businesses to explain how they use personal data and what their algorithms do. Failure to comply with the rules should result in sanctions. (Paragraph 100)

Response:

The Centre for Data Ethics and Innovation will play a key role in identifying best practice for the responsible use of algorithms, to enable safe and ethical innovation in the use of data. The CDEI will work closely with regulators, including the ICO, to ensure

that the law, regulation and guidance keep pace with developments in data-driven and AI-based technologies.

Moreover, the ICO has powers under s129 of the Data Protection Act 2018 to conduct consensual audits on whether a data controller or processor is complying with good practice in the processing of personal data, including in the use of algorithms. Additionally, one of the key safeguards in the GDPR, which ensures that people's fundamental rights are protected, is the requirement to produce Impact Assessments. Under the GDPR, data controllers must consult the Information Commissioner when a data protection Impact Assessment indicates that processing would pose a high risk to the rights and freedoms of data subjects, including via the use of algorithms. A Data Protection Impact Assessment is a dynamic document where measures to mitigate privacy risks are assessed on an ongoing basis.

7. The ICO should also publish a code of best practice informed by the work of the Centre for Data Ethics and Innovation around the use of algorithms. This code could form the basis of a gold-standard industry 'kitemark'. (Paragraph 101)

Response:

The Centre for Data Ethics and Innovation will identify the measures needed to strengthen and improve the way data and AI is used. It will produce best practice and guidance, as well as publishing reports with clear recommendations to Government.

The Centre recently published its strategy and work programme[1]. This sets out in greater detail how it will operate and its priorities for the coming year, including its initial projects which focus on algorithmic bias and microtargeting.

The Centre will work with regulators to understand and help develop the clear policies, powers and technical solutions they need to meet their regulatory duties in relation to data-driven technology. The CDEI expects to work closely and form partnerships with relevant regulators including the ICO.

8. Data subjects should be given the right to request a statement from a data processor explaining how, if applicable, algorithms are used to profile them, deliver content or drive their behaviour. (Paragraph 102)

Response:

Under Article 15 of the GDPR, individuals have a number of access rights, including the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Data controllers and data processors are under a legal responsibility to provide this information as requested

[1] https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-cdei-2019-20-work-programme

and have to provide this information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

9. Terms of service must be written in a form which is clearly accessible and understandable to internet users. Alongside terms of service statements a 'plain English' statement should be published which sets out clearly and concisely the most relevant provisions. These may make use of infographics or video statements where appropriate. (Paragraph 109)

10. Where children are permitted to access or use a service age-appropriate terms and conditions must be provided. These should be written in language clearly understandable to children of the minimum age allowed on the platform. (Paragraph 110)

11. Maximum privacy and safety settings should be included in services by default. The Information Commissioner's Office should provide guidance requiring platforms to provide greater choice to users to control how their data are collected and used. (Paragraph 115)

Response:

Companies will need, as set out in the Online Harms White Paper, to be able to show how they are fulfilling their statutory duty of care. As part of this, companies will have to ensure that relevant terms and conditions are sufficiently clear and accessible to all users (including to children and other vulnerable users). The future online harms regulator will assess how effectively these terms are enforced as part of an assessment of whether a company has fulfilled its duty of care.

The Data Protection Act 2018 requires the Information Commissioner's Office to produce an 'age-appropriate design code of practice'. This code will provide guidance on the privacy standards that organisations should adopt where they are offering online services and apps that children are likely to access and which will process their data. The code will address a number of areas including the need to implement high privacy settings by default and use language that is clear and easy to understand for children at different stages of their development. The draft code was published by the ICO on 15 April and is now out for public consultation.

12. Regulators must ensure that terms of service are fair and must bring enforcement action against organisations which routinely breach their terms of service. (Paragraph 116)

Response:

The regulator, as set out in the Online Harms White Paper, will assess whether companies have fulfilled their duty of care, including by reference to relevant codes of practice, and compliance with the companies' own relevant terms and conditions. Failure to meet these obligations may result in enforcement action by the regulator.

13. Design principles and standards are a normal part of business life across all sectors. Establishing and enforcing standards that would meet the 10 principles would help to reduce harms to users and society. We recommend that regulation should follow the precautionary principle to ensure ethical design while also recognising the importance of innovation and entrepreneurship. (Paragraph 120)

Response:

Our recently-updated Digital Charter recognises that where regulation is necessary, we will ensure it is well-targeted, proportionate and delivers a stable and predictable business environment for innovation to thrive.

As set out in the Online Harms White Paper, the Government believes that creating a safe user environment online requires online services and products to be designed and built with user safety in mind.

To help drive up safety standards in advance of a regulatory framework we will work with industry and civil society to develop guidance, through a Safety by Design framework, that enables designers of online products and services to clearly understand what safety standards are expected of them - at each stage of product development.

We expect the regulator will use this framework to inform the development of codes of practice that will help companies fulfil their duty of care by ensuring products and services are safe by design. The Government agrees that innovation and entrepreneurship are extremely important and to reflect this the regulator will have a duty to pay due regard to innovation.

14. We recommend that the ethical approach outlined in our 10 principles should be embedded in the teaching of all levels of computer science. The Government should promote and support this. The Centre for Data Ethics and Innovation will also have a role in providing guidance which can be incorporated into teaching, as well as educating users on the ethics and risks of the internet. (Paragraph 121)

Response:

The current computing curriculum covers the safe, responsible, respectful and secure use of technology; how to keep personal information private; and where to go for help and support when there are concerns about online activity or content.

Government and industry have a shared responsibility to educate and empower users to manage their online safety. The new online harms regulator will have a responsibility to promote online media literacy. Ahead of the regulator, the Government will develop an online media literacy strategy. The Centre for Data Ethics and Innovation will identify best practice for the responsible use of data and AI, facilitating, shaping and informing public debates. However, large scale education campaigns are outside the Centre's scope.

Market concentration

15. Mergers and acquisitions should not allow large companies to become data monopolies. We recommend that in its review of competition law in the context of digital markets the Government should consider implementing a public-interest test for data-driven mergers and acquisitions. The public interest standard would be the management, in the public interest and through competition law, of the accumulation of data. If necessary, the Competition and Markets Authority (CMA) could therefore intervene as it currently does in cases relevant to media plurality or national security. (Paragraph 150)

16. The modern internet is characterised by the concentration of market power in a small number of companies which operate online platforms. These services have been very popular and networks effects have helped them to become dominant. Yet the nature of digital markets challenges traditional competition law. The meticulous ex post analyses that competition regulators use struggle to keep pace with the digital economy. The ability of platforms to cross-subsidise their products and services across markets to deliver them free or discounted to users challenges traditional understanding of the consumer welfare standard. (Paragraph 161)

17. In reviewing the application of competition law to digital markets, the Government should recognise the inherent power of intermediaries and broaden the consumer welfare standard to ensure that it takes adequate account of long-term innovation. The Government should work with the Competition and Markets Authority (CMA) to make the process for imposing interim measures more effective. (Paragraph 162)

    Response:

    The Government's Modernising Consumer Markets Green Paper sought views on how well equipped the UK's competition regime is to manage emerging challenges, including the growth of fast-moving digital markets. We continue to consider policy options across the range of measures proposed in the green paper, including for digital markets, and are due to report in summer 2019. This will be informed by the work of the independent Digital Competition Expert Panel, led by Professor Jason Furman which published its recommendations for Government on 13 March 2019. The Government will consider these recommendations carefully and respond to Furman's specific recommendations later this year. Any changes, including legislative, would be subject to further consultation.

18. We take this opportunity to repeat the recommendation that we made in our report 'UK advertising in a digital world' that the CMA should undertake a market study of the digital advertising market. We would be grateful for an update from the Government and the CMA. (Paragraph 163)

    Response:

    The Government supports the committee's recommendation that the CMA conducts a

market study of the digital advertising market, which has been echoed by the Cairncross review and Digital Competition Expert Panel. In his immediate response to the Cairncross review, the Secretary of State for Digital, Culture, Media and Sport confirmed that he has written to the CMA to announce his support for this recommendation, and announced that DCMS will conduct a review on how online advertising is regulated. Government will ensure that DCMS's review is positioned to complement and build on any work the CMA does in this space.

19. Online communications platforms act as gatekeepers for the internet, controlling what users can access and how they behave. They can be compared to utilities in the sense that users feel they cannot do without them and so have limited choice but to accept their terms of service. Providers of these services currently have little incentive to address concerns about data misuse or online harms, including harms to society (Paragraph 172)

20. It is appropriate to put special obligations on these companies to ensure that they act fairly to users, other companies and in the interests of society. These obligations should be drawn up in accordance with the 10 principles we have set out earlier in this report and enforced by a regulator. (Paragraph 173)

Response:

We agree that online communications platforms have special responsibilities to treat users fairly and act in the interests of society.

The Digital Charter sets out our work to protect citizens online and ensure that technology benefits society as a whole. As mentioned above, the principles underpinning the Charter are closely aligned with those set out in this report.

This work includes the plans for world-leading legislation set out in the Online Harms White Paper. A statutory duty of care will make companies more responsible for their users' safety online, especially children and other vulnerable groups. Companies will be held to account for tackling a comprehensive set of online harms. Our proposals will also help companies to protect freedom of expression and other norms that underpin our democratic society.

This also includes a wider programme of work to ensure that the internet and technology work for society as a whole: establishing the Centre for Data Ethics and Innovation to advise on ethical and innovative uses of AI and data-driven technologies; commissioning the independent Furman Review to investigate Digital Competition; and commissioning the Cairncross Review into the future of journalism in the digital age.

21. It is too early to say how effective the right to data portability will be. It has the potential to help counteract the switching costs which lock users into services by giving them more autonomy over and control of their data. This will require greater interoperability. Portability would be more effective if the right applied to social graphs and other inferred data. The Centre for Data Ethics and Innovation should play a role developing

best practice in this area. The Information Commissioner's Office should monitor the operation and effectiveness of this right and set out the basis on which it will be enforced. (Paragraph 180)

Response:

The Government recognises the potential of data portability to grant consumers greater autonomy and control over their data. This is why we commissioned and published research in November 2018 on data mobility, (the report, "Data Mobility, the personal data portability growth opportunity" is available at the following link: https://www.gov.uk/government/publications/research-on-data-portability).

The recent Furman Review also highlighted the role of data mobility in improving competition in digital markets, and Government is considering recommendations in this space. The National Data Strategy will further consider how data portability and data mobility can be used to unlock the power of data for consumers.

The Centre for Data Ethics and Innovation may have a role in advising on data portability.

Online platforms

22. Some have argued that the conditional exemption from liability should be abolished altogether. It has been suggested that using artificial intelligence to identify illegal content could allow companies to comply with strict liability. However, such technology is not capable of identifying illegal content accurately and can have a discriminatory effect. Imposing strict liability would therefore have a chilling effect on freedom of speech. These concerns would need to be addressed before the 'safe harbour' provisions of the e-Commerce Directive are repealed. (Paragraph 194)

Response:

We agree that treating platforms as 'publishers' in regards to content liability, and thereby removing their conditional exemption to liability, would not be proportionate, and might result in the over-removal of legal content with implications for freedom of expression.

In 2018, the Prime Minister announced the Government's intention to review the current liability platforms have for the illegal content that they host. While it is important to ensure that platforms have the right level of liability for the content that they host it is also important to consider what is proportionate and necessary.

Entirely removing the conditional exemption from liability for platforms would likely require companies to undertake mass monitoring of their content, the volume of which can be vast. The current capabilities of monitoring technology, as the committee has noted, do not have perfect accuracy, with accuracy varying between types of content and harms.

We have concluded that standalone changes to the liability regime would be insufficient. Instead, the new regulatory framework will increase the responsibility that services have in relation to online harms, in line with the existing law that enables platforms to operate.

23. Online platforms have developed new services which were not envisaged when the e-Commerce Directive was introduced. They now play a key role in curating content for users, going beyond the role of a simple hosting platform. As such, they can facilitate the propagation of illegal content online. 'Notice and takedown' is not an adequate model for content regulation. Case law has already developed on situations where the conditional exemption from liability under the e-Commerce Directive should not apply. Nevertheless, the directive may need to be revised or replaced to reflect better its original purpose. (Paragraph 195)

Response:

As discussed above, following the Prime Minister's announcement at Davos 2018, the Government has reviewed the current liability platforms have for the illegal content that they host.

Our review found that standalone changes to the content liability regime would be insufficient at driving changes in companies' behaviour, and at tackling online harms. In particular it would fail to address the full range of harms users experience online (addressing only the illegal), and would not tackle the need for companies to have adequate processes and governance systems to mitigate against harm occurring.
The Online Harms White Paper proposes a more thorough approach addressing a broader scope of harms, and the internal systems and processes of a company, while also ensuring the effective oversight of the take-down of illegal content.

It also consults on proposals for new powers that would enable the regulator to disrupt the business activities of a non-compliant company, measures to impose liability on individual members of senior management, and measures to block non-compliant services.

24. Technology companies provide venues for illegal content and other forms of online abuse, bullying and fake news. Although they acknowledge some responsibility, their responses are not commensurate with the scale of the problem. We recommend that a duty of care should be imposed on online services which host and curate content which can openly be uploaded and accessed by the public. This would aim to create a culture of risk management at all stages of the design and delivery of services. (Paragraph 207)

Response:

This recommendation is closely aligned to our proposals in the Online Harms White Paper.

As set out in response to recommendation 1, the Government will establish a new statutory duty of care, enforced by an independent regulator, to make companies take more responsibility for the safety of their users online and tackle harm caused by content or activity on their services. All companies will need to be able to show that they are fulfilling their duty of care. We propose that the regulatory framework should apply to companies that allow users to share or discover user-generated content or interact with each other online. These services are offered by a very wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines.

25. To be effective, a duty of care would have to be upheld by a regulator with a full set of enforcement powers. Given the urgency of the need to address online harms, we believe that in the first instance the remit of Ofcom should be expanded to include responsibility for enforcing the duty of care. Ofcom has experience of surveying digital literacy and consumption, and experience in assessing inappropriate content and balancing it against other rights, including freedom of expression. It may be that in time a new regulator is required. (Paragraph 208)

Response:

As set out in response to recommendation 1, the Government will establish a new statutory duty of care, enforced by an independent regulator. The regulator will have a legal duty to pay due regard to innovation, and to protect users' rights online, particularly their privacy and freedom of expression.

The Government is consulting on whether the regulator should be a new or existing body. If we were to establish a new, dedicated regulator over the long term, we would need to consider options for the interim period, given the time it would take to set up a new body. These include empowering an existing regulator for a limited time period (Ofcom would be a strong candidate, given its experience in upholding its current remit to tackle harmful or offensive content, in the context of TV, film and radio), or establishing a shadow body that can make the necessary preparations ahead of the new authority. Either approach will require cooperation with other regulators to ensure the new framework complements existing safeguards.

26. Content moderation is often ineffective in removing content which is either illegal or breaks community standards. Major platforms have failed to invest in their moderation systems, leaving moderators overstretched and inadequately trained. There is little clarity about the expected standard of behaviour and little recourse for a user to seek to reverse a moderation decision against them. In cases where a user's content is blocked or removed this can impinge their right to freedom of expression. (Paragraph 224)

Response:

The Government agrees that while many companies claim to hold a strong track record on online safety, there is limited transparency about how they implement or enforce their policies, and there is a persistent mismatch with users' experiences.

Companies' terms and conditions are often difficult for users to understand, and safety policies are not consistent across different platforms, with take-down times, description of harms and reporting processes varying. 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. The Government believes that voluntary efforts have not led to adequate or consistent steps to protect users online.

A series of investigations have also highlighted the risk of serious shortcomings in the training, working conditions and support provided for content moderators.

To fulfil the new duty of care set out in the Online Harms White Paper, we will expect companies, where appropriate, to have an effective and easy-to-access complaints function, allowing users to raise either concerns about specific pieces of harmful content or activity, or wider concerns that the company has breached its duty of care. The regulator will have oversight of these processes. We are also consulting on what, if any, other measures should be introduced for users who wish to raise concerns.

27. Community standards should be easily accessible to users and written in plain English. Ofcom should have power to investigate whether the standards are being upheld and to consider appeals against moderation decisions. Ofcom should be empowered to impose fines against a company if it finds that the company persistently breaches its terms of use. (Paragraph 225)

Response:

As set out in response to recommendations 9 and 10, companies' relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The online harms regulator will assess how effectively these terms are enforced as part of any regulatory action.

As outlined in response to recommendation 25, the Government is consulting on whether the regulator should be a new or existing body. The regulator will have a range of enforcement powers, including the power to levy substantial fines.

28. The sector should collaborate with Ofcom to devise a labelling scheme for social media websites and apps. A classification framework similar to that of the British Board of Film Classification would help users to identify more quickly the risks of using a platform. This would allow sites which wish to allow unfettered conversation or legal adult material to do so. Users could then more easily choose between platforms with stricter or more relaxed community standards. (Paragraph 226)

29. Community standards and classifications should be consistent with a platform's age policy. (Paragraph 228)

Response:

As set out in the White Paper, in order to fulfil the duty of care, companies will be required to take robust action where there is evidence that children are accessing inappropriate content. The regulator will set out steps that companies should take to protect children from inappropriate content, in codes of practice. We expect the codes of practice to make clear that companies must ensure that their terms of service state what behaviour and activity is tolerated on the service as well as the measures that are in place to prevent children accessing inappropriate content. The regulator will assess how effectively these terms are enforced as part of any regulatory action.

The Digital Authority

30. We recommend that a new body, which we call the Digital Authority, should be established to co-ordinate regulators in the digital world. We recommend that the Digital Authority should have the following functions:
    - to continually assess regulation in the digital world and make recommendations on where additional powers are necessary to fill gaps;
    - to establish an internal centre of expertise on digital trends which helps to scan the horizon for emerging risks and gaps in regulation;
    - to help regulators to implement the law effectively and in the public interest, in line with the 10 principles set out in this report;
    - to inform Parliament, the Government and public bodies of technological developments;
    - to provide a pool of expert investigators to be consulted by regulators for specific investigations;
    - to survey the public to identify how their attitudes to technology change over time, and to ensure that the concerns of the public are taken into account by regulators and policy-makers;
    - to raise awareness of issues connected to the digital world among the public;
    - to engage with the tech sector;
    - to ensure that human rights and children's rights are upheld in the digital world;
    - to liaise with European and international bodies responsible for internet regulation. (Paragraph 240)

31. Policy-makers across different sectors have not responded adequately to changes in the digital world. The Digital Authority should be empowered to instruct regulators to address specific problems or areas. In cases where this is not possible because problems are not within the remit of any regulator, the Digital Authority should advise the Government and Parliament that new or strengthened legal powers are needed. (Paragraph 241)

32. The Digital Authority will co-ordinate regulators across different sectors and multiple Government department. We therefore recommend that it should report to the Cabinet Office and be overseen at the highest level. (Paragraph 245)

Response:

We support the committee's view that effective regulation of digital technology requires a coordinated and coherent approach across the various sector regulators and bodies tasked with overseeing digital businesses. Government must lead the way in providing oversight and coordination of digital regulation and ensuring consistency and coherence. The Digital Charter outlines Government's programme of work to ensure regulation and governance of digital technology are robust, clear, proportionate and keep pace with challenges arising from a rapidly-evolving sector, as well as the fundamental principles underpinning our approach to regulating the digital world.

As part of this programme of work, we look to the tech sector, businesses and civil society, as well as the regulators themselves, to own these challenges with us, using our convening power to bring them together to find solutions where possible. We are committed to making it as easy as possible for citizens and others to give us their views. Where regulation is necessary, we will ensure it is well-targeted, proportionate and delivers a stable and predictable business environment for innovation to thrive.

We are taking a wide range of measures to strengthen the regulation of the internet and digital technology. These include the new Online Harms White Paper, Centre for Data Ethics and Innovation, Furman Review and Cairncross Review. We will ensure our overall approach is coherent and easy to understand for citizens as well as businesses. However, we also recognise the need for further action in this complex and fast moving space.

The government is carefully considering potential overlaps between new regulatory functions, such as that proposed through the Online Harms White Paper, and the remits of existing regulators. Consolidation of these functions, or a broader restructuring of the regulatory landscape, could play an important role in supporting an effective overall approach to the regulation of digital, as well as minimising burdens on businesses, and this is something we will carefully consider.

We thank the Committee for their recommendation and will carefully consider this and their other recommendations as we continue to assess the need for further intervention.

These are challenges with which every nation is grappling. The internet is a global network and we will liaise with European and international organisations that share our ambition and determination to get this right.

33. We recommend that a joint committee of both Houses of Parliament should be established to consider matters related to the digital environment. In addition to advising the Government the Digital Authority should report to Parliament on a quarterly basis and regularly give evidence to the new joint committee to discuss the adequacy of powers and resources in regulating the digital world. The combined force of the Digital Authority and the joint committee will bring a new consistency and urgency to regulation. (Paragraph 246)

Response:

The Department for Digital, Culture, Media and Sport notes the recommendation for the creation of a new committee comprising of members from both Houses. The Government believes that the decision over whether to create a new committee is one for Parliament to take independently of Government.

If a new committee is convened, the Department for Digital, Culture, Media and Sport looks forward to working closely with it in the future.