House of Commons

Digital, Culture, Media and Sport Committee

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

Fifth Special Report of Session 2017–19

Ordered by the House of Commons to be printed 17 October 2018

HC 1630
Published on 23 October 2018
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*)

The following Members were also members of the Committee during the inquiry

Christian Matheson MP (*Labour, City of Chester*)

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), Mubeen Bhutta (Second Clerk), Josephine Willows (Senior Committee Specialist), Lois Jeary (Committee Specialist), Andy Boyd (Senior Committee Assistant), Keely Bishop (Committee Assistant), Sarah Potter (Attached Hansard Scholar), Anne Peacock (DCMS Committee media team member) and Lucy Dargahi (Media 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

1 Fifth Special Report

The Digital, Culture, Media and Sport Committee published its Fifth Report of Session 2017–19, *Disinformation and 'fake news': Interim Report* (HC 363) on 29 July 2018. The Government's response was received on 9 October 2018 and is appended to this report.

Appendix: Government Response

Introduction

The Government is grateful for the Committee's timely inquiry into disinformation or 'fake news' and for its valuable contribution to the debate on these topics. The Committee's ongoing inquiry is highlighting areas of concern to Government, Parliament and the public and we look forward to the final report in the autumn.

Recommendations 8 and 20 are addressed to Facebook. The Government regularly engages with Facebook and has made clear that social media companies need to take far more responsibility for illegal and harmful content on their platforms. Recommendation 24 is for the Competition and Markets Authority (CMA) to respond to. Recommendations 14, 33, 43, 44, and 50 concern investigations by the Information Commissioner's Office (ICO), Electoral Commission (EC) and National Crime Agency (NCA). It is not appropriate for Government to comment on independent bodies or ongoing investigations.

The Government is already undertaking work to address a range of online harms, including disinformation. Disinformation is not a new phenomenon, but the online environment has enabled it to increase dramatically in terms of quantity, reach and speed of transmission. Through the Digital Charter we want to make sure the Internet works for everyone – for citizens, businesses and society as a whole. Tackling disinformation is a key pillar of the Charter. We want to reduce the impact of disinformation on UK society and our national interests, in line with our democratic values.

In May this year, the Government response to the Internet Safety Strategy Green Paper announced our intention to publish a White Paper in Winter 2018/2019 as a precursor to bringing forward online safety legislation. The Online Harms White Paper will establish a coherent and Government-wide approach to a range of online harms including disinformation, through both legislative and non-legislative initiatives. It supports the Digital Charter's ambitions of making the UK the safest place in the world to be online, whilst also leading the world in innovation-friendly regulation that supports the growth of the tech sector. This work is being jointly led by the Department for Culture Media and Sport and the Home Office.

The Government's interim response to the recommendations is set out below, ahead of the Committee's final report.

Recommendation 1

The term 'fake news' is bandied around with no clear idea of what it means, or agreed definition. The term has taken on a variety of meanings, including a description of any statement that is not liked or agreed with by the reader. We recommend that the Government rejects the term 'fake news', and instead puts forward an agreed definition of the words 'misinformation' and 'disinformation'. With such a shared definition, and clear guidelines for companies, organisations, and the Government to follow, there will be a shared consistency of meaning across the platforms, which can be used as the basis of regulation and enforcement. (Paragraph 14)

Government response

We agree that 'fake news' is a poorly-defined and misleading term that conflates a variety of false information, from genuine error through to foreign interference in democratic processes. Over the past several months during its work on this issue the Government has sought to move away from 'fake news' and instead has sought to address 'disinformation' and wider online manipulation. In our work we have defined disinformation as the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain. 'Misinformation' refers to the inadvertent sharing of false information.

Recommendation 2

We recommend that the Government uses the rules given to Ofcom under the Communications Act 2003 to set and enforce content standards for television and radio broadcasters, including rules relating to accuracy and impartiality, as a basis for setting standards for online content. We look forward to hearing Ofcom's plans for greater regulation of social media this autumn. We plan to comment on these in our further Report. (Paragraph 15)

Government response

The Government is committed to maintaining a news environment, both online and offline, where accurate content can prevail and high-quality news online has a sustainable future. While mechanisms are in place to enforce accuracy and impartiality in the broadcast and press industries, we agree with the spirit of the recommendations that greater regulation is needed in the online space.

The Government is developing a range of regulatory and non-regulatory initiatives to improve transparency and accountability in the online environment where information is shared. We are committed to ensuring that freedom of expression in the UK is protected and enhanced online. This work cannot and should not be done by Government alone and we will continue to work in partnership with industry, the media and civil society institutions.

Where the public is at risk from harmful content online, the Government has already taken action, for example we are introducing new age verification rules to prevent children accessing pornographic material online.

Recommendation 3

The Government should support research into the methods by which misinformation and disinformation are created and spread across the Internet: a core part of this is fact-checking. We recommend that the Government initiate a working group of experts to create a credible annotation of standards, so that people can see, at a glance, the level of verification of a site. This would help people to decide on the level of importance that they put on those sites. (Paragraph 18)

Government response

The Government is currently undertaking a range of research projects to better understand the scale, scope and impact of disinformation campaigns in the UK. For example, in March 2018, DCMS and Demos jointly hosted a workshop with academics, media and representatives from the tech sector. This discussed potential uses of technology such as text analysis and machine learning to identify disinformation online. Since then, we have been engaging in a number of other research projects with leading academic and industry experts. As the Committee have highlighted through their comprehensive evidence gathering, there are already a variety of initiatives aiming to create an annotation of standards or set levels of verification. We will continue to work with industry, civil society, academic and international partners to conduct research and build a robust evidence base that informs any policy response.

In parallel to this work, the Government is building its own capabilities dedicated to the assessment and countering of disinformation. For example, the Defence, Science, and Technology Lab is also conducting research projects into disinformation and is working with industry, academia and international partners on the subject matter. UK expertise in this field is widely recognised, and the Government is working closely with international partners to share our skills and experiences.

Recommendation 6

The Data Protection Act 2018 gives greater protection to people's data than did its predecessor, the 1998 Data Protection Act, and follows the law set out in the GDPR. However, when the UK leaves the EU, social media companies will be able to process personal data of people in the UK from bases in the US, without any coverage of data protection law. We urge the Government to clarify this loophole in a White Paper this Autumn. (Paragraph 30)

Government response

The UK is a global leader in strong data protection standards. We are strongly committed to protecting the personal data of all citizens, as demonstrated by the passage of our new Data Protection Act 2018. The EU Withdrawal Act 2018 allows the Government to make secondary legislation to deal with any deficiencies that would arise on exit in retained EU law. We will bring forward proposals to do this in respect of retained data protection regulations in due course. In doing so, the Government will take into account the importance of protecting UK residents' rights abroad. Furthermore, achieving a deal

on data protection is one of the foundations that must underpin the UK-EU trading relationship. The UK is ready to begin preliminary discussions on an adequacy assessment straight away to provide the earliest possible reassurance that data flows can continue.

Recommendation 7

We welcome the increased powers that the Information Commissioner has been given as a result of the Data Protection Act 2018, and the ability to be able to look behind the curtain of tech companies, and to examine the data for themselves. However, to be a sheriff in the wild west of the Internet, which is how the Information Commissioner has described her office, the ICO needs to have the same if not more technical expert knowledge as those organisations under scrutiny. The ICO needs to attract and employ more technically-skilled engineers who not only can analyse current technologies, but have the capacity to predict future technologies. We acknowledge the fact that the Government has given the ICO pay flexibility to retain and recruit more expert staff, but it is uncertain whether pay flexibility will be enough to retain and attract the expertise that the ICO needs. We recommend that the White Paper explores the possibility of major investment in the ICO and the way in which that money should be raised. One possible route could be a levy on tech companies operating in the UK, to help pay for the expanded work of the ICO, in a similar vein to the way in which the banking sector pays for the upkeep of the Financial Conduct Authority. (Paragraph 36)

Government response

The ICO is the UK's independent authority for upholding information rights, which includes individuals' rights to data protection, found in the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

Government is committed to ensuring that the ICO is able to continue to function as a world class regulator, working effectively across the UK to safeguard the rights of individuals in relation to their data. To this end, as the report highlights, we have granted the ICO pay flexibility up to 2020/21 so it can review and update its pay and grading structure, to ensure that the organisation is in the best position to develop and retain effectively its existing resources and expertise.

We have also recently introduced new data protection charges, which will provide an increase of over £10 million per annum to the ICO's income. These increased funds will also enable the ICO to continue to develop the level of expertise available to it and, crucially, to recruit an additional 30% of their current headcount to support ongoing data protection work, including effective regulation of the digital and technology sector.

The Information Commissioner has said of our actions that she is "confident that this will allow me to prepare the ICO for its critical role under the new data protection regime ensuring that the UK has a strong and expert regulator in an area recognised for its importance to the digital economy and society as a whole."

Government will continue to work closely with the Commissioner and her office to ensure that the regulator has the appropriate resources and expertise to be able to deliver on their important and challenging remit. We welcome the efforts of the Committee to highlight the critical role the ICO plays in today's data driven society.

Recommendation 9

Electoral law in this country is not fit for purpose for the digital age, and needs to be amended to reflect new technologies. We support the Electoral Commission's suggestion that all electronic campaigning should have easily accessible digital imprint requirements, including information on the publishing organisation and who is legally responsible for the spending, so that it is obvious at a glance who has sponsored that campaigning material, thereby bringing all online advertisements and messages into line with physically published leaflets, circulars and advertisements. We note that a similar recommendation was made by the Committee on Standards in Public Life, and urge the Government to study the practicalities of giving the Electoral Commission this power in its White Paper. (Paragraph 45)

Government response

The Committee on Standards in Public Life's report on intimidation in public life, published in December 2017, recommended that the Government should consult on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners. The Government published an open consultation entitled 'Protecting the Debate: Intimidating, Influence and Information', on Sunday 29 July 2018. It seeks views on proposed changes to electoral law, including whether the Government should extend electoral law requirements for an imprint on campaigning materials to digital communications. Campaigners are increasingly using new forms of digital communication to reach voters, and it is important that the campaigning process remains transparent.

The consultation includes high level questions around the definition of electoral material, the timeframe for when the rules could apply and what forms of digital communications could be covered. The core thrust of these questions is to protect a healthy democracy and political debate, whilst also ensuring that there are adequate provisions to manage new techniques in digital campaigning, which could reduce the confidence of voters in the integrity of elections and referendums.

The consultation will close at midnight on 22 October 2018 and it can be found online at gov.uk.[1]

Recommendation 10

As well as having digital imprints, the Government should consider the feasibility of clear, persistent banners on all paid-for political adverts and videos, indicating the source and making it easy for users to identify what is in the adverts, and who the advertiser is. (Paragraph 46)

1 https://www.gov.uk/government/consultations/protecting-the-debate-intimidation-influence-and-information

Government response

The Government is awaiting the outcome of the 'Protecting the Debate: Intimidating, Influence and Information' consultation. Following this we will consider how imprints on online content could be implemented more widely.

We welcome recent moves by social media companies to improve transparency around advertising, including Facebook which plans to include information on advertisements stating who has paid for them by the summer of 2019. Government believes more could be done both to tackle the problem on individual large platforms, and to support other smaller companies. As part of the Digital Charter, we are working with regulators, platforms and advertising companies to ensure that the principles that govern advertising in traditional media also apply and are enforced online and we will consider further options to increase transparency.

Recommendation 11

The Electoral Commission's current maximum fine limit of £20,000 should be changed to a larger fine based on a fixed percentage of turnover, such as has been granted recently to the Information Commissioner's Office in the Data Protection Act 2018. Furthermore, the Electoral Commission should have the ability to refer matters to the Crown Prosecution Service, before their investigations have been completed. (Paragraph 47)

Government response

The Government is currently considering the Electoral Commission's report, 'Digital Campaigning: Increasing Transparency for Voters', which included a recommendation that its sanctioning powers be increased, as well as other recommendations relating to its investigatory and regulatory powers. When reflecting on the Commission's recommendations, we will also consider this suggestion that they be able to refer matters to the Crown Prosecution Service, before their investigations have been completed.

Recommendation 12

Electoral law needs to be updated to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, micro-targeted political campaigning, as well as the many digital subcategories covered by paid and organic campaigning. The Government must 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; definitions of what constitutes political campaigning; absolute transparency of online political campaigning; a category introduced for digital spending on campaigns; reducing the time for spending returns to be sent to the Electoral Commission (the current time for large political organisations is six months); and increasing the fine for not complying with the electoral law. (Paragraph 48)

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. This includes ensuring that the law and regulations around campaigning are up-to-date with technological advances in campaign techniques.

The Government will continue to strengthen our electoral law. Recognising the challenges faced by our democracy, we are committed to encouraging as many eligible electors to vote as possible, as well as ensuring that voting remains fair and secure. This includes ensuring that the law and regulations around campaigning keep pace with technological advances in campaign techniques. As stated in response to Recommendation 9, the Government published an open consultation entitled 'Protecting the Debate: Intimidating, Influence and Information', on Sunday 29 July 2018. In regards to campaigning, the consultation includes high level questions around what forms of digital communications could be covered, the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners and clarifying the electoral offence of undue influence. We will consider policy changes following the outcome of this consultation.

As stated in response to Recommendation 11, the Government will be carefully considering recent recommendations made by the Electoral Commission's report 'Digital campaigning: increasing transparency for voters', published in June 2018. Recommendations include increasing the Electoral Commission's ability to impose tougher sanctions, amending the rules for reporting spending and working with social media companies to improve their policies on campaign material.

It is worth noting that the new Centre for Data Ethics and Innovation is expected to look closely at issues around transparency and targeting. More details about the Centre's work are set out in the response to Recommendation 23.

Recommendation 13

The Government should consider giving the Electoral Commission the power to compel organisations that it does not specifically regulate, including tech companies and individuals, to provide information relevant to their inquiries, subject to due process. (Paragraph 49)

Government response

As set out in response to Recommendation 11, the Government is currently considering the Electoral Commission's report, 'Digital Campaigning: Increasing Transparency for Voters', which included recommendations relating to its investigatory and regulatory powers. The Government will respond to the Electoral Commission's report in due course and also consider this issue during its considerations. A copy of the Government's response will be made available to the House of Commons Digital, Culture, Media and Sport Committee.

Recommendation 17

We recommend 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'. We anticipate that the Government will put forward these proposals in its White Paper later this year and hope that sufficient time will be built in for our Committee to comment on new policies and possible legislation. (Paragraph 58)

Government response

The current regime governing intermediary liability is harmonised across the EU through the eCommerce Directive (ECD), which covers Information Society Services (ISS) defining them in the categories of 'mere conduit', 'cache' and 'host'. Social media companies fall under the 'host' category for content 'that consists of the storage of information provided by a recipient of the service', which provides them with limited liability for illegal content until they have 'actual knowledge' of the content and 'act expeditiously' to remove it.

As the Prime Minister announced in January 2018, we are looking at the legal liability that social media companies have for illegal and harmful content shared on their sites. This is an important issue and we look forward to engaging with important stakeholders such as the Committee, to hear their views and to inform our ideas as we develop proposals to take this forward. It is vital we approach this carefully, to ensure any decision is future proofed, does not damage unduly the UK's vibrant tech industry, and fulfils our manifesto commitment to make the UK the safest place in the world to be online.

Recommendation 18

We support the launch of the Government's Cairncross Review, which has been charged with studying the role of the digital advertising supply chain, and whether its model incentivises the proliferation of inaccurate or misleading news. We propose that this Report is taken into account as a submission to the Cairncross Review. We recommend that the possibility of the Advertising Standards Agency regulating digital advertising be considered as part of the Review. We ourselves plan to take evidence on this question this autumn, from the ASA themselves, and as part of wider discussions with DCMS and Ofcom. (Paragraph 59)

Government response

The Cairncross Review's terms of reference make specific reference to the operation of the digital advertising supply chain in the monetisation of online news, however, the Review is independent from Government, and any recommendations made will be those of the Chair, Dame Frances Cairncross. We welcome the Committee's proposal that the report be considered as part of the review's call for evidence, and encourage Dame Frances to take its evidence into account as she considers recommendations in this area. We will await the review's findings and recommendations before making specific policy decisions.

Recommendation 19

It is our recommendation that this process should establish clear legal liability for the tech companies to act against harmful and illegal content on their platforms. This should include both content that has been referred to them for takedown by their users, and other content that should have been easy for the tech companies to identify for themselves. In these cases, failure to act on behalf of the tech companies could leave them open to legal proceedings launched either by a public regulator, and/or by individuals or organisations who have suffered as a result of this content being freely disseminated on a social media platform. (Paragraph 60)

Government response

As stated in response to Recommendation 17, we are currently looking at the legal liability that social media companies have for the illegal content shared on their sites, as set by the ECD.

Beyond our membership of the EU, Government has made clear that social media companies need to take more responsibility for illegal and harmful content on their platforms. We will explore a broad range of legislative and non-legislative options and set out our plans as part of the White Paper.

Recommendation 21

Facebook and other social media companies should not be in a position of 'marking their own homework'. As part of its White Paper this Autumn, the Government needs to carry out proactive work to find practical solutions to issues surrounding transparency that will work for both users, the Government, and the tech companies. (Paragraph 65)

Government response

We believe that it is right for the Government to set out clear standards for social media platforms, and to hold them to account if they fail to live up to these.

In February, the Prime Minister announced that we would establish a new Annual Internet Safety Transparency Report, to provide UK-level data. Further details relating to this transparency report were set out in May, as part of the Government response to the Internet Safety Strategy Green Paper.

Ahead of publishing the forthcoming Online Harms White Paper, the Government is proactively working with stakeholders, including tech companies and civil society organisations who represent a wide spectrum of users, to refine our transparency reporting proposals.

We hope transparency reports will help users and Government understand the extent of online harms and how effectively companies are tackling breaches of their terms and conditions. The White Paper will set out our plans for forthcoming legislation. Potential areas where the Government will consider legislation include transparency reporting.

Recommendation 22

Facebook and other social media companies have a duty to publish and to follow transparent rules. The Defamation Act 2013 contains provisions stating that, if a user is defamed on social media, and the offending individual cannot be identified, the liability rests with the platform. We urge the Government to examine the effectiveness of these provisions, and to monitor tech companies to ensure they are complying with court orders in the UK and to provide details of the source of disputed content-including advertisements - to ensure that they are operating in accordance with the law, or any future industry Codes of Ethics or Conduct. Tech companies also have a responsibility to ensure full disclosure of the source of any political advertising they carry. (Paragraph 66)

Government response

Section 5 of the Defamation Act 2013 provides a defence for website operators against liability in damages in the event of their receiving a complaint about an allegedly defamatory posting on a site they are operating. To avail itself of the defence the operator must comply with the procedure set out in Section 5 and accompanying regulations (which, broadly speaking, is aimed at giving the claimant the information necessary to pursue the person responsible for the posting in the event that the latter is unwilling to remove the posting, or otherwise to secure removal of the posting). However, if the operator chooses not to avail itself of the defence it may still be able to rely on other defences, for example under Article 19 of the E-Commerce Regulations.

The Government will review the effectiveness of Section 5 and other provisions in the Act in due course in the context of post-legislative scrutiny. More generally, non-compliance with court orders requiring the removal of material or the identification of the source of disputed content may amount to contempt of court, and the Government considers that any issues which may arise in this area are best dealt with by the courts.

That said, we are considering a range of regulatory and non-regulatory options to ensure that platforms take more responsibility for the harm that takes place on their services.

With regard to advertising, a number of content service providers, including Facebook, have taken steps to increase transparency. We welcome these steps but will assess options to ensure greater transparency. As stated elsewhere in this response, the Government is currently consulting on whether to extend electoral law requirements for an imprint on campaigning materials to digital communications.

Recommendation 23

Just as the finances of companies are audited and scrutinised, the same type of auditing and scrutinising should be carried out on the non-financial aspects of technology companies, including their security mechanisms and algorithms, to ensure they are operating responsibly. The Government should provide the appropriate body with the power to audit these companies, including algorithmic auditing, and we reiterate the point that the ICO's powers should be substantially strengthened in these respects. (Paragraph 72)

Government response

The Government is committed to making sure the ICO has the necessary powers and resources to make sure personal data is handled properly and within the law.

Section 129 of the Data Protection Act 2018 permits the Commissioner to carry out consensual audits to establish whether a data controller or processor is complying with the data protection rules. In addition, under Article 35 of the GDPR, all organisations have to produce a data protection impact assessment before they conduct a processing activity that may pose a 'high risk' to the rights and freedoms of individuals. 'High risk' processing would include automated decision-making processes and processing involving the use of new technologies, or the novel application of existing technologies including artificial intelligence.

However, the Government recognises that as technological advancements are made, and the use of data and AI becomes more complex, our existing governance frameworks may need to be strengthened and updated. That is why we are setting up the Centre for Data Ethics and Innovation.

As set out in the recent consultation on the Centre[2], we expect it to look closely at issues around the use of algorithms, such as fairness, transparency, and targeting. In the autumn the Government will publish a response to the consultation, and the Centre's initial work programme will be confirmed.

Recommendation 26

The UK Government should consider establishing a digital Atlantic Charter as a new mechanism to reassure users that their digital rights are guaranteed. This innovation would demonstrate the UK's commitment to protecting and supporting users, and establish a formal basis for collaboration with the US on this issue. The Charter would be voluntary, but would be underpinned by a framework setting out clearly the respective legal obligations in signatory countries. This would help ensure alignment, if not in law, then in what users can expect in terms of liability and protections. (Paragraph 76)

Government response

The Government is already working closely with a range of of countries on digital rights issues, taking an active role in discussions at international fora and multilateral organisations such as the G20, G7, D7 and OECD as we seek to build a clear global consensus. For example, we are supporting the work of 'The Freedom Online Coalition', a grouping of 30 governments that have committed to work together to support Internet freedoms and protect fundamental human rights - free expression, association, assembly, and privacy online - around the world. We are keen to prioritise this multilateral approach.

The Digital Charter aims to make the Internet work for everyone – for citizens, businesses and society as a whole. Our starting point is that we should have the same rights and expect the same behaviour online as we do offline. As we work on the Digital Charter, we are committing to build an international coalition of like-minded countries to develop a joint approach.

2 https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation

Recommendation 28

The hate speech against the Rohingya—built up on Facebook, much of which is disseminated through fake accounts—and subsequent ethnic cleansing, has potentially resulted in the success of DfID's aid programmes being greatly reduced, based on the qualifications they set for success. The activity of Facebook undermines international aid to Burma, including the UK Government's work. Facebook is releasing a product that is dangerous to consumers and deeply unethical. We urge the Government to demonstrate how seriously it takes Facebook's apparent collusion in spreading disinformation in Burma, at the earliest opportunity. This is a further example of Facebook failing to take responsibility for the misuse of its platform. (Paragraph 83)

Government response

The Government continues to be deeply concerned by hate speech against minorities, including Muslims and Christians in Burma, and particularly the Rohingya in Rakhine State. We have raised our concerns about hate speech regularly with the Burmese Government.

The Department for International Development (DfID) works with the Foreign and Commonwealth Office and local partners in Burma to tackle hate speech and misinformation online. We are not aware of any direct impact on DfID's programmes in Burma caused by misinformation spread on social media.

There is evidence that false information and hate speech spread via social media, including on Facebook, have fuelled widespread violence in other parts of the world. We are concerned by these developments and have discussed this issue with Facebook. Government welcomes their action to remove accounts and ban individuals and organisations following publication of the UN's Myanmar fact-finding mission report. However the Government has made it clear to Facebook, and other social media companies, that they must do more to remove illegal and harmful content. The Online Harms White Paper will also set out a range of policies to tackle harmful content.

Recommendation 29

A professional global Code of Ethics should be developed by tech companies, in collaboration with this and other governments, academics, and interested parties, including the World Summit on Information Society, to set down in writing what is and what is not acceptable by users on social media, with possible liabilities for companies and for individuals working for those companies, including those technical engineers involved in creating the software for the companies. New products should be tested to ensure that products are fit-for-purpose and do not constitute dangers to the users, or to society. (Paragraph 89)

Government response

As stated in response to Recommendation 19, the leading social media companies are already taking significant steps to better protect their users from a number of illegal online harms through the development of technical tools and successful partnerships with charities. However, the Government also wants to see greater consistency across

platforms so that users understand what standards of behaviour are acceptable across the whole online ecosystem. For example, startups developing new products have told us they lack the capacity and expertise to build safety into their products from the very start, so we will work with industry bodies to develop a set of common 'safety by design' principles. The Government's social media code of practice, published in draft in May 2018, provides guidance to social media providers on appropriate reporting mechanisms and moderation processes to tackle abusive content. By setting out clear standards for industry, we will make sure there is improved support for users online, and that more companies are taking consistent action to tackle abuse.

Recommendation 30

The Code of Ethics should be the backbone of tech companies' work, and should be continually referred to when developing new technologies and algorithms. If companies fail to adhere to their own Code of Ethics, the UK Government should introduce regulation to make such ethical rules compulsory. (Paragraph 90)

Government response

The use of data and AI is giving rise to complex, fast moving and far reaching economic and ethical issues. We need to be able to respond quickly and effectively to these and other emerging issues. To do this we need a governance regime - a set of norms, rules and structures - that determines how data and AI can and should be used.

The Data Protection Act is a major step towards ensuring our laws are fit for the digital age. It introduces new rights and responsibilities that ensure greater accountability, transparency and control in the way data and AI are used and deployed. Significant regulatory steps have also been taken to strengthen the way data and AI are used within specific sectors or spheres of activity.

The new Centre for Data Ethics and Innovation will examine issues of targeting, fairness, transparency and liability around the use of algorithms and data-driven technologies. The Centre will set out measures needed to build trust and enable innovation in data-driven technologies, including through agreeing best practice around data use and identifying potential new regulations.

Recommendation 31

The dominance of a handful of powerful tech companies, such as Facebook, Twitter and Google, has resulted in their behaving as if they were monopolies in their specific area. While this portrayal of tech companies does not appreciate the benefits of a shared service, where people can communicate freely, there are considerations around the data on which those services are based, and how these companies are using the vast amount of data they hold on users. In its White Paper, the Government must set out why the issue of monopolies is different in the tech world, and the measures needed to protect users' data. (Paragraph 91)

Government response

With regard to the enforcement of competition policy, the Competition and Markets Authority (CMA) is the independent body which has been given powers by Parliament to make sure that competition works across the economy. Our competition tools are designed to be sufficiently flexible to tackle competition issues across the economy.

As the interim report states, digital services – particularly those that are free-to-use and funded by advertising – pose challenges to our existing competition frameworks. As set out in the Modernising Consumer Markets Green Paper, the Government is reviewing the UK's competition powers in a broad sense and will report by April 2019. One part of this review is in the context of digital markets, to make sure the powers are effective in responding to the new digital challenges. The review will also help ensure that the UK remains at the centre of the digital revolution and that digital markets work well for businesses and consumers alike.

We also launched an Expert Panel, chaired by Jason Furman, that will independently consider whether the UK's competition regime – and pro-competition policy more generally – remains robust to the challenges of the emerging digital economy. This will inform the competition law review.

The Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) came into force on 25 May. The new legislation updates our data protection framework making 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. The ICO can issue fines if organisations fail to meet particular legal requirements.

Recommendation 36

We recommend that the Government look at ways in which the UK law defines digital campaigning. This should include online adverts that use political terminology that are not sponsored by a specific political party. There should be a public register for political advertising, requiring all political advertising work to be listed for public display so that, even if work is not requiring regulation, it is accountable, clear, and transparent for all to see. There should be a ban on micro-targeted political advertising to lookalikes online, and a minimum limit for the number of voters sent individual political messages should be agreed, at a national level. (Paragraph 142)

Government response

As stated in response to Recommendation 9, the Government published an open consultation entitled 'Protecting the Debate: Intimidating, Influence and Information', on Sunday 29 July 2018, which explores how electoral material is defined and what forms of digital communications should be covered by electoral rules.

As explained in response to Recommendation 10, we are awaiting the outcome of this consultation before considering how this could be applied more widely. We have also already noted that the new Centre for Data Ethics and Innovation is expected to look closely at issues around transparency and targeting.

Furthermore, we welcome the Information Commissioner's ongoing investigation into the use of data analytics for political purposes, which addresses the issue of microtargeting. We look forward to the Commissioner's full report and will consider its recommendations.

Recommendation 37

We reiterate our support for the Cairncross Review and will engage with the consultation in the coming months. In particular, we hope that Frances Cairncross will give due weight to the role of digital advertising in elections, and will make concrete recommendations about how clearer rules can be introduced to ensure fairness and transparency. (Paragraph 143)

Government response

The Cairncross review's terms of reference make specific reference to the operation of the digital advertising supply chain in the monetisation of online news, however, the review will not address politically motivated disinformation, propaganda or political advertisements during elections.

As already highlighted, on 29 July we launched the 'Protecting the Debate: Intimidating, Influence and Information' consultation, which explores which forms of digital communications should be covered by electoral rules, e.g. the requirement for imprints on campaigning materials. We are awaiting the outcome of this consultation and will consider how imprints could be implemented more widely to other forms of political advertising.

Recommendation 38

The Government should investigate ways in which to enforce transparency requirements on tech companies, to ensure that paid-for political advertising data on social media platforms, particularly in relation to political adverts, are publicly accessible, are clear and easily searchable, and identify the source, explaining who uploaded it, who sponsored it, and its country of origin. This information should be imprinted into the content, or included in a banner at the top of the content. Such transparency would also enable members of the public to understand the behaviour and intent of the content providers, and it would also enable interested academics and organisations to conduct analyses and to highlight trends. (Paragraph 144)

Government response

As with Recommendation 36, this Recommendation will be considered following the conclusion of the Government's 'Protecting the Debate' consultation.

Recommendation 39

Tech companies must also address the issue of shell corporations and other professional attempts to hide identity in advert purchasing, especially around election advertising. There should be full disclosure of targeting used as part of advert transparency. The Government should explore ways of regulating the use of external targeting on social media platforms, such as Facebook's Custom Audiences. We expect to see the detail of how this will be achieved in its White Paper later this year. (Paragraph 145)

Government response

The Government recognises the highly complex nature of the online advertising industry and as part of the Digital Charter's work programme we are keen to gather more evidence on digital business models. We will consider the Committee's recommendations on transparency in online advertising and how to best address these through workstrands of the Digital Charter.

As highlighted in response to Recommendation 23, the new Centre for Data Ethics and Innovation is expected to look closely at issues around transparency and targeting. Furthermore, as stated throughout this response, extending the imprint requirement for campaigning materials to digital communications is an area we are exploring as part of the 'Protecting the Debate' consultation, launched on 29 July. Government will give further detail following the closure of the consultation.

Recommendation 41

In November 2017, the Prime Minister accused Russia of meddling in elections and planting 'fake news' in an attempt to 'weaponise information' and sow discord in the West. It is clear from comments made by the then Secretary of State in evidence to us that he shares her concerns. However, there is a disconnect between the Government's expressed concerns about foreign interference in elections, and tech companies' intractability in recognising the issue. We would anticipate that this issue will be addressed, with possible plans of action, in the White Paper this Autumn. (Paragraph 176)

Government response

In November 2017, the Prime Minister accused the Russian state of 'a sustained campaign of cyber espionage and disruption' which has included meddling in elections and hacking the Danish Ministry of Defence and the [German] Bundestag. As noted by the Committee, the Prime Minister stated that Russia is seeking to weaponise information, 'deploying its state-run media organisations to plant fake stories and photo-shopped images in an attempt to sow discord in the West and undermine our institutions'. Following the nerve agent attack in Salisbury in March this year, we judged the Russian state promulgated at least 38 false disinformation narratives around this criminal act.

We want to reiterate, however, that the Government has not seen evidence of successful use of disinformation by foreign actors, including Russia, to influence UK democratic processes. But we are not being complacent and the Government is actively engaging with partners to develop robust policies to tackle this issue.

With regard to tackling disinformation, the Government is currently focusing on five key areas:

- further research to understand the problem,
- education and guidance to ensure citizens have the skills to tell fact from fiction;
- working with the tech sector and social media platforms to develop technological responses;
- considering whether the right regulation is in place; and
- improving our strategic communications across government.

Work to develop policies will continue and further information will be published in due course.

The Government will monitor hostile state activity online and 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.

Recently Facebook, Microsoft and Twitter have all taken action against malign activity and campaigns of foreign origin to manipulate political debate. Government welcomes these efforts and companies' willingness to share information publicly to tackle this issue. However, we believe that more needs to be done to tackle this problem proactively and across all platforms. We are actively engaging with a range of technology companies on this issue.

Recommendation 45

The Electoral Commission has recommended that there should be a change in the rules covering political spending, so that limits are put on the amount of money an individual can donate. We agree with this recommendation, and urge the Government to take this proposal on board. (Paragraph 192)

Government response

Despite talks over the last decade, there is still no cross-party consensus on the separate and broader issue of party funding at this time. The Government remains open to constructive debate and dialogue on how we can further strengthen confidence in our democratic process, and increase transparency and accountability. There is already a statutory ban on foreign donations, and we will carefully consider the Electoral Commission's observations on clarifying the rules to make clear that foreign spending on elections is also not allowed.

Recommendation 47

We recommend that the UK Government approaches other governments and follows the recommendation agreed by US and EU representatives, including representatives from this Committee, at the recent inter-parliamentary meeting at the Atlantic Council. The Government should share information on risks, vulnerabilities, and best practices to counter Russian interference, and co-ordinate between parliamentarians

across the world. Only by sharing information, resources, and best practice will this Government be able to combat Russian interference in our elections. We look forward to a White Paper this autumn, and the opportunity for the Government to set out the practical steps that it will follow to ensure greater global cooperation to combat Russian interference. (Paragraph 202)

Government response

The Government is working extensively with close partners on sharing good practice in building resilience to disinformation. We worked in the G7 to establish a Rapid Response Mechanism to counter disinformation and actively supported the establishment of the NATO Centre of Excellence for Strategic Communication. The Government also led EU partners at the June European Union Council to raise the level of ambition and resourcing of the EU External Action Service Task Forces. We fully supported the Finnish initiative to establish the Helsinki-based Hybrid Centre of Excellence, and are working with Poland to counter Russian disinformation, ensure cyber security and strengthen resilience of Eastern Partnership Countries. The Government has committed over £100m over five years to tackling the threat of Russian State disinformation internationally. This includes research on the threat online, working with NGOs who expose disinformation and developing 21st century skills amongst communities most vulnerable to disinformation.

Furthermore, the FCO strongly supports the BBC's mission to bring high quality and impartial news to global audiences. The BBC World Service is one of the world's largest international broadcasters, broadcasting news, speech and discussions in 42 languages and reaching 346 million people worldwide, with a particular focus on regions where free speech is limited. The World Service brings the UK to the world, providing a link to the UK for people and communities who wouldn't otherwise have this opportunity.

The government is investing £289m during 2016-2020 to support the BBC World Service through the World 2020 Programme. This funding has enabled the BBC World Service to undergo it largest expansion in over 70 years. World 2020 expands the BBC World Service's digital, TV and audio offering, including new and enhanced services. Twelve new language services have been launched since 2017 and existing services such as Arabic and Russian significantly enhanced. The new services are Yoruba, Pidgin, Igbo (Nigeria) Amharic, Oromo (Ethiopia), Tigrinya (Eritrea) Marathi, Gujarati, Punjabi, Telugu (India), Korean and Serbian.

Recommendation 48

Just as six Select Committees have joined forces in an attempt to combat Russian influence in our political discourse, so the Government should coordinate joint working with the different relevant Departments. Those Departments should not be working in silos, but should work together, sharing data, intelligence and expert knowledge, to counter the emerging threat of Russia, and other malign players. (Paragraph 203)

Government response

The Government supports a collaborative approach that spans departmental boundaries and makes the best use of capabilities both within and outside of Government. This 'Fusion

Doctrine' approach is integral to our delivery of national security and is set out in the National Security Capability Review of March 2018. As such the Government is already actively coordinating its own policy, analysis and strategic communications activity, as well as engaging with industry, academia, civil society and international partners to build public resilience to disinformation and respond effectively to different forms of interference. The Cabinet Office is coordinating a number of Departments including the Department for Digital, Culture, Media and Sport, the Foreign Office, the Ministry of Defence (incl. Dstl) the Home Office and the Security and Intelligence Agencies to tackle the threat from disinformation and hostile states.

Recommendation 49

We note that the Mueller Inquiry into Russian interference in the United States is ongoing. It would be wrong for Robert Mueller's investigation to take the lead about related issues in the UK. We recommend that the Government makes a statement about how many investigations are currently being carried out into Russian interference in UK politics and ensures that a coordinated structure exists, involving the Electoral Commission and the Information Commissioner, as well as other relevant authorities. (Paragraph 204)

Government response

The remit of the Special Counsel's investigation into Russian interference in the 2016 Presidential election is a matter for the United States. The Special Counsel's investigation would not take the lead on any investigations into allegations about Russian interference in the UK. 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, whether from Russia or any other State. The Government is committed to protecting the UK against any attempts to interfere with the security and integrity of our democratic processes. There has, however, been no evidence to date of any successful foreign interference.

Recommendation 51

We recommend that the Government put forward proposals in its White Paper for an educational levy to be raised by social media companies, to finance a comprehensive educational framework (developed by charities and non-governmental organisations) and based online. Digital literacy should be the fourth pillar of education, alongside reading, writing and maths. The DCMS Department should coordinate with the Department for Education, in highlighting proposals to include digital literacy, as part of the Physical, Social, Health and Economic curriculum (PSHE). The social media educational levy should be used, in part, by the Government, to finance this additional part of the curriculum. (Paragraph 246)

Government response

The Government is continuing to build the evidence base on a social media levy to inform our approach in this area. We are aware that companies and charities are undertaking a

wide range of work to tackle online harms and would want to ensure we do not negatively impact existing work. We will be considering any levy in the context of existing work being led by HM Treasury in relation to corporate tax and the digital economy.

We agree that improved digital literacy is key to tackling the spread of disinformation; the Government wants all citizens to have the digital literacy skills they need to analyse the information they consume online and protect themselves from the full range of online harms.

Digital literacy is already taught across the national school curriculum. It is covered in the computing curriculum, which also teaches pupils about e-safety. Furthermore, in the citizenship curriculum pupils are equipped to think critically, for example through media literacy so that they can distinguish fact from fiction as well as explore freedom of speech and the role and responsibility of the media in informing and shaping public opinion. In offering a broad and balanced curriculum, schools are free to address these areas when teaching on topics like media, advertising, and safe and judicious use of social media, for example through Personal, Social, Health and Economic education (PSHE).

To support young people further, the Government is making Relationships Education compulsory in all primary schools in England and Relationships and Sex Education compulsory in all secondary schools, as well as making Health Education compulsory in all state-funded schools. Navigating the online world, developing positive, respectful relationships and core knowledge on mental wellbeing is integral throughout these subjects - pupils will be taught for example, the rules and principles for keeping safe online, 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.

As set out above, there are already a range of opportunities across the curriculum to improve children's digital literacy skills and help them protect themselves from online harms. We will continue engaging with a wide range of external partners to consider how best to empower users to understand and respond to harmful content and conduct.

Recommendation 52

There should be a unified public awareness initiative, supported by the Departments for DCMS, Health, and Education, with additional information and guidance from the Information Commissioner's Office and the Electoral Commission, and funded in part by the tech company levy. Such an initiative would set the context of social media content, explain to people what their rights over their data are, within the context of current legislation, and set out ways in which people can interact with political campaigning on social media. This initiative should be a rolling programme, and not one that occurs only before general elections or referenda. (Paragraph 247)

Government response

As stated in response to Recommendation 51, we are continuing to build the evidence base around a social media levy to inform our approach in this area.

The Government is particularly concerned about the impact of disinformation on the way that the public engages with politics and political information. We recognise that online participation is now an important part of people's political engagement and as such the Government is committed to ensuring that citizens have the information and skills they need to navigate an online political world. This includes increasing transparency of election adverts, an area being explored as part of the 'Protecting the Debate' campaign referenced throughout this response. Furthermore, as part of our ongoing education and awareness-raising work, we will consider options to improve critical thinking skills and resilience to disinformation in the context of political engagement.

As also set out in response to Recommendation 51, the Government wants to ensure that all citizens - not just those in full or part-time education - have the digital literacy skills needed to spot dangers, critically assess the content they consume and navigate their lives online. We are considering the best ways of reaching an adult audience through communications campaigns and institutions such as libraries.