House of Commons

Digital, Culture, Media and Sport Committee

Misinformation in the COVID-19 Infodemic: Government Response to the Committee's Second Report

Fourth Special Report of Session 2019–21

Ordered by the House of Commons
to be printed 13 October 2020

The Digital, Culture, Media and Sport Committee

The Digital, Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Digital, Culture, Media and Sport and its associated public bodies.

Current membership

Julian Knight MP (*Conservative, Solihull*) (Chair)

Kevin Brennan MP (*Labour, Cardiff West*)

Steve Brine MP (*Conservative, Winchester*)

Philip Davies MP (*Conservative, Shipley*)

Alex Davies-Jones MP (*Labour, Pontypridd*)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Damian Green MP (*Conservative, Ashford*)

Damian Hinds MP (*Conservative, East Hampshire*)

John Nicolson MP (*Scottish National Party, Ochil and South Perthshire*)

Giles Watling MP (*Conservative, Clacton*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/dcmscom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Kate Anderson (Second Clerk), Keely Bishop (Committee Operations Assistant), Andy Boyd (Committee Operations Manager), Conor Durham (Committee Specialist), Lois Jeary (Committee Specialist), Stephen McGinness (Clerk), Charlotte Swift (Second Clerk), Anne Peacock (Senior Media and Communications Officer) and Gina Degtyareva (Media and Communications Officer).

Contacts

All correspondence should be addressed to the Clerk of the Digital, Culture, Media and Sport Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6188; the Committee's email address is cmscom@parliament.uk.

You can follow the Committee on Twitter using @CommonsDCMS.

Fourth Special Report

The Digital, Culture, Media and Sport Committee published its Second Report of Session 2019–21, Misinformation in the COVID-19 Infodemic (HC 234) on 21 July 2020. The Government's response was received on 9 October 2020 and is appended to this Report.

Appendix: Government Response

The Government welcomes this report and is grateful for the Committee's comprehensive inquiry into "Misinformation in the COVID-19 Infodemic".

The Government recognises the Committee's concerns that alongside the outbreak of COVID-19, the world also faced an 'infodemic' of information—both accurate and false. The Government takes the issue of disinformation and misinformation very seriously. It is vitally important, at a time of national emergency, that the public has accurate information. The Department for Digital, Culture, Meda and Sport has been leading work across Government to tackle disinformation and misinformation relating to COVID-19. The Cross-Whitehall Counter Disinformation Unit stood up on 5 March 2020, brings together cross-Government monitoring and analysis capabilities to provide a comprehensive picture of the extent, scope and the reach of disinformation and misinformation on COVID-19, and to work with partners to ensure appropriate action is taken. We continue to work with industry to support the introduction of systems and processes that promote authoritative sources of information. Latest Ofcom figures state that among adult internet users, traditional media sources (broadcasters, newspapers, radio) remain both the most-used source of news and information about Covid-19.

Since publishing the Online Harms White Paper, the Government has continued to see new risks and threats posed by disinformation and misinformation. In recent months, social media has been a significant source of misinformation about COVID-19. The Government recognises the threat presented by disinformation and misinformation online and is taking action to address this. The Government is aiming to publish the Online Harms full Government Response later this year. The Government acknowledges that further detail on some of our policy proposals will be laid out in the Online Harms full Government Response.

The Government's response to the report's recommendations is below.

Introduction

1.   *We recommend that the Government publish draft legislation, either in part or in full, alongside the full consultation response this autumn if a finalised Bill is not ready. Given our ongoing interest and expertise in this area, we plan to undertake pre-legislative scrutiny. We also remind the Government of our predecessor Committee's recommendation for the DCMS Committee to have a statutory veto over the appointment and dismissal of the Chief Executive to ensure public confidence in their independence, similar to the Treasury Committee's veto over senior appointments to the Office of Budget Responsibility, and urge the Government to include similar provisions in the Bill.* (Paragraph 12)

The Government is firmly committed to making the UK the safest place to be online, and will introduce Online Harms legislation as soon as possible. The increased reliance on the internet during the COVID-19 pandemic has highlighted the importance of introducing a new regulatory regime that will enable us to protect users and adapt to new challenges online.

The Government is working at pace to publish the full consultation response to the Online Harms White Paper consultation later this year. This will be shortly followed by legislation, which will be ready early next year.

2.   *We strongly recommend that the Government bring forward a detailed process for deciding which harms are in scope for legislation. This process must always be evidence-led and subject to democratic oversight, rather than delegated entirely to the regulator. Legislation should also establish clearly the differentiated expectations of tech companies for illegal content and 'harmful but legal'.* (Paragraph 16)

Further detail on our policy proposals will be laid out in the Online Harms full Government Response, including on 'harmful but legal' content. The final policy position will provide clarity for companies about harms in scope, while ensuring flexibility to respond to emerging harms.

As per the interim consultation response published in February this year, the legislation will establish differentiated expectations on companies for illegal content and activity, versus conduct that is not illegal but has the potential to cause harm.

Services in scope of the regulation will be required to ensure that illegal content is removed expeditiously and that the risk of it appearing in the first place is minimised by effective systems. Reflecting the threat to national security and the physical safety of children, companies will be required to take particularly robust action to tackle terrorist content and online child sexual exploitation and abuse.

For conduct that is not illegal but has the potential to cause harm, the interim response noted that the new regulatory framework will instead require companies to set out what type of legal content or behaviour is acceptable on their services in clear and accessible terms and conditions. They will need to enforce these terms effectively, consistently and transparently. The proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content where this occurs.

3.   **These technologies, media and usage trends are fast-changing in nature. Whatever harms are specified in legislation, we welcome the inclusion alongside them of the wider duty of care, which will allow the regulator to consider issues outside the specified list (and allow for recourse through the courts). The Committee reject the notion that an appropriate definition of the anti-online harms measures that operators should be subject to are simply those stated in their own terms and conditions.** (Paragraph 17)

The new online harms regime will apply to user-generated content on companies' platforms.

The duty of care will require that companies have appropriate systems and processes in place to deal with harmful content and activity on their services to keep their users safe. The regulator will issue codes of practice setting out steps that companies can take to fulfil the duty of care and to address the range of harmful user generated content that is in scope.

Under the regulatory framework, providers will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised by effective systems. Companies will also be required to take reasonable steps to protect children from harm.

The framework will give companies, where relevant, a duty for legal but harmful content on their services which are accessed by adults. Companies will need to set out what type of legal content or behaviour is acceptable on their services in clear and accessible terms and conditions. They will need to enforce these terms effectively, consistently and transparently. The proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content where this occurs.

Further detail on our policy proposals will be laid out in the Online Harms full Government Response.

Tech companies' response

4.   *The Government should consider how algorithmic auditing can be done in practice and bring forward detailed proposals in the final consultation response to the White Paper.* (Paragraph 20)

As set out in the Online Harms White Paper, the Government has committed to giving the regulator the power to require annual transparency reports from companies in scope, which will include information about the measures being taken to address harmful content and activity.

To fulfill the duty of care, companies will need to understand the risks associated with the operation of their algorithms and recommendation tools and put in place measures to mitigate these risks where relevant.

The Government will ensure that the regulator is equipped with the powers and expertise it needs to determine whether companies are fulfilling their duty of care, including in relation to the operation of their algorithms.

5.   *To properly address these issues, the online harms regulator will need sight of comprehensive advertising libraries to see if and how advertisers are spreading misinformation through paid advertising or are exploiting misinformation or other online harms for financial gain. Tech companies should also address the disparity in transparency regarding ad libraries by standardising the information they make publicly available. Legislation should also require advertising providers like Google to provide directories of websites that they provide advertising for, to allow for greater oversight in the monetisation of online harms by third parties.* (Paragraph 24)

Online Harms regulation will apply to companies that facilitate sharing of user-generated content and user interaction. Full details of the scope of regulation will be included in the Full Government Response.

The Government is considering holistic approaches to address harms which may arise as a result of advertising online, including the monetisation of potentially harmful content. In February 2019, the Department for Digital, Culture, Media and Sport announced it will consider how online advertising is regulated and In January 2020, the Government launched a call for evidence to gather additional evidence. The Call for Evidence closed on 4 May 2020. The Government is analysing the responses received and will publish a response document in due course.

6.   **Tech companies rely on quality journalism to provide authoritative information. They earn revenue both from users consuming this on their platforms as well as (in the case of Google) providing advertising on news websites, and news drives users to their services. We agree with the Competition and Markets Authority that features of the digital advertising market controlled by companies such as Facebook and Google must not undermine the ability of newspapers and others to produce quality content. Tech companies should be elevating authoritative journalistic sources to combat the spread of misinformation. This is an issue to which the Committee will no doubt return.** (Paragraph 26)

Dynamic and competitive digital markets are key to building a world-leading digital economy that works for consumers, businesses and society. The Government is committed to ensuring that it takes an effective, pro-innovation and coherent approach to governing digital technologies and this includes supporting news publishers to adopt sustainable digital business models online.

The Government recognises the vital role of newspapers in supporting communities and isolated individuals, and in ensuring the provision of reliable, high-quality information. It has been an absolute priority to ensure we do all we can as a Government to support news publishers at this time of financial instability. Measures to support news publishers include bringing forward the commencement of zero-rating of VAT on e-newspapers in order to bring savings to readers during the coronavirus outbreak, as well as to support publishers.

The Government thanks the Competition and Markets Authority for completing their market study report and will carefully consider its recommendations and respond in due course.

Platforms' efforts to help users identify the reliability and trustworthiness of news sources may continue and expand as a result of the proposals in the Online Harms White Paper.

Whilst the Government is taking action to address false narratives online, we will ensure that freedom of expression in the UK is protected and enhanced online.

7. **The Government is acutely conscious that disinformation around the public health issues of the COVID-19 crisis have been relatively easy for tech companies to deal with, as binary true/false judgements are often applicable. In normal times, dealing with the greater nuance of political claims, the prominence of quality news sources on platforms, and their financial viability, will be all the more important in tackling misinformation and disinformation.** (Paragraph 27)

The Government agrees that a free and independent media are essential qualities of any functioning democracy and quality journalism plays a critical role in tackling misinformation and disinformation. Platforms' efforts to help users identify the reliability and trustworthiness of sources can allow these sources to reach audiences more easily and may continue and expand as a result of the proposals in the Online Harms White Paper.

Online media literacy can equip users with the skills they need to critically appraise the content they consume online, including information about political discourse, and take steps to keep themselves and others safe online. The Online Harms White Paper set out the Government's intention to develop an online media literacy strategy. The strategy will ensure a coordinated and strategic approach to online media literacy education and awareness for children, young people and adults. The Government aims to publish the media literacy strategy in Spring 2021.

8. *The Government must empower the new regulator to go beyond ensuring that tech companies enforce their own policies, community standards and terms of service. The regulator must ensure that these policies themselves are adequate in addressing the harms faced by society. It should have the power to standardise these policies across different platforms, ensuring minimum standards under the duty of care. The regulator should moreover be empowered to hand out significant fines for non- compliance. It should also have the ability to disrupt the activities of businesses that are not complying, and ultimately to ensure that custodial sentences are available as a sanction where required.* (Paragraph 32)

As per the interim consultation response published in February this year, regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that is not illegal but has the potential to cause harm.

Under the regulatory framework, providers will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised by effective systems. All companies in scope will need to ensure a higher level of protection for children, and take reasonable steps to protect them from inappropriate or harmful content.

For conduct that is not illegal but has the potential to cause harm, companies will need to set out what type of legal content or behaviour is acceptable on their services in clear and accessible terms and conditions. They will need to enforce these terms effectively, consistently and transparently. The proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content and also failure to properly enforce terms and remove prohibited content, where this occurs.

This approach will make companies more responsible for their users' safety online and address concerns about legal but harmful content, while at the same time ensuring that freedom of expression is protected.

The regulator will be able to take enforcement action against companies that do not fulfil these duties. The regulator will have the power to issue warnings, notices and fines. Alongside this the Government consulted on whether the regulator should have further powers to disrupt business activities, including blocking by internet service providers.

Further detail on our policy proposals will be laid out in the Online Harms full Government Response, including on 'harmful but legal' content.

9.   *Alongside developing its voluntary codes of practice for child sexual exploitation and abuse and terrorist content, the Government should urgently work with tech companies to develop a voluntary code of practice to protect citizens from the harmful impacts of misinformation and disinformation, in concert with academics, civil society and regulators. A well-developed code of practice for misinformation and disinformation would be world-leading and will prepare the ground for legislation in this area.* (Paragraph 34)

Since publishing the Online Harms White Paper, the Government has continued to see new risks and threats posed by disinformation and misinformation. In recent months, social media has been a significant source of misinformation about COVID-19. The Government recognises the threat presented by disinformation and misinformation online and is taking action to address this.

In addition to potential measures to be brought in through the Online Harms legislation, there are a number of other steps being taken to tackle misinformation and disinformation. In particular, building the public's critical thinking skills and digital resilience, enabling them to tell fact from fabrication, is key to long-term success in tackling this issue. The Online Harms White Paper set out the Government's intention to develop a coordinated strategy for online media literacy education and awareness for children, young people and adults. The Government aims to publish the media literacy strategy in Spring 2021.

The Government is clear that social media firms have further work to do to tackle misinformation and disinformation on their platforms. In particular they should:

- Continue to develop their technological capabilities for detecting and removing disinformation as well as other harmful content on their platforms.

- Ensure that their users are fully informed of the risks of misinformation and disinformation on their platforms and the steps they can take to protect themselves.

- Provide greater transparency on the actions they are taking to tackle this kind of content on their platforms, including improving access for researchers to better understand the scale, scope and impact of misinformation and disinformation.

10.   **Currently, tech companies emphasise the effectiveness of AI content moderation over user reporting and human content moderation. However, the evidence has shown that an overreliance on AI moderation has limitations, particularly as regards speech, but also often with images and video too. We believe that both easy-to- use, transparent user reporting systems and robust proactive systems, which combine AI moderation but also human review, are needed to identify and respond to misinformation and other instances of harm.** *To fulfil their duty of care, tech companies must be required to have easy-to-use user reporting systems and the capacity to respond to these in a timely fashion. To provide transparency, they must produce clear and specific information to the public about how reports regarding content that breaches legislative standards, or a company's own standards (where these go further than legislation), are dealt with, and what the response has been. The new regulator should also regularly test and audit each platform's user reporting functions, centring the user experience from report to resolution in its considerations.* (Paragraph 39)

Improving users' access to reporting and redress will be a key part of the new online harms regulatory framework. All companies will be required to have accessible and effective mechanisms for users to report and seek redress for harmful content, as well as if they consider their rights to have been infringed (for example through wrongful takedown of content), or have wider concerns about a company's conduct. Mechanisms will need to be transparent and consistently applied. Expectations must also be proportionate to the risk of harm and a company's capacity to address harm. The regulator will have oversight of services' user redress mechanisms.

The Government has also consulted on a super-complaints mechanism, which would enable designated bodies to raise concerns with the regulator in specific and clearly-evidenced circumstances.

As set out in the Online Harms White Paper, the Government has committed to giving the regulator the power to require annual transparency reports from companies in scope, which will include information about the enforcement of companies terms and conditions and the user reporting processes that are in place.

The Government is also supporting the growth of the UK safety tech industry, companies offering helping to deliver safer online experiences. Safety tech can support online communities and businesses across a wide range of issues. This includes reducing the burden on human content moderators through the use of cutting-edge artificial intelligence, allowing moderators to focus on the cases most in need of human review and flagging user interactions which are potentially harmful, illegal, or which break a site's own terms and conditions. The UK's safety tech industry is world-leading and has clear potential to provide safety solutions to respond to a wide range of online harms.

11.   **Research has consistently suggested that bots play an active role in spreading disinformation into users' news feeds.** *Tech companies should be required to regularly report on the number of bots on their platform, particularly where research suggests these might contribute to the spread of disinformation. To provide transparency for platform users and to safeguard them where they may unknowingly interact with and be manipulated by bots, we also recommend that the regulator should require companies to label bots and uses of automation separately and clearly.* (Paragraph 42)

As set out in the Online Harms White Paper, the Government has committed to giving the regulator the power to require annual transparency reports from companies in scope, which will include information about the prevalence of harmful content on platforms, and what measures are being taken to address these.

The Government has made clear to social media companies that significant action is needed to protect users from coordinated inauthentic behaviour and other forms of manipulation on their platforms. Bots present a particular challenge, and whilst automated accounts can have a positive impact on user experience, for example the World Health Organisation COVID-19 Facebook messenger chatbot, social media companies need to address this issue as part of wider activity to tackle the spread of misinformation and disinformation on their platforms.

Following our engagement during the COVID-19 pandemic, platforms have updated their terms of service to be able to take more decisive action against mis- and disinformation related to the virus and made some positive technical changes to their products. However, it is clear that there is much more work to be done and the Government will continue to put pressure on the platforms to enhance transparency and drive user resilience, including in response to the malign use of bots and automation.

The Government continues to work closely with social media companies and civil society to develop solutions to the problem of coordinated inauthentic behaviour and related threats. As part of this, the Government will look to build on the positive discussions that we have had with platforms throughout the Covid response to ensure that we are able to effectively respond to the current and emerging challenges in this space.

12. ***The new regulator should be empowered to examine the role of user verification in the spread of misinformation and other online harms, and should look closely at the implications of how policies are applied to some accounts relative to others.*** (Paragraph 45)

In order to reduce the potential impact of disinformation, the Government must take account not only of the actors involved, but of the environment that enables them to spread and amplify falsehoods, and the audience that they reach.

The Online Harms White Paper set out disinformation and online manipulation as harms proposed to be in scope of the regulatory framework. The Government has been considering this legislative option and a number of non-legislative options to address the issue.

The Government has undertaken research into how attributes of a user's identity, in particular their age, can be used to counter online harms. The Verification of Children Online is a joint research project between DCMS, HO and GCHQ. It has looked in detail at how age assurance solutions and the knowledge of a user's age could be used to improve standards of online safety.

The Government recognises that some users will take deliberate attempts to conceal their identity online, to spread false information or to abuse others. There are, however, many legitimate reasons why an individual would not wish to identify themselves online. For example, whistle-blowers, victims of modern slavery and surivors of domestic abuse may want to remain anonymous online. Our proposals strike the right balance

between protecting users' online, so they are safe from harm, while preserving freedom of expression. Further details will be published in the full Government Response later this year.

13. **We recognise tech companies' innovations in tackling misinformation, such as 'correct the record' tools and warning labels. We also applaud the role of independent fact-checking organisations, who have provided the basis for these tools. These contributions have shown what is possible in technological responses to misinformation, though we have observed that often these responses do not go far enough, with little to no explanation as to why such shortcomings cannot be addressed. Twitter's labelling, for instance, has been inconsistent, while we are concerned that Facebook's corrective tool overlooks many people who may be exposed to misinformation. For users who are known to have dwelt on material that has been disproved and may be harmful to their health, it strikes us that the burden of proof should be to show why they should not have this made known to them, rather than the other way around.** (Paragraph 49)

The Government notes the Committee's views on labelling, and agrees platforms must do more to ensure users are fully equipped to make decisions on the authenticity of content they see.

The Government is working closely with social media companies and civil society organisations, particularly in the COVID-19 context at present, and are exploring ways to enhance our understanding of which interventions are proving most effective for tackling misinformation on the platforms. Part of this work includes examining whether platform policies are fit for purpose and being appropriately applied.

The Government is also working closely with the UK safety technology industry to support the growth of a market in products and services that help keep users safer online. This has included support for the launch of a new industry association (the Online Safety Tech Industry Association) in April 2020, and publication of a report into sector value in May 2020. In coming weeks the Government will be sponsoring a major safety tech sector conference, and launching a Safety Technology Innovation Network to facilitate cross-sector collaboration and raise buyer awareness of the industry. The Government is also launching a £2.6m project to improve the data infrastructure around online harms, to improve competitiveness and promote interoperability of solutions.

14. *The new regulator needs to ensure that research is carried out into the best way of mitigating harms and, in the case of misinformation, increasing the circulation and impact of authoritative fact-checks. It should also be able to support the development of new tools by independent researchers to tackle harms proactively and be given power to require that, where practical, those methods found to be effective are deployed across the industry in a consistent way. We call on the Government to bring forward proposals in response to this report, to give us the opportunity to engage with the research and regulatory communities and to scrutinise whether the proposals are adequate.* (Paragraph 50)

The Government will ensure that the regulator has the powers it needs to carry out research to build its understanding of how companies can mitigate online harms.

The White Paper recognised the important role that independent researchers can play in building the understanding of online harms and how they can be mitigated. The regulator will engage with independent researchers and will encourage companies to make relevant information available to researchers, subject to appropriate safeguards.

Public sector response

15. **Research has shown that the public has turned away from tech companies' platforms as a source of trusted news and towards public sector broadcasting during the COVID-19 crisis, demonstrating a lack of trust in social media. The Government must take account of this as it develops online harms legislation over the coming months. It has already committed to naming an independent regulator; it should also look to the 'clear set of requirements' and 'detailed content standards' in broadcasting as a benchmark for quantifying and measuring the range of harms in scope of legislation.** (Paragraph 54)

The Government will publish a Full Government Response to the Online Harms White Paper Consultation later this year, and further detail on our policy proposals will be laid out in the response, including on 'harmful but legal' content. The final policy position will need to provide clarity for companies about harms in scope, while ensuring flexibility to respond to emerging harm.

As per the interim consultation response published in February this year, regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that is not illegal but has the potential to cause harm.

Services in scope of the regulation will need to ensure that illegal content is removed expeditiously and that the risk of it appearing is minimised by effective systems. Reflecting the threat to national security and the physical safety of children, companies will be required to take particularly robust action to tackle terrorist content and online child sexual exploitation and abuse.

For conduct that is not illegal but has the potential to cause harm, the new regulatory framework will instead require companies to set out what type of legal content or behaviour is acceptable on their services in clear and accessible terms and conditions. They will need to enforce these terms effectively, consistently and transparently. The proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content where this occurs.

We are working with industry to support the introduction of systems and processes that promote authoritative sources of information. Ofcom figures state that among adult internet users, traditional media sources (broadcasters, newspapers, radio) remain both the most-used source of news and information about Covid-19 (84% in week twenty-five vs. 93% in week one) and the most important source of news and information to users (64% in week twenty-five vs. 71% in week one). Over 65s are more likely to use traditional media (96%) compared to 18-24s (73%).

16. *The Government should support the BBC to be more assertive in deepening private sector involvement, such as by adapting the Trusted News Initiative to changes in the social media ecosystem such as the emergence of TikTok and other new platforms. The Government and online harms regulator should use the TNI to ' join up' approaches to public media literacy and benefit from shared learning regarding misinformation and disinformation. It should do this in a way that respects the independence from Government and expertise of the group's members, and not impose a top-down approach.* (Paragraph 58)

The Government recognises the role and potential of the Trusted News Initiative in combating misinformation and disinformation. The Trusted News Initiative is supported by a range of public sector and private sector news organisations, including the British Broadcasting Corporation, who helped set up the initiative. As the committee notes, these organisations and the Trusted News Initiative itself are independent of Government. The Government will look at how best to engage with the the Trusted News Initiative, including considering how it may develop, in due course, initiatives which make the best use of available Government encouragement and support.

The Government is also developing a media literacy strategy which will ensure a coordinated and strategic approach to online media literacy education for children, young people and adults. The strategy will aim to support citizens as users in thinking critically about the things they come across online, and consider how tech platforms can include 'safety by design' features to assist users in making critical assessments. It is being developed in broad consultation with stakeholders, including major digital, broadcast and news media organisations, the education sector, researchers and civil society.

Additionally, the White Paper proposed that the new regulator will have responsibility to promote online media literacy, have oversight of industry activity and spend and have the power to require companies to report on their education and awareness activity. The Government is working with Ofcom on how they would deliver the new regulatory framework most effectively if the Government confirms its decision to appoint it as the online harms regulator. The Government will provide further details about the future online harms regulator in the full Government response later this year.

17. **The Government should reconsider how the various teams submitting information to the Counter Disinformation Unit best add value to tackling the infodemic. Factchecking 70 instances of misinformation a week duplicates the work of other organisations with professional expertise in the area.** *Instead, the Government should focus on opening up channels with organisations that verify information in a 'Factchecking Forum', convened by the Counter Disinformation Unit, and share instances that are flagged by these organisations across its stakeholders, including and especially to public health organisations and all NHS trusts, key and/or frontline workers and essential businesses to prepare them for what they may be facing as a direct result of misinformation, allowing them to take appropriate precautions.* (Paragraph 63)

The Counter Disinformation Unit coordinates Government response to misinformation and disinformation, focusing on issues where there is a clear risk to public health. The Unit does not provide a fact checking function, and is therefore not duplicative of fact checking organisations, but instead identifies the most appropriate way to ensure that the

public has access to reliable information. This includes delivering rebuttals through the Cabinet Office, or working with social media platforms to take action on content which violates their terms of service.

The Government works closely with independent fact checkers to promote verified information and ensure stakeholders are prepared to respond to mis-and disinformation risks as early as possible. In the COVID-19 context the Government is collaborating with the Department for Health and Social Care and the National Health Service to develop new ways to engage with social media companies and civil society organisations to understand which interventions are most effective for tackling misinformation on the platforms.

18.   *We recommend that the Government also empower the new online harms regulator to commission research into platforms' actions and to ensure that companies pass on the necessary data to independent researchers and independent academics with rights of access to social media platform data. It should also engage with the Information Commissioner's Office to ensure this is done with respect to data protection laws and data privacy. In the long term, the regulator should require tech companies to maintain 'takedown libraries', provide information on content takedown requests, and work with researchers and regulators to ensure this information is comprehensive and accessible. Proposals for oversight of takedowns, including redressal mechanisms, should be revisited to ensure freedom of expression is safeguarded.* (Paragraph 64)

The White Paper recognised the important role that independent researchers can play in building the understanding of online harms and how they can be mitigated. The regulator will engage with independent researchers and will encourage companies to make relevant information available to researchers, subject to appropriate safeguards.

As clarified in the initial response to the consultation, all companies will be required to have effective and accessible mechanisms for user reporting and redress. These mechanisms will need to enable users to challenge content takedown, as an important protection for freedom of expression.

19.   *In order to role model to demonstrate best practice regarding tech companies' advertising libraries, the Government should create its own ad archive, independent of the archive made available by tech companies, to provide transparency, oversight and scrutiny about how these ad credits are being used and what information is being disseminated to the public.* (Paragraph 67)

Through the Online Advertising Programme, the Government is in the process of assessing the current regulatory system for online advertising to ensure that it fosters fair, transparent and ethical online advertising that works for citizens, businesses and society as a whole. It will consider the recommendations to increase accountability of online advertising as part of this programme of work. The programme will reflect upon a wide range of sources to inform policy development, including the Centre for Data Ethics and Innovation report on online targeting, that proposes measures such as advertising libraries.

20. **The Government had committed to publishing a media literacy strategy this summer. We understand the pressures caused by the crisis, but believe such a strategy would be a key step in mitigating the impact of misinformation, including in the current pandemic.** *We urge the Government to publish its media literacy strategy at the latest by the time it responds to this Report in September. We welcome the non-statutory guidance from the Department for Education on 'Teaching online safety in school' (June 2019), bringing together computing, citizenship, health and relationships curricula, which among other things covers disinformation and misinformation. We ask that the Government reports on adoption of this material before the end of the academic year 2020/1.* (Paragraph 69)

The media literacy field is a broad one, and the Government is continuing to consult widely in order to ensure the strategy's objectives are well informed by evidence and take account of insights gathered on misinformation and disinformation during COVID-19. The Government aims to publish the media literacy strategy in Spring 2021.

Last year, the Department for Education published "Teaching online safety in schools" in June 2019 - non-statutory guidance which aims to support schools in teaching pupils how to stay safe online within new and existing school subjects, such as Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing.

In England, from September 2020, the Government has introduced the mandatory subjects of Relationships Education (for all primary school-aged pupils), Relationships and Sex Education (for all secondary school-aged pupils) and Health Education (for all pupils in primary and secondary state-funded schools). The new subjects, at their heart, are about empowering pupils with the knowledge that will support their relationships and health, now and in the future, enabling them to become active and positive members of society.

The Department will be conducting an evaluation on the impact of the new subjects as a whole, from October 2021. This will include a wider assessment on the impact of Religious, Sex & Health Education implementation. The evaluation will cover the content listed in statutory guidance.

In addition, the Department has invested £84m in the creation of a National Centre for Computing Education, to improve the quality of computing teaching in England. The National Centre for Computing Education are leading on an ambitious programme to train over 21,000 teachers, providing a computing hub network in England and high quality resources for teachers that link to other parts of the curriculum such as Personal, Social, Health & Economic Education and cover e-safety. In addition, all of the National Centre for Computing Education primary resources are linked to the 'Education for a Connected World' curriculum framework, a tool that is used by teachers of all subjects, to build effective online safety strategies and which outlines the digital knowledge and skills that children and young people should have at different ages and stages of their lives. Over 9,800 schools have engaged with the National Centre for Computing Education programme in 2020, which is over two and a half times higher than the number of schools engaging in 2019. The National Centre for Computing Education programme will run until July 2022.

Ofsted's new education inspection framework came into effect in September 2019 and has a new stronger emphasis on ensuring schools provide a broad and rich curriculum for all their pupils. The new arrangements also include a new separate graded judgement on pupils' personal development – strengthening the emphasis on this important aspect. The personal development judgement, outlined in the new Schools Inspection Handbook, focuses on the development of pupils' character, their confidence, resilience, independence and knowledge. It includes a range of matters including pupils' ability to recognise and respond to online and offline risks to their wellbeing. Ofsted plan to resume routine inspections from January 2021, with this date being kept under review. Once routine inspection resumes, inspections will evaluate schools against its new framework which includes the strong focus on the provision of a broad and balanced curriculum and pupils' personal development.

21.   *The Government should set out a comprehensive list of harms in scope for online harms legislation, rather than allowing companies to do so themselves or to set what they deem acceptable through their terms and conditions. The regulator should have the power instead to judge where these policies are inadequate and make recommendations accordingly against these harms.* (Paragraph 72)

As per the interim consultation response published in February this year, regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that is not illegal but has the potential to cause harm.

For conduct that is not illegal but has the potential to cause harm, our proposed approach will improve transparency for users about which content is and is not acceptable on different platforms, and will enhance users' ability to challenge removal of content where this occurs.

The regulator will be able to take enforcement action against companies that do not fulfil these duties. The regulator will have the power to issue warnings, notices and fines. Alongside this the Government has consulted on whether the regulator should have further powers to disrupt business activities, including blocking by internet service providers.

22.   **We are pleased that the Government has taken up our predecessor Committee's recommendation to appoint an independent regulator. The regulator must be named immediately to give it enough time to take on this critical remit. Any continued delay in naming an online harms regulator will bring into question how seriously the government is taking this crucial policy area. We note Ofcom's track record of research and expedited work on misinformation in other areas of its remit in this time of crisis as arguments in its favour.** *We urge the Government to finalise the regulator in the response to this Report. Alongside this decision, the Government should also make proposals regarding the powers Ofcom would need to deliver its remit and include the power to regulate disinformation. We reiterate our predecessor Committee's calls for criminal sanctions where there has been criminal wrongdoing. We also believe that the regulator should facilitate independent researchers 'road testing' new features against harms in scope, to assure the regulator that companies have designed these features ethically before they are released to the public.* (Paragraph 76)

In February 2020, the Government announced it was minded to appoint Ofcom as the online harms regulator. The Government will confirm the identity of the regulator in the Full Government Response due to be published later this year.

The Full Government Response will set out in detail the powers and responsibilities of the online harms regulator. In advance of regulation coming into force the Government will publish a Safety by Design Framework that will provide companies with practical guidance on what 'good' looks like for service design in relation to user safety.

The regulator will have a suite of enforcement powers to take action against companies that fail to fulfil their duty of care.

23.   *The Government should also consider how regulators can work together to address any gaps between existing regulation and online harms. It should do this in consultation with the Digital Regulation Cooperation Forum, the creation of which we note as a proactive step by the regulatory community in addressing this. We believe that other regulatory bodies should be able to bring super-complaints to the new online harms regulator.* (Paragraph 78)

The Government is committed to developing a strategic approach to governing digital technologies and is reviewing the institutional landscape to ensure it is fully coherent, efficient and effective.

The Government recognises that strong coordination across regulators is vital to delivering a coherent and joined up approach to digital regulation. The Government welcomes steps that have already been taken in this space, including the creation of the Digital Regulators Cooperation Forum, and are assessing the need for further measures.

The Government has consulted on a super-complaints mechanism and will announce further details in the full Government response later this year. However, it is important to note that there are many avenues for regulators to work with, and raise issues with, each other. Ongoing collaboration between the online harms regulator and other organisations will be essential as part of our joined-up approach to digital regulation. Ofcom has shown a strong track record in engaging with other organisations, including the Information Commissioner's Office and Competition and Markets Authority, through formal and informal means of cooperation.