House of Commons

Digital, Culture, Media and Sport Committee

Disinformation and 'fake news': Final Report: Government Response to the Committee's Eighth Report of Session 2017–19

Seventh Special Report of Session 2017–19

Ordered by the House of Commons to be printed 8 May 2019

HC 2184
Published on 9 May 2019
by authority of the House of Commons

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

Damian Collins MP (*Conservative, Folkestone and Hythe*) (Chair)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Paul Farrelly MP (*Labour, Newcastle-under-Lyme*)

Simon Hart MP (*Conservative, Carmarthen West and South Pembrokeshire*)

Julian Knight MP (*Conservative, Solihull*)

Ian C. Lucas MP (*Labour, Wrexham*)

Brendan O'Hara MP (*Scottish National Party, Argyll and Bute*)

Rebecca Pow MP (*Conservative, Taunton Deane*)

Jo Stevens MP (*Labour, Cardiff Central*)

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 Chloe Challender (Clerk), Mems Ayinla (Second Clerk), Mubeen Bhutta (Second Clerk), Lois Jeary (Committee Specialist), Andy Boyd (Senior Committee Assistant), Keely Bishop (Committee Assistant), Lucy Dargahi (Media Officer) and Anne Peacock (Senior 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 @CommonsCMS.

Seventh Special Report

The Digital, Culture, Media and Sport Committee published its Eighth Report of Session 2017–19, Disinformation and ' fake news': Final Report (HC 1791) on 18 February 2019. The Government's response was received on 3 May 2019 and is appended to this report.

Appendix: Government Response

Introduction

The Government is grateful for the Committee's comprehensive inquiry into 'fake news' and disinformation. We agree with the Committee that disinformation threatens the intrinsic values and principles of the UK, and it is right that Government addresses this issue as a matter of priority. This detailed and considered inquiry has made a valuable contribution to the public debate on disinformation and a range of other related issues. The evidence, conclusions and recommendations in the Committee's interim and final reports have enabled the Government to draw on a wide stakeholder and evidence base in considering how best to tackle these issues, including in preparing the Online Harms White Paper. Following the conclusion of the Committee's inquiry, the Government welcomes Parliament's continued engagement on this important issue. We hope the new Sub-Committee on disinformation expertise will continue to be valuable as we refine and implement our measures to tackle disinformation in all its forms.

This response builds on the Government's response to the Committee's Interim Report, which was published on 23 October 2018. This response should also be read in conjunction with the Online Harms White Paper, published on 8 April 2019. Many of the Committee's recommendations are in line with and addressed in the White Paper. The Secretary of State for Digital, Culture, Media and Sport wrote a letter sent to the Committee to outline how the White Paper tackled the Committee's recommendations on 8 April 2019.

The Government agrees with the Committee that the current self regulatory approach online is insufficient and that there is an urgent need to establish independent regulation. That is why the White Paper commits to introducing a new regulatory approach as well as proposals for new legislative measures to ensure that companies remove illegal content; adopt new safety technologies; better manage and monitor harmful content; and support safety education and awareness for all users. We have also initiated a major public consultation on the detail of how future regulation of online harms will be delivered in the UK.

The White Paper also clearly sets out the Government's concerns about disinformation and proposals to tackle this issue. Disinformation is one of the harms in scope of the new regulatory framework, and the White Paper makes clear our expectations for companies to take action to limit the spread of disinformation on their platforms. The Government also agrees with the Committee that education and awareness are key to long-term success in building society's resilience to disinformation as well as other online harms. We are confident that the White Paper's educational measures and initiatives will help to equip all citizens with the skills they need to assess critically the content they consume online.

Furthermore, the White Paper outlines the Government's concerns about wider online manipulation. We are confident that the measures outlined in the White Paper will tackle disinformation effectively in a way that protects freedom of expression and promotes innovation. However, we recognise that disinformation and other tactics to manipulate are complex and will continue to evolve with technology. The Government's work to tackle disinformation and online manipulation does not stop with the publication of the White Paper. We will continue to engage with stakeholders in industry, civil society and Parliament to build our understanding of emerging issues and how we, as a society, should respond to them.

A number of the Committee's recommendations relate to protecting our elections and other democratic processes. Government agrees that protecting these processes, be that from electoral fraud or foreign interference, is a key priority. The Online Harms White Paper outlines proposals for improving the safety of the whole information environment, which will support this objective. We also urge the Committee to consider the recent Government response to the 'Protecting the Debate: Intimidation, Influence and Information' consultation.

The need to tackle disinformation has emerged as a theme in a number of other independent and Government reviews. We encourage the Committee to review the 'Unlocking digital competition, Report of the Digital Competition Expert Panel' published 13 March 2019, which carefully considers competition in digital markets. As this response sets out, we will also be formally responding to the recommendations in Dame Cairncross' recent report on the sustainability of the press.

Recommendation 12 is addressed to the Information Commissioner's Office (ICO) and Recommendation 40 concerns the work of the National Crime Agency (NCA). Recommendations 15 and 47 are addressed wholly or in part to the Competition and Markets Authority (CMA), Ofcom, the ICO, the Electoral Commission, and the Advertising Standards Agency (ASA). As set out in our response to the Committee's Interim Report, it is not appropriate for the Government to comment on or respond on behalf of independent bodies or investigations. As such, this response focuses only on those recommendations addressed to Government.

Recommendation 1

We repeat the recommendation from our Interim Report that a new category of tech company is formulated, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'. This approach would see the tech companies assume legal liability for content identified as harmful after it has been posted by users. We ask the Government to consider this new category of tech company in its forthcoming White Paper. (Paragraph 14)

Government response:

The approach set out in the White Paper does not include creating a new category of tech company. We carefully considered how changes based on the existing content liability framework could place greater responsibility on companies and concluded that this is not the most effective mechanism for driving change. Instead, the White Paper sets out how

a wide range of companies will be expected to deal with both illegal and harmful, but legal, content on their platforms, through a statutory Duty of Care and Codes of Practice, enforced by an independent regulator.

The White Paper explains that following a review, the Government concluded that a regulatory model which focused solely on liability for the presence of illegal content would not incentivise the sort of systemic improvements in governance and risk management processes that are necessary. The Duty of Care model will incentivise such systemic improvements, and will also increase online service providers' responsibilities.

The White Paper proposes that this regulatory framework will apply to all companies that allow users to share or discover content or interact with each other online. This will ensure legislation remains fit for purpose and future proofed, as the nature and form of tech companies change over time. The White Paper includes a consultation question on whether this scope provides a suitable basis for an effective and proportionate approach.

In addition, the White Paper sets out the range of harms that will fall within the scope of new regulation This list is, by design, not exhaustive nor fixed to ensure swift regulatory action is possible to address new forms of online harm, new technologies, content and new online activities.

This approach will see companies required to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms, as well as to take appropriate and proportionate action when issues arise. The new regulatory regime will also ensure effective oversight of the take-down of illegal content and will introduce specific monitoring requirements for tightly defined categories of illegal content.

Recommendation 3

Our Interim Report recommended that clear legal liabilities should be established for tech companies to act against harmful or illegal content on their sites. There is now an urgent need to establish independent regulation. We believe that a compulsory Code of Ethics should be established, overseen by an independent regulator, setting out what constitutes harmful content. The independent regulator would have statutory powers to monitor relevant tech companies; this would create a regulatory system for online content that is as effective as that for offline content industries. (Paragraph 37)

Government response:

The Government strongly agrees with the need to establish independent regulation. The White Paper sets out a regulatory framework, based around a new statutory Duty of Care for companies to keep their users safe, with an independent regulator to enforce this.

The independent regulator will implement, oversee and enforce the new regulatory framework. We also expect the regulator to work with industry to encourage the development of technologies that aid compliance, and to facilitate cross-sector collaboration and sharing of expertise.

The White Paper also sets out how the regulator will produce Codes of Practice covering the key online harms that are set out in the White Paper. The Codes will set out what

companies in scope will need to do to meet their new legal responsibilities. We agree with the Committee that enforcement powers will be critical and the White Paper provides examples of the enforcement powers the regulator could have. It will be for the regulator to assess whether companies have fulfilled their Duty of Care to users by following the relevant Codes of Practice. If companies want to fulfil these duties in a manner not set out in the Codes, they will have to explain and justify to the regulator how their alternative approach will effectively tackle harmful content on their services.

Recommendation 4

As we said in our Interim Report, such a Code of Ethics should be similar to the Broadcasting Code issued by Ofcom - which is based on the guidelines established in section 319 of the 2003 Communications Act. The Code of Ethics should be developed by technical experts and overseen by the independent regulator, in order to set down in writing what is and is not acceptable on social media. This should include harmful and illegal content that has been referred to the companies for removal by their users, or that should have been easy for tech companies themselves to identify. (Paragraph 38)

Government response:

The White Paper sets out that the regulator will issue Codes of Practice setting out the steps companies should take to fulfil their Duty of Care. The White Paper sets out high-level expectations which the Government expects the regulator to include within the Codes. These include areas such as ensuring reporting processes and processes for moderating content and activity are transparent and effective, and ensuring that harmful content is dealt with promptly. The regulator will ultimately decide on the content of the Codes but will develop them with stakeholders in an open and transparent way.

Recommendation 5

The process should establish clear, legal liability for tech companies to act against agreed harmful and illegal content on their platform and such companies should have relevant systems in place to highlight and remove 'types of harm' and to ensure that cyber security structures are in place. If tech companies (including technical engineers involved in creating the software for the companies) are found to have failed to meet their obligations under such a Code, and not acted against the distribution of harmful and illegal content, the independent regulator should have the ability to launch legal proceedings against them, with the prospect of large fines being administered as the penalty for non-compliance with the Code. (Paragraph 39)

Government response:

Government agrees that sufficient enforcement powers will be critical to the success of the regulator. The White Paper sets out the Government's plans to introduce a statutory Duty of Care for an independent regulator to enforce. The Government is committed to ensuring that the regulator has sufficient powers to perform its duties effectively. The White Paper sets out in broad terms the core enforcement measures that the regulator will

have. The regulator will have powers to take action where breaches of the Duty of Care manifest, including the ability to levy substantial fines. We are confident that will ensure that all companies in scope of the regulatory framework fulfil their Duty of Care.

We are also consulting on additional powers that, in extreme cases, will hold senior management liable for major breaches of the Duty of Care and enable the regulator to require ISPs to block access to non-compliant websites or apps from within the UK.

The Government also expects the regulator to build on existing work that promotes design and adoption of systems for detecting and responding to illegal or harmful content, including the use of AI-based technology and trained moderators.

Recommendation 6

This same public body should have statutory powers to obtain any information from social media companies that are relevant to its inquiries. This could include the capability to check what data is being held on an individual user, if a user requests such information. This body should also have access to tech companies' security mechanisms and algorithms, to ensure they are operating responsibly. This public body should be accessible to the public and be able to take up complaints from members of the public about social media companies. We ask the Government to put forward these proposals in its forthcoming White Paper. (Paragraph 40)

Government response:

We agree with the Committee that social media companies have simply not provided sufficient access to their data to allow for the collection of robust information. It is right that the Government should intervene to establish clear standards. A key objective of the new regulatory framework will be to develop a culture of transparency, trust and accountability. Consistent standards of transparency will be a critical element of the new regulatory framework. Instrumental to this will be the regulator's information gathering powers, both to assess companies' compliance with the Duty of Care and to enable the regulator to require additional information, including about the operation of algorithms.

The White Paper proposes that the regulator is able to require companies to submit annual transparency reports and provide additional information to inform their oversight or enforcement activity and assess companies' compliance. The regulator will have the power to require additional information from companies to enable it to undertake thematic reviews of areas of concern, for example a review into the treatment of self-harm or suicide content. It should be emphasised that these processes will be consistent with data protection regulations.

The Government recognises the growing public concern about the risk that online harms pose to our citizens, especially children and the most vulnerable. We want to renew their confidence in the online world. The regulator will have responsibilities to engage with the public to promote education and awareness raising about online safety.

We do not envisage that the regulator will deal with individual complaints under the White Paper proposals. Under the regulatory framework, the user will get up to three tiers of consideration for their complaint under a company's T&Cs. There will be two

considerations by the company in question (i.e. a right to complain and the right to appeal a decision to the company), and once by either an industry-led scheme or body (Option 1) or by the regulator, via the super complaints route (Option 2). The third tier is being consulted on. We encourage the Committee to work with us throughout the consultation period.

Recommendation 7

We support the Recommendation from the ICO that inferred data should be as protected under the law as personal information. Protections of privacy law should be extended beyond personal information to include models used to make inferences about an individual. We recommend that the Government studies the way in which the protection of privacy law can be expanded to include models that are used to make inferences about individuals, in particular during political campaigning. This will ensure that inferences about individuals are treated as importantly as individuals' personal information. (Paragraph 48)

Government response:

The Data Protection Act 2018 and the GDPR introduced in May last year includes a robust framework protecting the information rights of individuals. The GDPR gives data subjects the tools to understand the way in which their data has been processed. Processing must be transparent, details of that processing must be provided to every data subject, whether or not the data was collected directly from them, and data subjects are entitled to a copy of the data held about them. Data controllers should not be able to hide behind complex algorithms.

The Government will continue to work closely with the Information Commissioner to make sure she has the powers she needs to equip her for complex investigations. Issues relating to inferred data will depend on the individual circumstances of the case and be considered in light of the relevant legislation. We will continue to work with the Commissioner to keep the data protection framework under review.

Recommendation 8

In our Interim Report, we recommended a levy should be placed on tech companies operating in the UK to support the enhanced work of the ICO. We reiterate this Recommendation. The Chancellor's decision, in his 2018 Budget, to impose a new 2% digital services tax on UK revenues of big technology companies from April 2020, shows that the Government is open to the idea of a levy on tech companies. The Government's response to our Interim Report implied that it would not be financially supporting the ICO any further, contrary to our Recommendation. We urge the Government to reassess this position. (Paragraph 51)

Government response:

The Government is committed to ensuring that the ICO is a world-class regulator, working effectively across the UK to safeguard the rights of individuals in relation to their data. As the ICO's sponsoring Department, DCMS has a specific responsibility to ensure adequate

ongoing funding for the ICO. We engage in regular dialogue with the Information Commissioner and her office about their current and future funding, including potential alternative sources of funding. We introduced new data protection charges in May of last year that have provided an estimated increase of £18 million to the ICO's income for 2018/19. These increased funds have enabled the ICO to develop its expertise and recruit an additional 200 staff to support their ongoing data protection work.

Recommendation 9

The new independent system and regulation that we recommend should be established must be adequately funded. We recommend that a levy is placed on tech companies operating in the UK to fund its work. (Paragraph 52)

Government response:

The Government strongly agrees that the independent regulator must have adequate funding. We are committed to ensuring the regulator has sufficient resources and the right expertise and capability to perform its role effectively. The White Paper includes a consultation question on whether the regulator should be a new or existing body. The regulator will be funded by industry in the medium term, and the Government is considering suitable funding models, including a levy, to put the regulator on a sustainable footing.

A wide variety of organisations of all sizes, including start-ups and SMEs, will be in scope of the regulatory framework. This comprehensive approach is important for the efficacy of the new regulatory framework. To ensure a proportionate approach, the application of the regulatory requirements and the Duty of Care model will reflect the diversity of organisations in scope. We will recognise this in developing options for the funding model. We encourage the Committee to engage with the Government on this further during the consultation period.

Recommendation 14

In our Interim Report, we stated that the dominance of a handful of powerful tech companies has resulted in their behaving as if they were monopolies in their specific area, and that there are considerations around the data on which those services are based. Facebook, in particular, is unwilling to be accountable to regulators around the world. The Government should consider the impact of such monopolies on the political world and on democracy. (Paragraph 138)

Government response:

As noted within the DCMS Select Committee Interim Report, the Government recognises that digital services – particularly those that are free-to-use and funded by advertising – pose challenges to our existing competition frameworks.

In September 2018 the Chancellor commissioned an independent Digital Competition Expert Panel, chaired by Professor Jason Furman, to look at competition in the digital economy. The Panel's report was published on 13 March. Its pro-innovation

recommendations fit with the Government's wider strategy for an open and competitive economy, demonstrating that, as the UK leaves the EU, Government is doing the important long-term economic planning to benefit businesses and consumers. The Government will respond to Furman's specific recommendations later this year.

The Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) updated our data protection framework to make it fit for the digital age, in which an ever-increasing amount of data is being processed. The GDPR sits alongside the DPA; strengthening provisions to keep people's data safe and secure while making sure organisations who use it are doing so properly and for legitimate reasons. The ICO has powers to investigate organisations that do not comply with the new data protection regime and can issue fines if organisations fail to meet particular legal requirements.

Recommendation 15

The Competitions and Market Authority (CMA) should conduct a comprehensive audit of the operation of the advertising market on social media. The Committee made this Recommendation its Interim Report, and we are pleased that it has also been supported in the independent Cairncross Report commissioned by the Government and published in February 2019. Given the contents of the Six4Three documents that we have published, it should also investigate whether Facebook specifically has been involved in any anti-competitive practices and conduct a review of Facebook's business practices towards other developers, to decide whether Facebook is unfairly using its dominant market position in social media to decide which businesses should succeed or fail. We hope that the Government will include these considerations when it reviews the UK's competition powers in April 2019, as stated in the Government response to our Interim Report. Companies like Facebook should not be allowed to behave like 'digital gangsters' in the online world, considering themselves to be ahead of and beyond the law. (Paragraph 139)

Government response:

The Competition and Markets Authority (CMA) is responsible for the enforcement of competition policy and therefore decisions over investigations are a matter for them. However, we agree that such an audit is necessary, given similar recommendations from both the Cairncross and Furman reviews. The Secretary of State has written to the CMA encouraging them to undertake such a review.

As noted in our response to Recommendation 14, we recognise the challenges digital services can pose to competition frameworks, and the Government will respond to the Furman Review's recommendations later in the year.

Recommendation 20

We repeat the Recommendation from our Interim Report, that the Government should look at the ways in which the UK law should define digital campaigning, including having agreed definitions of what constitutes online political advertising, such as agreed types of words that continually arise in adverts that are not sponsored

by a specific political party. There also needs to be an acknowledgement of the role and power of unpaid campaigns and Facebook Groups that influence elections and referendums (both inside and outside the designated period). (Paragraph 210)

Government response:

The Government acknowledges the potential threat to democracy posed by disinformation. We have set out in the White Paper how personal data and online advertising structures can be misused to target people with deliberately false or misleading information; and the importance of, and expectations for, transparency. Government expects the new regulator's Code of Practice for disinformation to include guidance for organisations on improving the transparency of political advertising, helping to meet any requirements in electoral law. The Government also announced on 12 February that we would conduct a review into online advertising in the UK. This will assess the wider impact online advertising has on the economy and society.

In addition, the Cabinet Office has considered the responses to the public consultation 'Protecting the Debate: Intimidation, Influence and Information' which closed on 28 October 2018. The consultation included proposed changes to electoral law, including the inclusion of digital imprints on digital electoral material, the definition of electoral material and what forms of digital communications could be covered by electoral law. The Government has published its response to the consultation setting out how the Government intends to proceed on this issue.

Recommendation 21

Electoral law is not fit for purpose and needs to be changed to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, micro-targeted political campaigning. There needs to be: absolute transparency of online political campaigning, including clear, persistent banners on all paid-for political adverts and videos, indicating the source and the advertiser; a category introduced for digital spending on campaigns; and explicit rules surrounding designated campaigners' role and responsibilities. (Paragraph 211)

Government response:

The Government agrees that the digital age has encouraged changes in campaigning techniques, and that greater transparency would be beneficial. The Online Harms White Paper includes a number of steps we expect the new regulator to include in a Code of Practice for disinformation, proposing that responsibilities could be placed on companies in scope to implement measures to increase transparency of political advertising and ensure that their users can clearly distinguish advertisements from organic content. Furthermore, we will use the findings from the Centre for Data Ethics and Innovation (CDEI)'s first two projects looking at microtargeting and algorithmic bias to inform our approach to ensuring these practices are used legitimately online.

Candidates, political parties and non-party campaigners are currently required to have an imprint on any printed election material, to demonstrate that they have produced it. Extending this to include digital communications is essential for promoting fact-based

political debate and tackling disinformation online. The Government sought views on this in a public consultation on 'Protecting the Debate', which was launched last year by the Prime Minister. The Government's recently published response reveals that the majority of people who engaged were in favour of this extension.

The Cabinet Office will work closely with the Department for Digital, Culture, Media and Sport and other stakeholders to confirm how such regulations will be put into practice and which third party organisations it would extend to. The Government will bring forward the technical proposal for this regime later on this year.

In addition, the Government is currently working with the Electoral Commission on statutory Codes of Practice for registered parties and candidates on electoral expenses. This provides clarity on digital campaigning election expenses. The Codes should come into force for the next major elections scheduled to take place in 2021 and 2022. The Government will also continue to work with the Electoral Commission on guidance for upcoming elections to ensure there is clarity on the processes and procedures for parties, candidates and campaigners.

Recommendation 22

We would expect that the Cabinet Office's consultation will result in the Government concluding that paid-for political advertising should be publicly accessible, clear and easily recognisable. Recipients should be able to identify the source, who uploaded it, who sponsored it, and its country of origin. (Paragraph 212)

Government response:

The Government has announced that candidates, political parties and non-party campaigners will be required to brand or 'imprint' their digital election materials, so the public is clear who is targeting them. This is a crucial step for helping prevent misleading political advertising online. The Cabinet Office will work closely with the Department for Digital, Culture, Media and Sport and other stakeholders to confirm how such regulations will be put into practice and which third party organisations it would extend to. The Government will bring forward the technical proposal for this regime later on this year. Furthermore, we recognise that political campaigning happens year-round, and we will consider how these proposals can be applied outside of electoral periods.

The Online Harms White Paper acknowledges how personal data and online advertising structures can be misused to target people with deliberately false or misleading information, and the importance of transparency. The White Paper proposes that the Code of Practice for disinformation, which will ultimately be determined by the independent regulator, could include responsibilities for companies in scope to implement measures to increase transparency of political advertising.

Recommendation 23

The Government should carry out a comprehensive review of the current rules and regulations surrounding political work during elections and referenda including:

increasing the length of the regulated period; defining what constitutes political campaigning; and reducing the time for spending returns to be sent to the Electoral Commission. (Paragraph 213)

Government response:

The Government will continue to work with the Electoral Commission and political parties to identify and implement any reforms and clarifications to the law, regulations and practices around campaigning. We are committed to ensuring that the law and regulations around campaigning are up-to-date with technological advances in campaign techniques.

This includes the Government's work with the Electoral Commission on statutory Codes of Practice for registered parties and candidates on electoral expenses. New Codes will provide clarity on digital campaigning election expenses. The Codes should come into force for the next major elections scheduled to take place in 2021 and 2022. The Government is carefully considering recent recommendations made by the Electoral Commission's report 'Digital campaigning: increasing transparency for voters', published in June 2018. Recommendations include amending the rules for reporting spending. The Government will also continue to work with the Electoral Commission on guidance for upcoming elections to ensure there is clarity on the processes and procedures for parties, candidates and campaigners.

Recommendation 24

The Government should explore ways in which the Electoral Commission can be given more powers to carry out its work comprehensively, including the following measures:

- **the legal right to compel organisations that they do not currently regulate, including social media companies, to provide information relevant to their inquiries;**
- **The Electoral Commission's current maximum fine limit of £20,000 should be increased, and changed to a fine based on a fixed percentage of turnover, in line with powers already conferred on other statutory regulators;**
- **The ability for the Electoral Commission to petition against an election due to illegal actions, which currently can only be brought by an individual;**
- **The ability for the Electoral Commission to intervene or stop someone acting illegally in a campaign if they live outside the UK. (Paragraph 214)**

Government response:

The Government is considering the Electoral Commission's recommendations in its June 2018 report, 'Digital campaigning: Increasing transparency for voters', plus other reports that propose increasing the Electoral Commission's powers. The Government recognise the importance of these issues and are not complacent, however it is critical we ensure that any regulation is proportionate. Political parties and other groups who seek to engage democratically are often voluntary organisations, not large corporations. There is a risk

that disproportionate regulation could discourage volunteering and undermine local democracy. These are all issues that the Government is considering and we will respond in due course. The Electoral Commission has civil sanctioning powers that apply to referendums and elections. More serious criminal matters can and are referred to the police, and then considered by a court of law. The courts already have the power to levy unlimited fines.

Recommendation 25

Political advertising items should be publicly accessible in a searchable repository—who is paying for the ads, which organisations are sponsoring the ad, who is being targeted by the ads—so that members of the public can understand the behaviour of individual advertisers. It should be run independently of the advertising industry and of political parties. This Recommendation builds on paragraph 144 of our Interim Report. (Paragraph 215)

Government response:

It is important that users have information on the advertising they see online and have the option to learn more. Several social media companies have introduced tools and policies to increase transparency of political advertising on their platforms, including repositories or 'ad libraries'. The Government welcomes these voluntary steps. However, we recognise that these measures are far from perfect, and agree with the Committee that more needs to be done to increase transparency. As highlighted previously in the responses to Recommendations 20, 21 and 22, the White Paper proposes that the Code of Practice for disinformation include expectations for companies to improve the overall transparency of political advertising on their platforms. This includes ensuring that their users can clearly distinguish advertisements from organic content and publishing data that supports research into the nature of online disinformation activity.

In addition, the online advertising review, announced on 12 February will consider additional measures the Government could take to promote better understanding of the advertising ecosystem.

Recommendation 26

We agree with the ICO's proposal that a Code of Practice, which highlights the use of personal information in political campaigning and applying to all data controllers who process personal data for the purpose of political campaigning, should be underpinned by primary legislation. We urge the Government to act on the ICO's Recommendation and bring forward primary legislation to place these Codes of Practice into statute. (Paragraph 216)

Government response:

The Information Commissioner's Office (ICO) intend to issue clearer guidance for political parties, regardless of whether it is later put on a statutory footing. As an independent regulator, they have powers in the Data Protection Act 2018 to introduce non-statutory codes of practice. In addition, the Government is considering the feasibility of having a

Statutory Code of Practice for political parties, whilst respecting the intent of Parliament to provide a lawful basis in the Act for data processing activities that are necessary to support or promote democratic engagement.

Recommendation 27

We support the ICO's Recommendation that all political parties should work with the ICO, the Cabinet Office and the Electoral Commission, to identify and implement a cross-party solution to improve transparency over the use of commonly-held data. This would be a practical solution to ensure that the use of data during elections and referenda is treated lawfully. We hope that the Government will work towards making this collaboration happen. We hope that the Government will address all of these issues when it responds to its consultation, "Protecting the Debate: Intimidation, Influence, and Information" and to the Electoral Commission's report, "Digital Campaigning: increasing transparency for voters". A crucial aspect of political advertising and influence is that of foreign interference in elections, which we hope it will also strongly address. (Paragraph 217)

Government response:

Political parties are still required to respect the overarching data protection principles, including requirements to process people's data fairly, lawfully and transparently. The Data Protection Act 2018 does not exempt them from these principles. We will continue to work with the ICO and other regulators such as the Electoral Commission to make sure that roles and responsibilities are clear.

The Government are reviewing existing legislation on access to electoral registers to ensure elected representatives and political parties can continue to use the electoral register for the purposes of democratic engagement. This reflects the commitment by Ministers during the Data Protection Bill. We have also engaged with political parties through the Parliamentary Parties Panel.

Recommendation 29

Tech companies must address the issue of shell companies and other professional attempts to hide identity in advert purchasing, especially around political advertising—both within and outside campaigning periods. There should be full disclosure of the targeting used as part of advertising transparency. The Government should explore ways of regulating the use of external targeting on social media platforms, such as Facebook's Custom Audiences. (Paragraph 223)

Government response:

The DCMS Secretary of State has asked the Chair of the Centre for Data Ethics and Innovation (CDEI) to investigate the advances in targeting and profiling practices and consider what steps can be taken to ensure they are understood and trusted by the public, while best supporting business. This review will play an important role in ensuring transparency and fairness in the practice of external targeting. The CDEI will publish

an interim progress update on this project this summer, followed by a final report in December 2019. The CDEI's recommendations will also feed into the Government's review of online advertising regulation.

As also stated above, the Government is encouraging action to increase transparency of political advertising. This is reflected in the steps we expect the new regulator to include in Code of Practice for disinformation outlined in the White Paper, which proposes that duties be placed on companies in scope to take steps to increase transparency of political advertising on their platforms and help their users distinguish between paid-for and organic content.

Recommendation 32

We support the Electoral Commission in its request that the Government extend the transparency rules around donations made to political parties in Northern Ireland from 2014. This period of time would cover two UK general elections, two Northern Ireland Assembly elections, the Scottish independence referendum, the EU referendum, and EU and local government elections. We urge the Government to make this change in the law as soon as is practicable to ensure full transparency over these elections and referendums. (Paragraph 234)

Government response:

The Transparency of Donations and Loans etc. (Northern Ireland Political Parties) Order 2018 introduced transparency from July 2017. This was the result of a consultation process with the Northern Ireland political parties, which provided a broad consensus in favour of transparency for future donations and loans. The Government intends to undertake an operational review of the broader framework for donations and loans in Northern Ireland in due course. This will consider if there is a case for further reform.

Recommendation 33

We welcome Dame Frances Cairncross's report on safeguarding the future of journalism, and the establishment of a code of conduct to rebalance the relationship between news providers and social media platforms. In particular, we welcome the Recommendation that online digital newspapers and magazines should be zero rated for VAT, as is the case for printed versions. This would remove the false incentive for news companies against developing more paid-for digital services. We support the Recommendation that chimes with our own on investigating online advertising, in particular focussing on the major search and social media companies, by the Competition and Markets Authority. (Paragraph 236)

Government response:

High quality news and journalism is vital to healthy social and democratic engagement. The Government commissioned Dame Frances Cairncross to conduct her independent report into the sustainability of high quality journalism in March 2018 and welcomed her detailed and considered report in February 2019. The Government is now considering her recommendations and will look to take action where appropriate.

The Secretary of State has already written to the CMA in support of Dame Frances' Recommendation that it undertakes a market review of digital advertising - it is right that policy-makers and regulators have an accurate understanding of how the market operates and check that it is enabling fair competition. A CMA review is the best means of achieving that. On zero-rating VAT for digital news publications, the Government keeps all taxes under review. Any decision to amend the UK tax regime is a matter for the Chancellor of the Exchequer as part of the annual fiscal cycle.

Dame Frances' proposal for new codes of conduct between publishers and the online platforms that distribute their content deserves the Government's full consideration. We will examine it closely along with considering the forthcoming report into digital competition in the UK by the Expert Panel chaired by Jason Furman.

We will continue to engage with press publishers, online platforms, regulators, academics, the public and parliamentarians, as we consider the way forward. We will set out our response later this year.

Recommendation 34

In common with other countries, the UK is clearly vulnerable to covert digital influence campaigns and the Government should be conducting analysis to understand the extent of the targeting of voters, by foreign players, during past elections. We ask the Government whether current legislation to protect the electoral process from malign influence is sufficient. Legislation should be in line with the latest technological developments, and should be explicit on the illegal influencing of the democratic process by foreign players. We urge the Government to look into this issue and to respond in its White Paper. (Paragraph 249)

Government response:

The Government is not being complacent about this issue and is committed to ensuring our democratic processes remain secure. The Government will continue to monitor hostile state activity. As highlighted above, the Online Harms White Paper sets out the steps we expect the new regulator to establish in a disinformation Code of Practice, which includes the requirement for service providers to improve the overall transparency of political advertising and publish data that supports research into the nature of online disinformation activity. We will take further steps where proportionate, and in line with our commitment to support freedom of speech and the GDPR, to detect, disrupt and deter hostile state disinformation.

Recommendation 36

There is a general principle that, subject to certain spending limits, funding from abroad is not allowed in UK elections. However, as the Electoral Commission has made clear, the current rules do not explicitly ban overseas spending. We recommend that, at the earliest opportunity, the Government reviews the current rules on overseas involvement in our UK elections to ensure that foreign interference in UK elections,

in the form of donations, cannot happen. We also need to be clear that Facebook, and all platforms, have a responsibility to comply with the law and not to facilitate illegal activity. (Paragraph 267)

Government response:

The law is clear that donations over £500 must come from permissible donors. This includes, but is not limited to, individuals in a UK electoral register (including overseas voters), UK-registered companies and trade unions, and political parties registered in Great Britain and Northern Ireland. The Government has committed to strengthening the current provisions which protect UK politics from foreign influence. While there is no evidence that Britain's elections or referendums have been compromised by foreign interference, it is right that the Government safeguards against future risks.

The Government will take views of interested groups like the Parliamentary Parties Panel and the Electoral Commission to better understand the problems which Government could seek to address in the consultation, and to see what scope there is for broad cross-party agreement. The consultation may consider recommendations for increasing transparency on digital political advertising, including by third parties; closing loopholes on foreign spending in elections; preventing shell companies from sidestepping the current rules on political finance and on action to tackle foreign lobbying.

Recommendation 38

The Government should put pressure on social media companies to publicise any instances of disinformation. The Government needs to ensure that social media companies share information they have about foreign interference on their sites—including who has paid for political adverts, who has seen the adverts, and who has clicked on the adverts—with the threat of financial liability if such information is not forthcoming. Security certificates, authenticating social media accounts, would ensure that a real person was behind the views expressed on the account. (Paragraph 272)

Government response:

It is vital that the social media companies are open and transparent about when foreign interference has taken place on their site and we strongly agree with the committee that this should be publicised where appropriate. The Government is encouraged by the efforts of several companies to make this information available. We have already seen many take steps to tackle the spread of disinformation and increase transparency on their platforms. Several have developed and implemented new systems to detect and remove fake accounts and coordinated inauthentic behaviour on their platforms. In addition, several of the major tech companies have produced transparency reports, which provide data on instances of such behaviour on their platforms, as well as the number of fake, spam or otherwise inauthentic accounts removed. We have also seen both Facebook and Twitter provide detailed accounts of coordinated inauthentic behaviour.

While these voluntary measures are welcome, we agree with the Committee that they do not go far enough. That is why the Online Harms White Paper sets out clearly the expectation for these companies to do more. This includes responsibilities for them to

increase the transparency of political advertising on their platforms; publish data that supports research into the nature of online disinformation activity; take action to eliminate and prevent accounts that misrepresent their owner's identity or location to spread disinformation; and make it clear to users when they are interacting with automated accounts. The White Paper also sets out potential enforcement powers for the regulator, including fines.

Recommendation 39

We repeat our call to the Government to make a statement about how many investigations are currently being carried out into Russian interference in UK politics. We further recommend that the Government launches an independent investigation into past elections - including the UK election of 2017, the UK Referendum of 2016, and the Scottish Referendum of 2014 - to explore what actually happened with regard to foreign influence, disinformation, funding, voter manipulation, and the sharing of data, so that appropriate changes to the law can be made and lessons can be learnt for future elections and referenda. (Paragraph 273)

Government response:

In the UK, the Government does not, and cannot, direct the police, Electoral Commission or the Security Service to investigate particular allegations. These organisations are operationally independent of Ministers and take a professional view of the necessity and proportionality of using their investigative powers. There is no evidence of successful foreign interference in UK democratic processes, this includes the 2016 referendum and the 2017 general election. However we are not complacent, and the Government has taken steps to ensure that there is a coordinated structure across all relevant UK authorities to defend against hostile foreign interference in British politics from any state.

Recommendation 41

We recommend that the Government looks into ways that PR and strategic communications companies are audited, possibly by an independent body, to ensure that their campaigns do not conflict with the UK national interest and security concerns and do not obstruct the imposition of legitimate sanctions, as is the case currently with the legal selling of passports. Barriers need to be put in place to ensure that such companies cannot work on both sensitive UK Government projects and with clients whose intention might be to undermine those interests. (Paragraph 298)

Government response:

The Government recognises the Committee's concern regarding PR and strategic communications companies. With regard to such companies working on UK Government projects, we have strict due diligence procedures in place to mitigate against conflicts of interest. During the formal procurement process conducted by the Crown Commercial Service (CCS), both the companies bidding for work and the government representatives evaluating them are required to declare any potential conflicts of interest. Bids are evaluated by the CCS, who accordingly determine whether company or evaluator can continue participating in the procurement process.

Recommendation 42

The transformation of Cambridge Analytica into Emerdata illustrates how easy it is for discredited companies to reinvent themselves and potentially use the same data and the same tactics to undermine governments, including in the UK. The industry needs cleaning up. As the SCL/Cambridge Analytica scandal shows, the sort of bad practices indulged in abroad or for foreign clients, risk making their way into UK politics. Currently the strategic communications industry is largely self-regulated. The UK Government should consider new regulations that curb bad behaviour in this industry.

Government response:

The Data Protection Act 2018 applies to all UK data controllers and non-UK data controllers processing the data of UK citizens for the purposes of providing goods and services or monitoring behaviour. As the Information Commissioner's report highlights, companies like Cambridge Analytica are as equally bound by these laws as any other data controller, and as such, the law explicitly prevents them from misusing personal data.

Under Section 198 of the Data Protection Act, criminal proceedings can be brought against a director, or person in or acting in a similar position, as well as the body corporate where it is proved that offences in the Act have occurred with the consent, connivance, or negligence of that person. The ICO would also be able to take enforcement action against those no longer in senior positions (for example through resignation), as long as they were a director at the relevant time. Criminal proceedings can be brought against such individuals even where the company they worked for has been dissolved or reinvented.

Recommendation 43

There needs to be transparency in these strategic communications companies, with a public record of all campaigns that they work on, both at home and abroad. They need to be held accountable for breaking laws during campaigns anywhere in the world or working for financially non-transparent campaigns. We recommend that the Government addresses this issue, when it responds to its consultation, 'Protecting the Debate: Intimidation, Influence and Information'.

Government response:

We thank the Committee for highlighting this issue and we will consider their recommendation carefully. This recommendation was out of scope of the 'Protecting the Debate: Intimidation, Influence and Information' consultation. However, as highlighted, the Government is committed to increasing transparency online. That is why the steps we expect the new regulator to establish in the Code of Practice for disinformation includes the requirement for companies in scope to improve the transparency of political advertising.

Following the publication of the Cairncross review, we have also announced a government-led review that will seek to assess the impact of the online advertising sector on both

society and the economy. It will consider the extent to which the current regulatory regime is equipped to tackle the challenges posed by rapid technological developments seen in online advertising.

Recommendation 44

We recommend that the Government revisits the UK Bribery Act, to gauge whether the legislation is enough of a regulatory brake on bad behaviour abroad. We also look to the Government to explore the feasibility of adopting a UK version of the US Foreign Agents and Registration Act (FARA), which requires "persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationships with the foreign principal, as well as activities, receipts and disbursements in support of those activities". (Paragraph 301)

Government response:

The Bribery Act 2010 has been subject to full post-legislative review very recently by a House of Lords Select Committee. The Bribery Act 2010 Committee were appointed on 9 May 2018. The Committee took oral and written evidence from Government, the prosecution agencies, private industry and legal experts in the field between July and December 2018. The Committee is expected to publish its findings in a final report at the end of March 2019. The Government will regard the Committee's findings with interest and will issue its official response in due course. All written and oral evidence given during the process of the review is also available on the Committee's House of Lords website at the following link:

- https://www.parliament.uk/business/committees/committees-a-z/lords-select/bribery-act-2010/timeline/

The Home Office is currently leading a review of existing Counter-Hostile State Activity (C-HSA) legislation in the UK, to establish whether further primary legislation is required to strengthen our response to all forms of HSA. This includes consideration of the merits of introducing some form of foreign agent registration transparency scheme similar to those adopted by the US and Australia.

Recommendation 46

As we wrote in our Interim Report, digital literacy should be a fourth pillar of education, alongside reading, writing and maths. In its response, the Government did not comment on our Recommendation of a social media company levy, to be used, in part, to finance a comprehensive educational framework—developed by charities, NGOs, and the regulators themselves—and based online. Such a framework would inform people of the implications of sharing their data willingly, their rights over their data, and ways in which they can constructively engage and interact with social media sites. People need to be resilient about their relationship with such sites, particularly around what they read and what they write. We reiterate this Recommendation to the Government, and look forward to its response. (Paragraph 312)

Government response:

The Government agrees with the Committee that digital literacy is key to long-term success in building our society's resilience to disinformation and other online harms. The White Paper sets out both existing and proposed educational measures and initiatives to boost digital literacy.

As we set out in our response to the Committee's Interim Report, digital literacy is already taught across the national school curriculum. This includes the computing curriculum, which teaches pupils about e-safety as well as the citizenship curriculum, which teaches pupils media literacy and explores freedom of speech and the role and responsibility of the media in informing and shaping public opinion. The White Paper highlights this and provides more detail on the subjects of Relationships Education, Relationships and Sex Education, and Health Education. We are making Relationships Education compulsory for all primary pupils, Relationships and Sex Education (RSE) compulsory for secondary pupils and Health Education compulsory for all pupils in all primary and secondary state-funded schools. These subjects will teach pupils, among other things, how to consider information critically; how people represent themselves online; how data is gathered, shared and used; the rules and principles for keeping safe online; and how to recognise risks, harmful content and contact, and how to report them. This will complement what is already taught currently in maintained schools through the national curriculum for computing.

In the White Paper, we also recognise the work happening outside of Government to promote media and digital literacy. Several organisations in the tech and media industries as well as civil society have developed news literacy initiatives and resources to help school children recognise disinformation. While we welcome these initiatives, it is clear that more needs to be done to support the digital and media literacy needs of adults. We also recognise the need for improved coordination of activity. To address this, as the White Paper sets out, Ofcom are working with a number of partners to map existing media literacy initiatives. This work will help identify gaps and opportunities.

In addition, the White Paper announces our intention to develop an online media literacy strategy. To ensure its objectives are well informed by evidence and take account of existing work, we will consult widely, possibly through a new taskforce. Working with a range of partners, the first step will be a comprehensive mapping exercise to assess existing provision and identify what additional action is needed to make progress against key objectives, which may include building resilience to disinformation; ensuring people with disabilities are not excluded from digital literacy education and support; and equipping people to recognise and deal with a range of deceptive and manipulative behaviours online, including catfishing, grooming, extremism.

Furthermore, the Government wants to give the public confidence in information so they are equipped to make their own decisions about the issues that matter. To support this, as set out in the White Paper, we are developing a counter disinformation communications campaign which will support the public by providing them with the skills they need in order to recognise and respond to disinformation; showing people how it can affect them and what they can do about it.

As highlighted in our response to Recommendation 9, the White Paper announces that we are considering a levy on tech companies to fund the 'new' regulator. This levy will indirectly fund digital literacy initiatives, as the regulator will have broader responsibilities to promote education and awareness raising about online safety, and to promote the development and adoption of safety technologies to tackle online harms, including disinformation. The White Paper also outlines the Government's expectation for companies to fund and support preventative education and awareness-raising activity for users of their platforms.

The Cairncross Report (published on 12 February 2019) proposed that a 'news quality obligation' be imposed upon social media companies, with regulatory oversight. That would require these companies to improve how their users understand the origin of an article of news and the trustworthiness of its source. Dame Frances recognises that social media companies are already starting to accept responsibility in this regard. This proposal deserves the Government's full consideration, and we will examine how it can inform our approach, including as part of the work set out in the White Paper.

Recommendation 47

The public need to know more about their ability to report digital campaigning that they think is misleading and or unlawful. Ofcom, the ASA, the ICO and the Electoral Commission need to raise their profiles so that people know about their services and roles. The Government should take a leading role in coordinating this crucial service for the public. The Government must provide clarity for members of the public about their rights with regards to social media companies. (Paragraph 313)

Government response:

The Government believes that accessible reporting options and features on social media platforms are important for empowering the public to flag the potentially harmful content they encounter online. Having effective reporting processes will be an integral part of fulfilling the new Duty of Care and will be covered in the Codes of Practice issued by the independent regulator. Furthermore, the Safety by Design framework proposed in the White Paper will include principles around user reporting, so that this crucial feature is built into new products and platforms as standard.

As highlighted in our response to Recommendation 25, the White Paper also notes that the disinformation Code of Practice, created by the regulator, should include the requirement for having clear reporting options for users to flag content and accounts they believe to be false or misleading.

The Government encourages Ofcom, the ASA, ICO and the Electoral Commission to continue to consider how best to raise their profile among the public, how to inform the public of their regulatory roles, and educate on rights both off and online.

Recommendation 48

Ofcom, the ICO, the Electoral Commission and the Advertising Standards Authority have all written separately about their role in promoting digital literacy. We recommend that the Government ensures that the four main regulators produce a

more united strategy in relation to digital literacy. Included in this united approach should be a public discussion on how we, as individuals, are happy for our data to be used and shared. People need to know how their data is being used (building on Recommendations we set out in Chapter Two of this Final Report). Users need to know how to set the boundaries that they want to, and how those boundaries should be set, with regard to their personal data. Included in this debate should be arguments around whether users want an agreed basic expectation of privacy, in a similar vein to a basic level of hygiene. Users could have the ability of opting out of such minimum thresholds, if they chose. (Paragraph 316)

Government response:

As stated above in response to Recommendation 46, the Government agrees with the Committee on the importance of digital and media literacy in helping people - both children and adults - critically assess information and protect themselves online. The White Paper sets out plans to develop an online media literacy strategy through broad consultation with a wide range of stakeholders (including tech companies, regulators, libraries, civil society and academics) to map out and assess work currently underway to build media and digital literacy, and also identify opportunities for further action. This will be part of the Government's wider efforts to coordinate work in this area, complemented by Ofcom's work with a number of partners to map existing media literacy initiatives. In addition, Ofcom have also committed to conducting further research around digital literacy levels in the UK to build understanding of existing provision and possible gaps. The White Paper also announces that the independent regulator will have a role in promoting digital and media literacy.