House of Commons

Digital, Culture, Media and Sport Committee

Misinformation in the COVID-19 Infodemic

Second Report of Session 2019–21

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 16 July 2020

HC 234
Published on 21 July 2020
by authority of the House of Commons

Digital, Culture, Media and Sport Committee

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

Current membership

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

Kevin Brennan MP *(Labour, Cardiff West)*

Steve Brine MP *(Conservative, Winchester)*

Philip Davies MP *(Conservative, Shipley)*

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

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Rt Hon Damian Green MP *(Conservative, Ashford)*

Rt Hon Damian Hinds MP *(Conservative, East Hampshire)*

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

Giles Watling MP (*Conservative, Clacton*)

Powers

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

Publication

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

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

Committee staff

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

Contacts

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

You can follow the Committee on Twitter using @CommonsDCMS.

Contents

Summary

In February, the World Health Organisation warned that, alongside the outbreak of COVID-19, the world faced an 'infodemic', an unprecedented overabundance of information—both accurate and false—that prevented people from accessing authoritative, reliable guidance about the virus. The infodemic has allowed for harmful misinformation, disinformation, scams and cybercrime to spread. False narratives have resulted in people harming themselves by resorting to dangerous hoax cures or forgoing medical treatment altogether. There have been attacks on frontline workers and critical national infrastructure as a result of alarmist conspiracy theories.

The UK Government is currently developing proposals for 'online harms' legislation that would impose a duty of care on tech companies. Whilst not a silver bullet in addressing harmful content, this legislation is expected to give a new online harms regulator the power to investigate and sanction tech companies. Even so, legislation has been delayed. As yet, the Government has not produced the final response to its consultation (which closed over a year ago), voluntary interim codes of practice, or a media literacy strategy. Moreover, there are concerns that the proposed legislation will not address the harms caused by misinformation and disinformation and will not contain necessary sanctions for tech companies who fail in their duty of care

We have conducted an inquiry into the impact of misinformation about COVID-19, and the efforts of tech companies and relevant public sector bodies to tackle it. This has presented an opportunity to scrutinise how online harms proposals might work in practice. Whilst tech companies have introduced new ways of tackling misinformation through the introduction of warning labels and tools to correct the record, these innovations have been applied inconsistently, particularly in the case of high-profile accounts. Platform policies have been also been too slow to adapt, while automated content moderation at the expense of human review and user reporting has had limited effectiveness. The business models of tech companies themselves disincentivise action against misinformation while affording opportunities to bad actors to monetise misleading content. At least until well-drafted, robust legislation is brought forward, the public is reliant on the goodwill of tech companies, or the bad press they attract, to compel them to act.

During the crisis the public have turned to public service broadcasting as the main and most trusted source of information. Beyond broadcasting, public service broadcasters (PSBs) have contributed through fact-checking and media literacy initiatives and through engagement with tech companies. The Government has also acted against misinformation by reforming its Counter Disinformation Unit to co-ordinate its response and tasked its Rapid Response Unit with refuting seventy pieces of misinformation a week. We have raised concerns, however, that the Government has been duplicating the efforts of other organisations in this field and could have taken a more active role in resourcing an offline, digital literacy-focused response. Finally, we have considered the work of Ofcom, as the Government's current preferred candidate for online harms regulator, as part of our discussion of online harms proposals. We call on the Government to make a final decision now on the online harms regulator to begin laying the groundwork for legislation to come into effect.

1 Introduction

Inquiry origins and scope

1. Our predecessor Committee carried out a landmark inquiry into *Disinformation and 'fake news'* and produced two reports in 2018 and 2019. Recognising a problem that transcended national boundaries, the Committee established and convened the first 'International Grand Committee on Disinformation' (IGC) in Westminster in November 2018. The IGC has reconvened twice since and plans to meet next in Washington D.C. to hold tech companies[1] to account. We take this opportunity to reaffirm our commitment to working with policymakers from across the globe. Our predecessor Committee also set up a Sub-Committee on Disinformation as Parliament's 'institutional home' to continue this work. As a result of growing disquiet over the role of the internet, the Government subsequently published a White Paper in April 2019 to tackle 'Online Harms' such as disinformation. In February 2020, the current Government announced that it was "minded" to name Ofcom as a proposed new 'Online Harms Regulator'.[2]

2. The current coronavirus crisis is not just a public health emergency; it has created the conditions that have exacerbated online harms before the machinery to deal with them has been put in place. On 2 February 2020, the World Health Organisation (WHO) warned that the then-epidemic had been accompanied by "a massive 'infodemic'", an overabundance of both accurate and false information that prevents people from accessing trustworthy, reliable guidance.[3] The combination of both presented an issue for public health authorities, and as such the WHO focused on working with tech companies to clarify authoritative content. By March, the focus had shifted specifically to misinformation and disinformation. UN Secretary-General António Guterres warned specifically about the "'infodemic' of misinformation and cybercrime".[4] The UN identified several harms caused by the infodemic, ranging from false narratives and scams to indirect harms exacerbated by public health measures, such as increased instances of child exploitation and abuse.[5] Months on from that warning, research has shown that a significant number of people still see misinformation about COVID-19 online each week, causing confusion, fear and mistrust.[6]

3. On 11 March, we re-established the Sub-Committee on Online Harms and Disinformation[7] and wrote to the Rt. Hon. Oliver Dowden MP, Secretary of State for Digital, Culture, Media and Sport, expressing our growing concern about the Government's

1 Consistent with the report of our predecessor Committee, we use the term 'tech company' to refer to the different types of social media and online service providers, including Facebook, Google, Twitter and TikTok. Facebook also owns Instagram and WhatsApp; Google and YouTube are owned by the parent company Alphabet.

2 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response*, February 2020

3 World Health Organisation, *Novel Coronavirus (2019-nCoV) Situation Report - 13* (2 February 2020), p 2

4 United Nations, 'UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis,' accessed 9 July 2020

5 *Ibid*

6 Ofcom, 'COVID-19 news and information: consumption and attitudes,' accessed 21 June 2020

7 Like all sub-committees, the predecessor Sub-Committee on Disinformation lapsed at the end of the last Parliament. The scope of the new Sub-Committee was broadened to reflect the Committee's ongoing intention to scrutinise the Government's online harms legislation.

delay in tackling COVID-19 disinformation and misinformation.[8] Since March, we have ourselves responded to the crisis by questioning Facebook, Google and Twitter twice each on how they are tackling misinformation and disinformation. We were dissatisfied with answers we received from the first session and were left with no option but to recall the companies, represented this time by US-based senior executives with accountability and responsibility for company policy. We also took evidence from academics, frontline health workers and Ofcom, to help us understand the causes and impact of the COVID-19 infodemic and how it can be tackled. Finally, we heard from Government ministers across several sessions, including Caroline Dinenage MP, Minister for Digital and Culture, as well as the Secretary of State. In addition to oral evidence, we also called on the public to submit examples of misinformation they have seen, and we thank all those who submitted written evidence.

Causes of the infodemic

Foreign actors

4. Causes of the infodemic are multifaceted. Evidence we received consistently emphasised loss of trust in institutions as an aim and opportunity for hostile actors. Both state (Russia, China and Iran) and non-state (such as Daesh and the UK and US far right) campaigns have spread false news and malicious content.[9] In addition, Heads of State, especially Donald Trump and Jair Bolsonaro, have deliberately spread false narratives regarding COVID-19. Professor Philip Howard, Director of the Oxford Internet Institute, told us that these actors aim "to degrade our trust in public institutions, collective leadership or public health officials".[10] Some of this content is spread through state-backed media agencies; such agencies, unlike tech companies' platforms, are regulated by Ofcom.[11] Evidence submitted by the Henry Jackson Society asserts that information disseminated by the Chinese state aimed to extol China's role in managing the virus, delegitimise factual reporting that reflects badly on the Chinese Communist Party and to create "doubt, confusion and fear" amongst target audiences whilst the world is distracted by the pandemic.[12]

Financial gain

5. Others have sought to gain financially. Several witnesses claimed that they had observed people attempting to exploit the crisis for financial gain, either through scams or quack cures.[13] Dr. Claire Wardle of First Draft News told us "[w]e are seeing a huge increase in scams and hoaxes and people motivated by financial gain", including elderberry supplements or testing kits that are falsely advertised as FDA- or CDC-approved.[14] Whilst not directly harmful, such scams may divert sick patients away from medical interventions

8 Letter from Chair to Rt Hon Oliver Dowden MP, Secretary of State for DCMS, re Coronavirus disinformation, 11 March 2020
9 Qq2, 12, 17; Henry Jackson Society (DIS0010)
10 Q2
11 *Ibid*
12 Henry Jackson Society (DIS0010) para 15
13 Q34
14 Qq34, 40

and allow the virus to continue to spread. Another witness alleged that a registered nurse has used the "veneer of trust, which other nurses have deservedly earned, to manipulate the public" by mis-selling health products.[15]

Good intentions

6. While the reasons for sharing content are well understood, it is fair to say that there remain very significant gaps in our knowledge of the originators of these messages, and their motivations, beyond those initiated by hostile foreign states and political extremists as mentioned above. Many people have shared misleading or false information with well-meaning intentions. Dr. Wardle provided insight into the psychological and social reasons why people may share misinformation, saying that "[l]arger proportions of the population are losing trust in institutions, feel hard done by, and conspiracies basically say, 'you don't know the truth. I'm telling you the truth'".[16] As a result many people "are inadvertently sharing false information believing they are doing the right thing".[17]

Impact of misinformation

Public health impact

7. Throughout our inquiry, we have heard about harms caused by misinformation to individual and public health, critical national infrastructure and frontline workers. Early examples of misinformation during the pandemic often misled people about cures or preventative measures to infection. Some people have mistakenly turned to unproven home remedies, stopped taking ibuprofen and prescribed medicine, or elsewise ingested harmful chemicals such as disinfectant.[18] Otherwise, people have avoided hospital altogether. Dr. Megan Emma Smith, consultant anaesthetist at a leading London hospital and EveryDoctor member, told us that, "[a]t the point in time when they come through the doors of the hospital, because they did not want to come to hospital, they are so, so sick. They are unbelievably unwell".[19] This impact has been particularly drastic amongst specific British communities. Another UK GP in written evidence claimed that this type of misinformation has caused particularly acute panic and confusion amongst British Asian communities, some of whom "feel adamant that doctors are actively trying to harm them or discharging them without treating them".[20]

5G conspiracies

8. Whilst misinformation has encouraged some people to take drastic measures with their own health, it has also provoked action against others. Written evidence from BT stated that, between 23 March and 23 April alone, there were 30 separate attempts of sabotage on the UK's digital infrastructure and that there had likely been 80 attacks across sites operated by all four mobile networks, with 19 occurring near critical infrastructure such as fire, police and ambulance stations.[21] EE personnel and subcontractors alone

15 Q127
16 Q37
17 Q46
18 Frontline healthcare professionals (DIS0019) para 8
19 Q116
20 Frontline healthcare professionals (DIS0019) para 32
21 British Telecom (DIS0017)

have faced 70 separate incidents, including "threats to kill and vehicles driven directly at staff".[22] Mobile UK, the trade association for the UK's four mobile network operators, was forced to issue a statement in April warning about the impact of the harassment of staff and damage to infrastructure on "the resilience and operational capacity of the networks to support mass home working and critical connectivity to the emergency services, vulnerable consumers and hospitals".[23]

Impact on frontline health workers

9. Misinformation has also directly and indirectly impacted health workers themselves. As one doctor wrote, medical staff are "battling two challenges: trying to save the lives of ICU patients succumbing to the virus and tackling the infodemic".[24] Thomas Knowles, an advanced paramedic practitioner, described the disparity in reach between authoritative NHS 111 information and misinformation spread through social media:

> I can speak to one person for ten minutes and have an influence on that one person's experience of healthcare. The Committee is probably familiar with the pandemic documentary that was circulating on YouTube, and one version of that had 40 million views within 48 hours. That is 25,000 people in ten minutes. I cannot speak to 25,000 people in ten minutes, so that level of exposure is why I think so many of us are so concerned that we need to take action to identify those clear harms that people are experiencing as a consequence.[25]

Conspiracy theories have also helped fuel targeted abuse and harassment online.[26] Worryingly, a belief that "'Asians carry the virus'" has also led to attacks and trolling and one doctor, based in the USA, wrote to us that "[a]n Asian colleague […] has had people yell at her in stores […] and had patients refuse to allow her to treat them".[27] Whilst this might appear anecdotal, UK police statistics have registered a 20% increase in anti-Asian hate crimes with more than 260 offences recorded in the UK since lockdown began.[28]

Legislative context

Online harms legislation

10. The causes and impacts of the infodemic are many and varied. Tackling such harms therefore requires a multifaceted approach. In its Online Harms White Paper, the Government stated its aim "to make Britain the safest place in the world to be online".[29] Legislation will take a "proportionate, risk-based response" by introducing "a new duty of care on companies and an independent regulator responsible for overseeing this

22 *Ibid*
23 Mobile UK, 'Statement: Mobile industry warns against the spread of baseless 5G Coronavirus (COVID-19) theories,' accessed 21 June 2020
24 Frontline healthcare professionals (DIS0019) para 12
25 Q120
26 Glitch (CVD0296) pp.8, 11, 22, 34
27 Frontline healthcare professionals (DIS0019) para 23
28 Glitch (CVD0296) pp.8, 11, 22, 34
29 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper*, CP 57, April 2019, p 5

framework".[30] These proposals satisfied two of the most important recommendations of our predecessor Committee's *Disinformation and 'fake news'* inquiry. This approach can be contrasted to Section 230 of the Communications Decency Act in the US, which protects tech companies from being held liable for third-party content hosted on their sites and takes a self-regulatory approach,[31] and the Network Enforcement Act ('NetzDG') in Germany, which forces tech companies to remove hate speech from their sites within 24 hours or face a 20 million euro fine.[32]

11. Throughout our inquiry, we expressed concern to Ministers about the pace of legislation. Changes in leadership have not helped. There have been five Secretaries of State since the Internet Safety Strategy Green Paper was introduced.[33] It has been more than a year since the White Paper consultation closed and a final consultation response has not yet been published, nor has there been a final decision on who should be the independent regulator.[34] There is no definitive date for when a Bill will be published (draft or otherwise)[35] and interim voluntary codes of practice for terrorist and child sexual exploitation and abuse content that were due in the spring are yet to materialise.[36] Our letter to the Secretary of State on 11 March 2020 raised concerns about the Government's delays in standing up the Counter Disinformation Unit despite the fact that false narratives were already spreading uncontrollably in January.[37] The Minister for Digital has contradicted initial assurances to us that legislation will be brought forward alongside the final consultation response this autumn[38] in response to a subsequent written question, where she stated instead that legislation will follow the consultation response sometime during this parliamentary session.[39] This lack of clarity at the heart of Government is deeply concerning.

12. **We are pleased that the Government has listened to our predecessor Committee's two headline recommendations, and that it will launch a duty of care and an independent regulator of online harms in forthcoming legislation. However, we are very concerned about the pace of the legislation, which may not appear even in draft form for over two years since the White Paper was published in February 2019.** ***We recommend that the Government publish draft legislation, either in part or in full, alongside the full consultation response this autumn if a finalised Bill is not ready. Given our ongoing interest and expertise in this area, we plan to undertake pre-legislative scrutiny. We also remind the Government of our predecessor Committee's recommendation for the DCMS Committee to have a statutory veto over the appointment and dismissal of the Chief***

30 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper*, CP 57, April 2019, p 8

31 "*DOJ takes aim at law that shields tech companies from lawsuits over material their users post*", CNBC, 17 June 2020

32 Digital, Culture, Media and Sport Committee, Fifth Report of the Session 2017–19, *Disinformation and 'fake news': Interim Report*, HC 363, paras 54–5

33 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q31

34 Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Qq520–1

35 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Qq376–7

36 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response*, February 2020

37 Letter from Chair to Rt Hon Oliver Dowden MP, Secretary of State for DCMS, re Coronavirus disinformation, 11 March 2020

38 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Q383

39 PQ 61725 [on internet: safety], 19 June 2020

Executive to ensure public confidence in their independence, similar to the Treasury Committee's veto over senior appointments to the Office of Budget Responsibility, and urge the Government to include similar provisions in the Bill.

Freedom of expression

13. Throughout our inquiry, we have raised concerns that legislation must not be "light touch".[40] The White Paper initially set out an illustrative, non-exhaustive list of harms in scope of the statutory duty of care that included disinformation.[41] This Government has since changed its approach. The initial consultation response subsequently clarified that there would be differentiated expectations for illegal content and so-called "harmful but legal" content.[42] At the outset of our inquiry, the Secretary of State clarified that, beyond illegal or age-restricted content, "[t]he essence of online harms legislation is holding social media companies to what they have promised to do and to their own terms and conditions".[43] Following our second session with the companies, when the impact of COVID-19 disinformation was put to him, the Secretary of State reiterated that legislation will simply "hold social media companies to their own terms and conditions".[44] Ministers repeatedly cited the tension between online harms legislation and freedom of expression as the reason for this.[45]

14. We are aware of and appreciate concerns about freedom of speech. Campaign groups Global Partners Digital, Index on Censorship, Open Rights Group, and Article 19, in a joint submission, warned against Government overreach in the context of coronavirus, arguing that "many governments are taking steps to restrict freedom of expression on the basis of the health crisis".[46] On the other hand, we are concerned about deferring responsibility for the scope of restrictions to speech to tech companies. In correspondence with Facebook, we questioned how the company defines 'harmful misinformation' and 'imminent physical harm' in the policies that underpin its action against online harms.[47] We have also observed a lack of consistent standards across platforms throughout our inquiry, and we will discuss this further in the next chapter. Moreover, ongoing bilateral discussions between tech companies and public authorities lack transparency, scrutiny and an underlying legal framework. In their submission, the four campaign groups raised "serious concerns around informal government pressure, with no legal basis, for platforms to censor, filter or restrict content" in the name of tackling online harms.[48]

40 Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Q520
41 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper*, CP 57, April 2019, p 31
42 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response,* February 2020
43 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q20
44 HC Deb, 4 June 2020, col 984 [Commons Chamber]
45 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q26; Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Qq512–3, 528–9, 543; Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Q381, 383, 386
46 Global Partners Digital, Index on Censorship, Open Rights Group, and Article 19 (DIS0005)
47 Letter from the Chair to Facebook, re Misinformation about the COVID-19 crisis supplementary, 7 May 2020
48 Global Partners Digital, Index on Censorship, Open Rights Group, and Article 19 (DIS0005)

15. We concur with evidence we received that legislation to tackle online harms must comply with principles established in international human rights law. Articles 10 and 11 (the rights to freedom of expression and freedom of assembly) of the Human Rights Act 1998 provide some conditions for freedoms of expression and assembly (as 'qualified' rights) where necessary. The recent Civil Rights Audit emphatically criticised Facebook's attitudes towards free speech, arguing that "the value of non-discrimination is equally important" as freedom of expression and that "the two need not be mutually exclusive".[49] Consultation responses to the White Paper from stakeholders such as the Internet Watch Foundation agree that harms should be set out in secondary legislation or codes of practice to provide parliamentary oversight, proportionality and to prevent overly-broad interpretations of the duty of care.[50] Despite Government proposals that the regulator should determine the scope of online harms,[51] Ofcom, the preferred candidate, told us definitively that such scope should be a matter for Parliament.[52] Full Fact suggest using the super-affirmative procedure as set out in the Legislative and Regulatory Reform Act 2006 as a mechanism to do this.[53] Several examples of 'harmful but legal' content raised during our inquiry that would require further consideration (and need to be established in legislation) are given below:

Table 1: Online Harms

Harms	Notes
Harmful misinformation	Throughout our inquiry, companies recognised that spreading 'harmful misinformation' was against their policies, though (as will be discussed below) such policies often differed in their definition and breadth of what constitutes 'misinformation' and what might make it 'harmful'.
Disinformation	Disinformation was a harm proposed by the Online Harms White Paper as a 'harm with a less clear definition'. The White Paper stated that "[c]ompanies will need to take proportionate and proactive measures to help users understand the nature and reliability of the information they are receiving, to minimise the spread of misleading and harmful disinformation".[54]
Hatred by sex—whether birth sex or acquired sex/ gender	Written evidence from Glitch, a leading UK charity championing people's right to be online safely without discrimination, called for the Government to include 'hatred by sex' in its definition of online harms. Their evidence observed that "[m]ultiple reports have shown that women and marginalised communities, who are at higher risk of facing online abuse, have been heavily impacted by the pandemic's effect on online safety".[55]

49 Laura W. Murphy, Megan Cacace et al, Facebook's Civil Rights Audit – Final Report (July 2020), p 12
50 Internet Watch Foundation, *Online Harms White Paper Response* (April 2019), p 7
51 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Q380
52 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 June 2020, HC (2019–21) 439, Q6
53 Full Fact, Full Fact response to the Online Harms White Paper, accessed 25 June 2020
54 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response*, February 2020
55 Glitch (CVD0296) pp.8, 11, 22, 34

Harms	Notes
Incitement to self-harm	The Online Harms White Paper also proposed that 'Advocacy of self-harm' could be a harm in scope.56 Dame Melanie Dawes, CEO of Ofcom, noted that "images of self-harm can be hugely damaging, so platforms that have a younger audience will need to demonstrate that they understand the sorts of harms that might be happening on their platforms, that they have identified what those are, that they have researched the impact and that they have in place procedures to prevent, mitigate or deal with those sorts of harms when they come up".[57]
Anonymous online abuse	The impact of anonymous online abuse was raised in our first session with tech companies and in a Home Affairs Select Committee session at which our Chair was a guest. In the latter session, the Minister for Digital said that "this kind of faceless attack can bully people away from engaging in social media and other platforms in which they might want to participate, so it is anti-democratic in many senses".[58]

16. **Online harms legislation must respect the principles established in international human rights law, with a clear and precise legal basis. Despite the Government's intention that the regulator should decide what 'harmful but legal' content should be in scope, Ofcom has emphasised repeatedly that it believes this is a matter for Parliament. Parliamentary scrutiny is necessary to ensure online harms legislation has democratic legitimacy, and to ensure the scope is sufficiently well-delineated to protect freedom of expression.** ***We strongly recommend that the Government bring forward a detailed process for deciding which harms are in scope for legislation. This process must always be evidence-led and subject to democratic oversight, rather than delegated entirely to the regulator. Legislation should also establish clearly the differentiated expectations of tech companies for illegal content and 'harmful but legal'.***

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

56 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response*, February 2020

57 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 June 2020, HC (2019–21) 439, Q14

58 Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Q529

2 Tech companies' response

Monetising misinformation

The role of algorithms

18. The prevalence of misinformation online must be understood within the business context of tech companies. Tech companies generate revenue primarily through advertising targeted at users based on observed or perceived tastes and preferences, which is maximised by increasing the user base, data collection, average user time and user personalisation. We know that novelty and fear (along with anger and disgust) are factors which drive 'engagement' with social media posts; that in turn pushes posts with these features further up users' newsfeeds—this is one reason why false news can travel so fast. This is opposite to the corporate social responsibility policies espoused by tech companies relying on this business model. The more people engage with conspiracy theories and false news online, the more platforms are incentivised to continue surfacing similar content, which theoretically encourages users to continue using the platform so that more data can be collected and more adverts can be displayed. This model, described as the *attention economy*, underpins the addictive[59] features of social media.[60] Stacie Hoffmann of Oxford Information Labs told us that misinformation and disinformation in particular "elicits a very strong reaction one way or the other but we do know that the algorithms are rewarding negative reactions" to this content.[61] Thomas Knowles described how the social and financial costs of mitigating the impact of misinformation then falls to the public:

> If somebody watches something that might be a bit flat-earthy, maybe they will be interested in something a bit homeopathic. It is effectively a monetisation of the content that is published on those services. When we are looking at monetisation of content that actively engenders a social harm, that is actively damaging to public trust and to public health, I think we are looking at a moral obligation. That cost cannot be borne by the public purse when we are looking at organisations that are turning over billions of pounds a year.[62]

The Minister for Digital has confirmed that, given that algorithms constitute a design choice, the online harms regulator will be empowered "to request explanations about the way an algorithm operates, and to look at the design choices that some companies have made and be able to call those into question".[63]

19. Tech companies rejected this characterisation, citing ongoing efforts to promote authoritative information and demote misinformation, though we did not receive evidence to support this.[64] Asked whether the fact that people engage with misinformation meant

59 Our predecessor also published a report into '*Immersive and addictive technologies*', examining these issues in more detail; the Government agreed to our predecessor's most significant recommendations into loot boxes and the need for greater research in its response.

60 Dr. Nejra van Zalk (DIS0020)

61 Q29

62 Q128

63 Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Q561

64 Q67 [Katy Minshall]; Qq91–2, 94 [Richard Earley]; Qq99–100, 109 [Alina Dimofte]; Qq135, 139, 145 [Derek Slater]; Qq141, 147–8 [Leslie Miller]

the companies had no incentive to remove it, Richard Earley of Facebook argued that the company's aim is instead to drive "meaningful social interaction" with "content we think people are most likely to engage with".[65] YouTube, similarly, claimed that, "[o]n the recommendation-driven watch time of this type of borderline content, it reflects less than 1% of the totality of the watch time of content that is being recommended".[66] Despite these efforts, algorithms continue to recommend harmful material. Referring specifically to Google Search's algorithms, Stacie Hoffmann told us that:

> Google has tweaked its algorithms—and we know this from studies that we have done and that we have seen—since 2016 to help reduce the prominence of junk news or misinformation in their searches, but those also come back up. It takes about not even a year for the reach of those websites to go back up again.[67]

In further correspondence, YouTube did commit to "taking a closer look at how we can further reduce the spread of content that comes close to—but doesn't quite cross the line of—violating our Community Guidelines and will continue to make necessary changes to improve the effectiveness of our efforts".[68] We welcome this commitment, though we request that the company report back to the Committee in the future in recognition of our concerns on the subject and in good faith that this work will be undertaken.

20. **The need to tackle online harms often runs at odds with the financial incentives underpinned by the business model of tech companies. The role of algorithms in incentivising harmful content has been emphasised to us consistently by academia and by stakeholders. Tech companies cited difficulties in cases of 'borderline content' but did not fully explain what would constitute these cases. Given the central role of algorithms in surfacing content, and in the spread of online harms such as misinformation and disinformation in particular, it is right that the online harms regulator will be empowered to request transparency about tech companies' algorithms. *The Government should consider how algorithmic auditing can be done in practice and bring forward detailed proposals in the final consultation response to the White Paper.***

Transparency in advertising

21. Oral evidence to our inquiry argued that some companies have taken some action against opportunistic advertisers,[69] though some inconsistencies where some scammers have slipped through the net have also been observed.[70] Advertising libraries, which provide an archive of adverts promoted on their platforms, are not standardised. This means that different tech companies offer different amounts of information on their ads, which makes oversight difficult. Twitter's 'Ads Transparency Centre', for example, only provides an archive for adverts that appear in the previous seven days, with no meaningful data on targeting, audience or advertising spend, unlike the ad libraries of Google and Facebook, which archive more ads and do provide this information.

65 Q92 [Richard Earley]
66 Q141 [Leslie Miller]
67 Q25
68 Letter from Rebecca Stimson, Facebook, re evidence follow-up, 26 June 2020
69 Q22 [Stacie Hoffmann]
70 Qq34, 40 [Dr. Claire Wardle]; Q127 [Thomas Knowles]

Funding false narratives

22. Tech companies have also allowed spreaders of misinformation to monetise their content, to the benefit of both platform and publisher. Our inquiry found that YouTube, for example, have allowed actors to profit from peddling harmful misinformation.[71]

23. As well as selling advertising space on their own platforms, some tech companies, like Google and Amazon, provide adverts for third-party sites. Stacie Hoffmann noted that ad provider tech companies have often directly supplied advertising to sites that spread misinformation:

> we found that Google and Amazon are the two biggest ad providers for junk news purveyors and those are the websites that are getting those click-throughs to try to gain money as part of a round ecosystem. We have known that there is a plethora of websites since 2016 that have been key purveyors of junk news.[72]

Research from the Global Disinformation Index has recently found that Google has provided adverts for almost 90% of sites spreading coronavirus-related conspiracies.[73] When we first put this to Google the company questioned the validity of this study, claiming that "it is hard to peer review its findings" and that the "the revenue estimates also do not accurately represent how publishers earn money on our advertising platforms".[74] However, we observed that, despite providing general figures from 2019 (unrelated to misinformation and prior to the pandemic) and figures relating to takedowns of individual adverts, Google's response conspicuously omitted the number of advertising accounts removed for coronavirus-related misinformation.[75] When we challenged the company with corroborating studies in our second evidence session, Google reflected on the limitations of its proactive systems and policies, stating that "this has been a very fluid situation where we have been having to, in real time and 24/7, look at our policies, re-evaluate them and see how we can improve".[76]

24. **The current business model not only creates disincentives for tech companies to tackle misinformation, it also allows others to monetise misinformation too.** ***To properly address these issues, the online harms regulator will need sight of comprehensive advertising libraries to see if and how advertisers are spreading misinformation through paid advertising or are exploiting misinformation or other online harms for financial gain. Tech companies should also address the disparity in transparency regarding ad libraries by standardising the information they make publicly available. Legislation should also require advertising providers like Google to provide directories of websites that they provide advertising for, to allow for greater oversight in the monetisation of online harms by third parties.***

71 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020
72 Q22
73 Qq103–4 [Philip Davies MP]; Letter from the Chair to Google, re Misinformation about the COVID-19 crisis, 4 May 2020
74 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020
75 *Ibid*
76 Q161 [Derek Slater]

Funding quality journalism

25. Quality journalism has often been cited as an effective counter to misinformation, though the traditional markets for news have been disrupted by the advent of new media. We were told that tech companies' funding and support for quality journalism has increased during the pandemic, in recognition of the threat posed to the industry.[77] Google in particular emphasised its record in funding journalism projects, which have included setting up a global Journalism Emergency Relief Fund and making a $1 million donation to the International Center for Journalists.[78] As the biggest beneficiaries of traditional journalism, Google and YouTube were questioned whether the current division of revenue between quality news organisations, who generate information and are cited as authoritative sources counterbalancing false news, and themselves, who simply deliver that information, was equitable. Google robustly and repeatedly declined to comment on the division of revenue. Our concerns have since been vindicated by the Competition and Markets Authority's recent market study final report into the Online Platforms and Digital Advertising, which concluded that weak competition in digital advertising caused by players such as Facebook and Google "undermines the ability of newspapers and others to produce valuable content, to the detriment of broader society".[79]

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

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

Platform policies against misinformation

28. Tech companies' policies, terms, conditions, guidelines and community standards set the rules for what is and is not acceptable when posting or behaving on their platforms. These often go beyond the requirements of the law, such as in the case of hate speech or graphically violent content.[80] Throughout our inquiry, tech companies told us that their policies were their primary consideration when tackling misinformation, disinformation

77 Q28

78 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020

79 Competition and Markets Authority, *Online Platforms and Digital Advertising* (July 2020), p 5

80 Home Affairs Committee, Fourteenth Report of the Session 2016–17, *Hate crime: abuse, hate crime and extremism online*, HC 609 para 38

and other so-called 'harmful but legal' content online.[81] The Government has said that the "essence"[82] of online harms legislation will be to "hold social media companies to their own terms and conditions".[83]

29. The tech companies were often criticised for having unclear policies and applying them inconsistently. Indeed, Facebook conceded during our inquiry that "our enforcement is not perfect" regarding online harms.[84] Stacie Hoffmann explained that, whilst enforcement of policies had improved somewhat, such policies often do not set out how they will be applied in practice, particularly regarding 'takedowns', where content is removed outright.[85] When we wrote to Facebook after our first session in April, we asked about several examples of misinformation to see whether they would violate company policies on "harmful misinformation" and "imminent physical harm".[86] These examples included posts containing ineffective or outright harmful medical advice wrongfully attributed to either Stanford or St. George's Hospital, a video of several body bags wrongfully claiming to depict COVID-19 victims at St. Mary's Hospital, and an image of a crowded mosque wrongfully purporting to have been taken during the lockdown period.[87] Facebook's response did not address these examples, saying that "[t]he content and context of specific posts are essential to determining whether a piece of content breaches our Community Standards", despite their standards themselves describing several hypothetical examples.[88] Beyond misinformation, we also raised with Facebook two instances of hate speech that had been reported to the company. The first post incited violence against a minority community, threatening to "Bomb the Board of Deputies of British Jews"; the second racially caricatured and mocked the death of George Floyd.[89] Though Facebook acknowledged to us that these examples did go against their policies, we were surprised to hear that both were initially described by Facebook moderators as "not [going] against any of our community standards" and that, in the first instance, moderators suggested that "you unfriend the person who posted it".[90] Our findings were supported by the findings of the Civil Rights Audit, which found that Facebook's policy response to hateful content targeting Muslims and Black and Jewish people has been consistently inadequate.[91]

30. Prior to the pandemic, many of the tech companies did not have robust policies against harmful misinformation and have also often been slow in adapting their policies to combat it. Stacie Hoffmann told us that many tech companies "do not necessarily have a lot of terms specific to misinformation, disinformation or false news", whilst those "that are directly related to misinformation or junk news tend to be very high level and confusing".[92] Only Facebook argued that tackling COVID-19 misinformation such as 5G conspiracies

81 Q69 [Katy Minshall]; Q85 [Richard Earley]; Qq103–5, 107, 109 [Alina Dimofte]; Qq141, 143, 153–4, 158–161 [Derek Slater, Leslie Miller]; Qq165, 168, 170–2, 183, 191 [Monika Bickert]; Qq198, 203–4, 206, 217, 220, 225 [Nick Pickles]

82 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q20

83 HC Deb, 4 June 2020, col 984 [Commons Chamber]

84 Qq186–190 [John Nicolson MP, Monika Bickert]

85 Q21

86 Letter from the Chair to Facebook, re Misinformation about the COVID-19 crisis supplementary, 7 May 2020

87 We chose these examples as we considered that each example could, directly or indirectly, cause harm to their audience, either to the recipient through incorrect medical advice or encouraging them to stay away from hospitals to inciting damage against critical national infrastructure and employees or minority communities.

88 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020

89 Qq186–9 [John Nicolson MP]

90 *Ibid*

91 Laura W. Murphy, Megan Cacace *et al*, *Facebook's Civil Rights Audit – Final Report* (July 2020), p 8

92 Qq18, 21

was a matter of enforcing existing policies around real world harm rather than introducing new ones.[93] By contrast, American news website *The Hill* reported in February that Reddit, a sharing and discussion site, did not have any policies on health misinformation at all, leaving decisions to the discretion of volunteer 'subreddit' moderators; when asked if a policy against medical misinformation would help moderators, one reportedly replied "yes, full stop".[94] Similarly, TikTok's policies at the beginning of the pandemic reportedly only covered scams and fake profiles,[95] but has since been broadened to include medical misinformation, misinformation based on hate speech and misinformation likely to cause societal panic and real world harm.[96]

31. The lack of consistency in policy enforcement is in contrast to the standards enforced on broadcasters. In an interview in April hosted on the London Real channel, David Icke made several false claims linking coronavirus to 5G and that a vaccine would contain "nanotechnology microchips" that went unchallenged throughout the show.[97] When asked if people should attack 5G masts, he responded that "people have to make a decision" about what to do as "[i]f 5G continues and reaches where they want to take it, human life as we know it is over"; several users called for further attacks on 5G towers in the comments that appeared alongside the feed.[98] An expedited Ofcom investigation found the owner ESTV to be in breach of the broadcast code for "[failing] in its responsibility to ensure that viewers were adequately protected".[99] The next day, YouTube removed the video and announced that it would ban COVID-19 conspiracy theories, though the BBC reported that YouTube was aware of the video at the time it was livestreamed. Moreover, though Google argued at the time that it had donated its share of the revenue to charity,[100] it later confirmed in correspondence to us that the hosts had been allowed to keep revenue generated from 'Super Chats'.[101] When we raised this with Google, the company told us that initial action against 5G misinformation was constrained by pre-existing policies and only became possible when these policies were updated:

> At the time that we first viewed the video it was not against the policies we had at that time. That is why we understood that our policies needed to evolve.[102]

Google justified its approach, saying that "it was the first instance that we have seen where these kinds of 5G allegations were creating real-world harm and were being linked to the coronavirus in particular".[103] However, the company admitted that it was aware of trends regarding 5G misinformation prior to the London Real livestream.[104]

93 Q84
94 "*Reddit enlists users to combat coronavirus misinformation*", The Hill, 7 February 2020
95 *TikTok Adds New Rules to Ban Harmful Misinformation in the App*, Social Media Today, 9 January 2020
96 TikTok (DIS0018), p 3
97 "*Facebook removes David Icke coronavirus-5G conspiracy video*", ITV, 9 April 2020
98 Ibid
99 Ofcom, Ofcom decisions on recent programmes featuring David Icke and Eamonn Holmes, accessed 24 June 2020
100 Qq110–2 [Clive Efford MP, Julian Knight MP, Alina Dimofte]
101 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020
102 Q109
103 Q107
104 Q108

32. **The Government has repeatedly stated that online harms legislation will simply hold platforms to their own policies and community standards. However, we discovered that these policies were not fit for purpose, a fact that was seemingly acknowledged by the companies.** ***The Government must empower the new regulator to go beyond ensuring that tech companies enforce their own policies, community standards and terms of service. The regulator must ensure that these policies themselves are adequate in addressing the harms faced by society. It should have the power to standardise these policies across different platforms, ensuring minimum standards under the duty of care. The regulator should moreover be empowered to hand out significant fines for non-compliance. It should also have the ability to disrupt the activities of businesses that are not complying, and ultimately to ensure that custodial sentences are available as a sanction where required.***

33. Other lawmakers have taken steps to address disparities between platform responses to misinformation and disinformation, albeit through voluntary arrangements. The Electoral Commission of India, for example, last year developed a voluntary code of ethics with tech companies for all future elections, involving more transparency in political advertising and a 48-hour silence period before the end of polling.[105] The European Union has similarly agreed a voluntary code of practice for disinformation, requiring monthly reporting and certain principles of best practice in advertising, user reporting and fake accounts,[106] though it has been reportedly criticised by some member-states as "insufficient and unsuitable to serve as the basis for sustainably addressing disinformation on social platforms".[107] Finally, the Australian Government has asked digital platforms to develop voluntary codes of practice for online misinformation and the provision of quality journalism, which it expects to be in place by December 2020, and has tasked the Australian Communications and Media Authority to assess the codes' development and effectiveness.[108]

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

Identifying and reporting misinformation

Automated flagging vs human reporting

35. The first step in effectively tackling false information about COVID-19 is to identify and flag misinformation and disinformation. There are two main ways of identifying harmful content online. First, companies can respond to harmful content reported by users. The Online Harms White Paper's proposed duty of care would require companies to take "prompt, transparent and effective action following user reporting" of harms and to be transparent about "the number of reports received and how many of those reports

105 "*Social media platforms agree to follow 'code of ethics' in India for elections*", The Drum, 27 September 2019
106 European Commission, Code of Practice on Disinformation, accessed 9 July 2020
107 "*EU code of practice on disinformation 'insufficient and unsuitable,' member states say*", EURACTIV, 5 June 2020
108 ACMA, Australian voluntary code(s) of practice for online misinformation, accessed 9 July 2020

led to action".[109] For disinformation specifically, the White Paper proposed "[r]eporting processes […] to ensure that users can easily flag content that they suspect or know to be false, and which enable users to understand what actions have been taken and why".[110] Second, companies can proactively use systems to identify and tackle harmful content themselves. This is done using a combination of automated systems, based on artificial intelligence, and human moderators, who do not proactively search for illegal or harmful content but review content that has been flagged to them. Tech companies like Facebook, Google and Twitter have previously been criticised for outsourcing moderation to users to minimise expenses,[111] but nowadays the companies have moved more towards investment in AI flagging and moderation.[112]

36. At the outset of our inquiry, written and oral evidence endorsed the need for more user reporting and better responses from tech companies, particularly for instances of misinformation. Evidence submitted by the Henry Jackson Society recommended "the creation of a new misinformation flag […], which would allow users to pinpoint content that is factually incorrect or harmful".[113] The Tony Blair Institute similarly observed a "[l]ack of clear reporting frameworks specifically for public health misinformation" and recommended that "[t]he trusted-flagger system needs to be explicitly extended to COVID-19 misinformation to ensure external experts can advise on false information".[114] The response from tech companies has been inconsistent. One the one hand, TikTok told us that they have implemented a granular reporting function for misinformation, allowing users to "select 'Misleading information' and then 'COVID-19 misinformation' as the reason for their report".[115] Facebook also acknowledged the value of user reporting, saying that misinformation linking 5G to coronavirus was initially raised both by "reports from our work with Government, the media, NGO partners and also as flagged by our users" and subsequently "started then removing it on the basis of where it was flagged to us by users or where others flagged it to us".[116] On the other hand, oral evidence from researchers called for more granular reporting on Google Search to similar standards as provided by YouTube to report and counteract junk news surfacing through algorithmic curation and feedback loops.[117] We also saw evidence that companies were not responding efficiently to user reporting. Alongside the two examples of hate speech discussed above, we received written evidence from the Pirbright Institute, a research centre studying infectious diseases in farm animals, who detailed how, due to conspiracies linking Bill Gates to the virus outbreak, conspiracy theorists had begun harassing and doxxing (i.e. leaking personal or identifying information of) staff.[118] Pirbright's evidence, which was subsequently reported by BBC News Reality Check, claimed that trolls had created a false website to exacerbate these conspiracies, leading to other people being misled that the Institute was suppressing a vaccine to the virus.[119] The Institute informed us that Google

109 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper - Initial consultation response*, February 2020
110 *Ibid*
111 Home Affairs Committee, Fourteenth Report of the Session 2016–17, *Hate crime: abuse, hate crime and extremism online*, HC 609 para 31
112 "*How Facebook is using AI to combat COVID-19 misinformation and detect 'hateful memes'*", The Verge, 12 May 2020
113 Henry Jackson Society (DIS0010) para 26
114 Tony Blair Institute (DIS0013) p 3
115 TikTok (DIS0018)
116 Q85 [Richard Earley]
117 Qq24–5 [Stacie Hoffmann]
118 The Pirbright Institute (DIS0009)
119 *"Coronavirus: How a false rumour led to hate online"*, BBC News, 19 June 2020

Business had consistently refused to take action on this website despite reports to them emphasising the reputational damage and personal harm being done to the Institute and its staff.[120]

37. Throughout our inquiry, tech companies consistently downplayed the role of user reporting. Google, when justifying the lack of granular user reporting in Search compared to user reporting on YouTube,[121] wrote that "this kind of anecdotal reporting is not always the best way to address the important issues of low quality or misleading web pages in search results".[122] When later asked about this disparity directly, Google replied:

> Search is a reflection of the web; it indexes the web. It is not content we directly have control over or are responsible for, but we certainly take action on illegal content when we are sent notices for removal. As I said at the outset, we work very diligently to raise up authoritative sources and down-rank things that are low quality or misleading. We rely on a range of different signals to do that well. We have on every search page a place for people to send feedback, and we then take that feedback into account.[123]

However, whilst Google asserted in this response that Search simply 'reflects the web', it argued elsewhere that it had been curating results, including based on user feedback, as evidence of its action against misinformation, with no acknowledgement of this contradiction.[124] Twitter, meanwhile, which allows users to report "fake accounts" but not specific tweets as false,[125] argued that "user reports can add a lot of noise to the system, slowing down response and enabling people to report Tweets with which they simply disagree—not because they break the rules".[126]

38. Instead, tech companies consistently championed the efficiency of their own procedures in flagging and removing harmful content, particularly AI content moderation. These assertions often came in response to questions about, or in contrast to, user reporting,[127] even though both user reporting and proactive systems are considered complementary within the Online Harms White Paper.[128] In oral evidence, Facebook claimed that "[i]n the case of the child exploitative material […] that is well above 99% and has been for a number of years".[129] In correspondence, Google said that, on YouTube, "[w]e have removed thousands of videos promoting COVID-19 misinformation from our platform, and the majority of these videos were viewed 100 times or fewer".[130] Twitter, similarly, wrote that, during the 2019 general election, "the majority of Tweets we removed for breaking our rules on voter misinformation were detected proactively through our own systems, and

120 The Pirbright Institute (DIS0009)
121 By this, we observe that, in YouTube, users can report specific videos for, i.e., being misleading or featuring illegal or copyrighted content; in Google Search, users can only give feedback in a simple text box at the bottom of the page, rather than for specific results that appear with options for why.
122 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020
123 Q139 [Derek Slater]
124 Q145[Derek Slater] ("again what we strive to do with Search is raise up authoritative sources and demote and down-rank low-quality, misleading information")
125 Letter from the Chair to Twitter, re Misinformation about the COVID-19 crisis, 4 May 2020
126 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
127 Qq98–100 [Alina Dimofte]; Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020; Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020; Q191 [Monika Bickert]
128 Department for Digital, Culture, Media and Sport and Home Office, *Online Harms White Paper*, CP 57, April 2019, p 44
129 Q87 [Richard Earley]
130 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020

that user reports were a far less effective indicator of urgency and priority".[131] Despite these claims, written evidence consistently emphasised the limitations of automated systems. The charity Glitch wrote that "[i]ncreased reliance on artificial intelligence to filter out abusive harmful content on social media platforms during the pandemic can lead to erroneous content moderation decisions".[132] Glitch's criticism of tech companies' overreliance on AI moderation was evidenced by research recently published by the Internet Watch Foundation, which found that, as a result of COVID-19-related staffing constraints on tech company moderators and law enforcement, the number of URLs containing images of child sexual abuse taken down during the pandemic has fallen by 89%.[133] Google did acknowledge the limitations of AI moderation, emphasising the need for human review: "[m]achines help us with scale and speed, whereas humans can bring judgement and can understand context".[134] In oral evidence, the company reiterated that AI moderation can be limited when identifying misinformation, as it is "not as good at identifying particular context, and that is often very important or always very important when it comes to speech issues".[135] Evidence from Facebook, which does allow users to report specific posts as "false news",[136] similarly recognised that, "due to the adversarial nature of the space we find ourselves in, sometimes people are able to get round our systems—our human reviewers or our automated systems—and content can appear on the platform for a short time".[137] Moreover, Google also acknowledged that automated systems face "additional complexities" and can be less accurate when reviewing media such as images and video compared to text.[138]

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

Bots and 'blue ticks'

40. Our inquiry examined the role of different types of accounts during the COVID-19 infodemic: bots and influencers. We looked at the impact of bots. Bots are autonomous programmes designed to carry out specific tasks; chatbots, for instance, are used to conduct

131 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
132 Glitch (CVD0296) pp.8, 11, 22, 34
133 Glitch (CVD0296) pp.8, 11, 22, 34
134 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020
135 Q143 [Derek Slater]
136 Letter from the Chair to Twitter, re Misinformation about the COVID-19 crisis, 4 May 2020
137 Q81[Richard Earley]
138 Qq142, 144 [Giles Watling MP, Derek Slater]

online conversations, typically in customer service, request routing or information-gathering contexts.[139] Bots can also be used to kickstart the spread disinformation amongst people on social media. Professor Philip Howard of the Oxford Internet Institute told us that "[o]ne day they start waking up and spreading conspiracy stories about COVID-19 and that is how the content leaks into our social media feeds".[140] Professor Howard also notes that the use of bots and 'cyborg' accounts (which mix human and automated features)[141] in online manipulation can sometimes be hard to identify for the average user, particularly when the account in question does not conform to typical identifiers such as no profile picture, history or followers.[142] The Henry Jackson Society argued that China in particular has used "organised groups of online activists […] backed up by virtual-identity 'bots' and have spread disinformation about COVID-19".[143] Academic research has posited that there has been an upswell of bot activity on Twitter in particular to amplify disinformation.[144]

41. Throughout our inquiry, Twitter did not adequately engage with our concerns on the topic, claiming that it could not provide information on what proportion of accounts identified as spreading disinformation were bots or used extensive automation.[145] Twitter emphasised that the use of bots and automated functions (such as scheduling) is not against company policies and told us that "accounts use a range of different automated measures and so it would be misleading to say a specific number".[146] Concurrent to our inquiry, Twitter's Global Policy Director Nick Pickles, who also gave evidence on the subject, argued in a company blog post that "[w]e've seen innovative and creative uses of automation to enrich the Twitter experience—for example, accounts like @pentametron and @tinycarebot" (though it should be noted that these examples describe bots that are clearly labelled as such).[147] In correspondence, the company argued that its system of "source labels", which informs users whether content is published on a phone app or through third party software, was an adequate alternative approach to taking more proactive efforts to label bots.[148]

42. **Research has consistently suggested that bots play an active role in spreading disinformation into users' news feeds. Despite our several attempts to engage with Twitter about the extent of the use of bots in spreading disinformation on their platform, the company failed to provide us with the information we sought. *Tech companies should be required to regularly report on the number of bots on their platform, particularly where research suggests these might contribute to the spread of disinformation. To provide transparency for platform users and to safeguard them where they may unknowingly interact with and be manipulated by bots, we also recommend that the regulator should require companies to label bots and uses of automation separately and clearly.***

139 Our predecessor Committee discussed the role of bots in more depth in the Interim Report of its inquiry into *Disinformation and 'Fake News'*

140 Q4

141 Oxford Internet Institute, University of Oxford, The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation (4 September 2019) p 11

142 Q4

143 Henry Jackson Society (DIS0010) para 12

144 *"Nearly half of Twitter accounts pushing to reopen America may be bots"*, MIT Technology Review, 21 May 2020

145 Q53 [Katy Minshall]

146 Qq52–3 [Katy Minshall]; Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020

147 *"Bot or not? The facts about platform manipulation on Twitter"*, Twitter, 18 May 2020

148 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020

43. We also examined the role of prominent public figures in spreading misinformation, and the implications of verification of these accounts (often designated by a 'blue tick'). Twitter acknowledged that although verification "was meant to authenticate identity and voice", it has since also "been interpreted as an endorsement or an indicator of importance" by platforms.[149] Professor Howard told us that influencer accounts can often act as a "gateway drug" for misinformation and exacerbate the impact of bots:

> If a prominent Hollywood star or a prominent political figure says things that are not consistent with the science or the public health advice, some people will go looking for that stuff and they will spread it. That is how misinformation develops. Those human influencers are often the pivot point that takes a lie from something that bots just share with each other to something that passes in human networks.[150]

In oral evidence, we suggested that, given it amounts simply to a validation of identity, Twitter could offer verification to all users to prevent the blue tick being considered as an endorsement, as well as to tackle anonymous abuse.[151] Research from Clean Up the Internet conducted during lockdown has demonstrated a clear link between anonymous Twitter accounts and the spread of 5G conspiracy theories about COVID-19.[152] In subsequent correspondence, Twitter argued that in response to the 'verification as endorsement' misconception, it "closed all public submissions for verification in November 2017" and promised to keep us updated pending review of this process.[153]

44. Further, tech companies have not enforced policies, particularly around misinformation, as robustly or consistently for verified users as for the public. The independent Civil Rights Audit supports our findings in this regard. It states that, by not acting against the powerful (including powerful politicians), "a hierarchy of speech is created that privileges certain voices over less powerful voices".[154] In our first session with the companies, Twitter claimed that "[w]e have taken action against other world leaders around the globe, particularly in the past few weeks, when it comes to COVID-19 misinformation", though did not confirm explicitly whether this had been applied to the President of the United States, Donald Trump.[155] One week prior to our second session with the companies, Twitter labelled several tweets by President Trump for making misleading claims;[156] Facebook by contrast, left the same posts up, and was subsequently criticised by dozens of former employees in an open letter to CEO Mark Zuckerberg published in *The New York Times*.[157] Monika Bickert, Facebook's Head of Product Policy and Counterterrorism, surprisingly said she was unaware of the letter. When challenged about Facebook's lack of action, she emphasised several times that the posts did not violate Facebook's terms. When challenged specifically on one post, which is known to have originated from pro-segregationists during the civil rights movement,[158] Ms. Bickert

149 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
150 Q8
151 Qq54–8 [John Nicolson MP, Katy Minshall]
152 Clean Up the Internet, 'New research: anonymous Twitter accounts fuelled the spread of Coronavirus 5G conspiracy theories,' accessed 16 July 2020
153 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
154 Laura W. Murphy, Megan Cacace *et al.*, *Facebook's Civil Rights Audit – Final Report* (July 2020), p 9
155 Qq68–9 [Katy Minshall]
156 *"Twitter's decision to label Trump's tweets was two years in the making"*, The Washington Post, 30 May 2020
157 *"Early Facebook Employees Disavow Zuckerberg's Stance on Trump Posts"*, The New York Post, 3 June 2020
158 *"The History Behind 'When The Looting Starts, The Shooting Starts'"*, NPR, 29 May 2020

argued that "[o]ur policy is that we allow people to discuss Government use of force".[159] The Civil Rights Audit does note that, however, that Facebook also failed to act on a series of posts that "labelled official, state-issued ballots or ballot applications 'illegal' and gave false information about how to obtain a ballot", despite clear company policies against voter suppression.[160] These inconsistencies are not exclusive to Facebook. Twitter was also criticised for locking one user out of a parody account, @SuspendThePres, which copied the President's tweets word for word, for glorifying violence.[161] In response, Twitter said that:

> We said if an account breaks our rules but meets the criteria of being verified, having more than 100,000 followers and being operated by a public figure, we may take the option that, in the public interest, we want that tweet to be available. One of those accounts meets those criteria; one of them does not. […] This is the system working equally. Both tweets broke the rules; both tweets were actioned. One from a public figure was maintained to allow debate.[162]

45. **The pandemic has demonstrated that misinformation and disinformation are often spread by influential and powerful people who seem to be held to a different standard to everyone else. Freedom of expression must be respected, but it must also be recognised that currently tech companies place greater conditions on the public's freedom of expression than that of the powerful. *The new regulator should be empowered to examine the role of user verification in the spread of misinformation and other online harms, and should look closely at the implications of how policies are applied to some accounts relative to others.***

Stopping the spread: labelling and 'correct the record' tools

46. This crisis has demonstrated that some tech companies can use technological innovations to tackle online harms such as misinformation. Both Twitter and Facebook have begun to apply warning labels to content that has been independently fact-checked and debunked. Several contributors to our inquiry, including Professor Philip Howard, Dr. Claire Wardle of First Draft News, and the Tony Blair Institute, endorsed the use of warning labels to cover or contextualise misinformation and other harmful content, and direct users to authoritative sources information as a proportionate alternative to straightforward content takedowns.[163] Alongside Twitter's aforementioned labelling,[164] Facebook similarly asserted in correspondence that "100% of those who see content already flagged as false by our fact-checkers" will see a warning screen, which was applied to 40 million pieces of content in March and 50 million pieces of content in April.[165] Two weeks after our second evidence session, Google also announced that it would add warning labels to edited or decontextualised images.[166] YouTube and TikTok have not rolled out

159 Qq168–172 [Kevin Brennan MP, Monika Bickert]
160 Laura W. Murphy, Megan Cacace *et al.*, *Facebook's Civil Rights Audit – Final Report* (July 2020), p 37
161 *"A Twitter user was suspended for 'glorifying violence' after posting exactly what Trump tweets"*, Business Insider, 4 June 2020
162 Q225 [Nick Pickles]
163 Tony Blair Institute (DIS0013); Q8; Q43
164 *"Twitter labeled Trump tweets with a fact check for the first time"*, CNN, 27 May 2020; *"Another Tweet From Trump Gets a Label From Twitter"*, The New York Times, 23 June 2020
165 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020
166 *"Google adds contextual fact-checking for some image search results"*, TechCrunch, 22 June 2020

similar functions, instead tagging all COVID-19-related videos to direct users to trusted information and prioritising takedowns of violative content.[167] In written evidence, Dr. Harith Alani of the Open University called for investment in the development of tools and campaigns to raise awareness of people's exposure to and consumption of COVID-19 misinformation.[168]

47. Facebook has gone further and also developed a 'correct the record' tool to retroactively provide authoritative information to some people who have encountered misinformation. This tool sends notifications in two circumstances:

(1) To users who have previously shared information that has since been debunked, with a link to a fact-checked article; and

(2) To users who have engaged with (i.e. reacted to, shared or commented on) content that Facebook has removed as harmful, with links to the World Health Organisation's myth-busting page.[169]

Medical professionals supported the concept of correct the record tools. Dr. Megan Emma Smith of EveryDoctor observed that such tools would strike a balance between providing authoritative information and protecting freedom of expression:

> We are not saying clamp down and get rid of free speech, but you have to go back and correct it, and hopefully that will go at least some way towards helping those sorts of people who might be getting a bit of a kick out of putting themselves forward as a pseudo-expert, and/or hopefully it will at least flag up for those to whom they are proffering this misinformation that it is not accurate and is not true.[170]

Thomas Knowles, also of EveryDoctor, similarly argued that correcting the record could help discredit disreputable sources as well as provide authoritative information.[171]

48. By design, this tool does not provide notifications to every user that comes across examples of misinformation.[172] Facebook justified this decision so as not "to draw attention to false narratives among people who may not have noticed them". In a second round of correspondence, Facebook added that "it also risks diluting the impact of receiving a notification if it becomes too wide spread and commonplace, which is likely if it's sent to everyone who may have seen this kind of content".[173] Despite these arguments, we noted several times that Facebook measures 'linger time' (i.e. time a user spends looking at a post), and questioned the feasibility of introducing this feature for those who have spent enough time on misleading content or false news to have read it.[174] Other tech companies did not commit to rolling out similar tools on their platforms. Twitter's Nick Pickles, for example, rejected supportive academic research in support of such tools, saying that "a number of studies around correct the record are not peer reviewed".[175] Mr. Pickles added

167 TikTok (DIS0018) p 1
168 Open University (CVD0489) pp.26 and 27
169 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020
170 Q130
171 Q131
172 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020; Qq183–4 [Damian Hinds MP, Monika Bickert]
173 Letter from Derek Slater, Google, and Leslie Miller, YouTube, re evidence follow-up, 19 June 2020
174 *Ibid*
175 Q207 [Nick Pickles]

that "[t]here was a paper in Science earlier this year looking at something similar in Brazil, using the World Health Organisation, and it did not work".[176] We note, however, that the article referenced found that, whilst corrective information did not work for myths about Zika virus, it did decrease false beliefs about yellow fever.[177] Moreover, though the paper (specifically) concluded that "providing accurate factual information does not always have the expected effect on public support for related policies or leaders", it also recommended further research into different myth-busting sources and/or less neutral language about the myths themselves with a more representative sample.[178] Written evidence from Dr. Alani said that though "the publication of fact-checks has a positive impact in reducing the spread of misinformation on Twitter", there needs to be more "interdisciplinary research to assess the performance of current official fact-checks in halting the spread and acceptance of COVID-19 misinformation, and to establish more efficient and effective procedures and tools to boost this performance".[179]

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

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

176 *Ibid*

177 John M. Carey *et al.*, The effects of corrective information about disease epidemics and outbreaks: Evidence from Zika and yellow fever in Brazil, Science Advances, vol. 6, no. 5, (29 January 2020)

178 *Ibid*

179 Open University (CVD0489) pp.26 and 27

3 Public sector response

Public service broadcasters

The turn to public service broadcasting

51. In contrast to the lack and loss of trust in social media as a source of news, evidence has showed that people have turned increasingly to public service broadcasters (PSBs) during the crisis. Weekly research commissioned by Ofcom has found that, by week 12 of the UK lockdown, 60% of people felt that broadcasters were their most important source of news. 84% had turned to broadcasters for news in the previous week.[180] This is supported by PSB viewing figures. In the week of 23 March, for instance, BBC TV Network News reached 44 million people, the highest number since the 2003 Iraq War.[181] Channel 4's COVID-19 documentaries reached 9.9 million, including over 10% of 16–34s and over 15% of audiences described as 'BAME'.[182] Between 23 March and 16 April, BBC One special broadcasts reached almost two-thirds of the UK population;[183] over the month of March, Channel 4 News was watched by almost one-quarter.[184] Viewership increases have extended to regional news, radio and BBC News Online, the latter of which attracted 84 million unique views in the week commencing 16 March, far exceeding the previous record of 52 million set during the 2019 general election.[185]

52. Written and oral evidence argued that the role of regulation was significant in the turn to public service broadcasting. Stacie Hoffmann argued that social media regulation should be as robust as that applied to broadcasting, and should follow similar principles: "[i]t is a completely different ecosystem […], but there definitely should be the same expectations and the same kind of levels of restrictions or expectations on the actors involved as there is in current regulations for traditional media".[186] Campaign group Hacked Off, however, argued that regulation should be more robust than the self-regulatory regime overseen by IPSO.[187] Dr. Megan Emma Smith posited that:

> I would say that the print media and the television media are regulated and have obligations. If some of this misinformation appeared in their pages or on their screens, steps would be taken. Why should these other platforms be any different? I completely appreciate that they do not write the lies, they do not compose the lies, but they do facilitate the distribution of them, and that is what we have to get rid of.[188]

53. Channel 4's submission posits three reasons for people's choice of PSBs in particular over social media.[189] First, the UK supports a diverse PSB ecosystem with different funding models, missions and purposes. Second, these organisations are held accountable by "an independent system of regulation" with real powers to sanction and "strict rules on accuracy

180 Ofcom, 'COVID-19 news and information: consumption and attitudes,' accessed 25 June 2020
181 BBC (DIS0012) para 13
182 Channel 4 (DIS0016) para 3.14
183 BBC (DIS0012) para 23
184 Channel 4 (DIS0016)
185 BBC (DIS0012) para 3.11
186 Q27
187 Hacked Off (DIS0014)
188 Q125
189 Channel 4 (DIS0016) paras 3.6–7

and due impartiality and other detailed content standards".[190] Finally, these rules include "a clear set of quotas and requirements for the provision of high quality news and current affairs".[191] In oral evidence, Channel 4 chief executive Alex Mahon asserted explicitly that there has been "an increasing consumer awareness, and one might say backlash, against disinformation and misinformation", particularly where "misinformation and disinformation are remaining on the tech platforms and, in some cases, being prioritised by them", and called for "public service content [to have] a prioritised, prominent position across all these platforms".[192] YouTube maintained that it does act to support quality news, "to make sure that we are promoting their content in our top news shelf, the breaking news shelf, so we are exposing users to these outlets and helping drive traffic accordingly" (though it did not comment specifically on PSB prominence).[193]

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

Beyond broadcasting

55. We also found that PSBs have contributed to efforts to tackle misinformation and disinformation through other initiatives, both collaboratively and internally. Last year, the BBC set up the Trusted News Initiative (TNI) with the largest tech companies, global media organisations and independent researchers,[194] with the specific aims of flagging disinformation during elections, sharing learning and promoting media education.[195] Through the TNI, news organisations have put in place a shared alert system "so that content can be reviewed promptly by platforms"[196] (though Facebook have stressed that it interprets this is an "information sharing exercise" rather than a "technical implementation by any party into each other's systems").[197] We are interested whether and how this will need to adapt in response to the emergence of new platforms, such as TikTok, and new online behaviours associated with its distinct functionality and user base. The BBC also emphasises the work of its in-house BBC Monitoring disinformation team, Beyond Fake News team, User Generated Content Hub and Young Reporter project, which have separately undertaken and published research into disinformation and sought to improve media literacy for audiences in concert with the objectives of the TNI.[198] Finally, both the BBC and Channel 4 contribute work alongside the fact-checking community (such

190 *Ibid*, para 3.7
191 *Ibid*
192 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 16 June 2020, HC (2019–21) 156, Qq84, 89
193 Q151 [Leslie Miller]
194 The partners within the TNI are: (from traditional media) the BBC, Agence France-Presse, Reuters, European Broadcasting Union, Financial Times, Wall Street Journal, the Hindu and CBC/Radio-Canada; (from tech) Facebook, Google/YouTube, Twitter and Microsoft; and (from the research community) First Draft and the Reuters Institute for the Study of Journalism.
195 *Trusted News Initiative announces plans to tackle harmful Coronavirus disinformation*, BBC Press Office, 27 March 2020
196 BBC (DIS0012) para 42
197 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020
198 BBC (DIS0012)

as Full Fact) via BBC Reality Check, BBC Trending[199] and Channel 4 News' Coronavirus FactCheck.[200] The BBC shared with us several instances of misinformation that it has tackled, such as defective directions for homemade sanitiser and scam vaccine adverts originating in Italy, claims by the South China Morning Post that raw garlic prevents infection, and an investigation into the origins of social media posts.[201]

56. The potential role of BBC and Channel 4 in fact-checking is great—the former thanks to their overall brand, the latter having been an early innovator with Channel 4 FactCheck. Whilst there are now a number of other fact-check organisations, none can claim nearly the same brand equity in the UK.

57. We asked Facebook and Google about how the Trusted News Initiative has fed into their efforts. Facebook offered a somewhat lukewarm response, noting that the TNI group has met once a week and described the channel as "a valuable additional potential signal for misinformation on which we can, where appropriate, take action".[202] Google, meanwhile, stressed that "this partnership builds on our existing efforts to ensure authoritative information, including the work of fact checkers, is surfaced on our platforms" and committed to supporting First Draft, a TNI partner, as part of its $6.5 million investment in fact-checking through the Google News Initiative.[203] However, it struck us that this engagement could go further, such as whether there was any scope to give TNI partners access to WhatsApp accounts or automated features such as information bots that had been provided to the WHO, International Fact-Checking Network and Public Health England.

58. **Resources developed by public service broadcasters such as the Trusted News Initiative show huge potential as a framework in which public and private sector can come together to ensure verified, quality news provision. However, we are concerned that tech companies' engagement in the initiative is limited. Facebook, for example, has chosen not to provide TNI partners with accounts on WhatsApp, which could otherwise provide an independent but robust source of information of Government and public health advice. *The Government should support the BBC to be more assertive in deepening private sector involvement, such as by adapting the Trusted News Initiative to changes in the social media ecosystem such as the emergence of TikTok and other new platforms. The Government and online harms regulator should use the TNI to 'join up' approaches to public media literacy and benefit from shared learning regarding misinformation and disinformation. It should do this in a way that respects the independence from Government and expertise of the group's members, and not impose a top-down approach.***

UK Government

Counter Disinformation Unit

59. When we asked the Secretary of State about the steps being taken against misinformation, he described the Department's principal work as "both to understand

199 *Ibid*, para 46
200 Channel 4 (DIS0016) para 3.12
201 BBC (DIS0012)
202 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020
203 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020

the nature of what is going on and, in the process of that, to occasionally identify false narratives and things that the social media companies will take action to take down".[204] On 9 March, the Secretary of State announced his intention to re-establish the DCMS-led Counter Disinformation Unit, bringing together existing capability and capacity across government,[205] to "help provide a comprehensive picture on the potential extent, scope and impact of disinformation".[206] Later that month, the Government announced that its Rapid Response Unit, which feeds into the DCMS Counter Disinformation Unit, would be tackling "[u]p to 70 incidents a week".[207] The announcement cited several responses where false narratives were identified, including "direct rebuttal on social media, working with platforms to remove harmful content and ensuring public health campaigns are promoted through reliable sources".[208]

60. Throughout our inquiry, we raised concerns as to whether the Department has used its capability in the most effective way. On 11 March, we wrote to the Secretary of State to express support, but also ensure that the Counter Disinformation Unit was being resourced effectively.[209] In response, the Secretary of State wrote that "capability is resourced full time through existing cross-government teams and there are no additional costs associated with it" as "existing structures had been monitoring for disinformation related to the disease as part of their ongoing work prior to this".[210] The letter committed to channelling outputs from the Counter Disinformation Unit to COBR through the Secretary of State and to "looking at ways to actively engage harder to reach groups".[211]

61. There are lots of independent factchecking organisations already up and running. Public service broadcasters have several dedicated factchecking teams. Facebook[212] and Google[213] have themselves also provided funding to independent factcheckers. Full Fact has worked for several years as part of Facebook's Third Party Fact Checking programme, and has monitored and rebuffed misleading claims that have been circulated on WhatsApp, Twitter and in the mainstream media, submitted by the public directly through an online form, or made by public figures (including parliamentarians).[214] Indeed, the Government's own webpage for its 'Don't Feed The Beast' campaign against disinformation directs users to the Full Fact website alongside links to the NHS and GOV.UK sites.[215] It remains, however, unclear as to how the Government engages with factcheckers like Full Fact, or disseminates its own information to frontline health services such as NHS 111 (or if these efforts are being duplicated by the health service as well). Dr. Megan Emma Smith recommended that factchecking be demonstrably independent and speciality-specific, noting the tension created by Government factchecking:

204 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q18

205 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Q381

206 *"Coronavirus: Unit set up to counter false claims"* , BBC News, 9 March 2020

207 *"Government cracks down on spread of false coronavirus information online"*, Cabinet Office and Department for Digital, Culture, Media and Sport press release, 30 March 2020

208 *Ibid*

209 Letter from Chair to Rt. Hon. Oliver Dowden MP, Secretary of State for DCMS, re. Coronavirus disinformation, 11 March 2020

210 Letter from Rt Hon Oliver Dowden MP, Secretary of State for DCMS, re Coronavirus disinformation, 27 March 2020

211 *Ibid*

212 Letter from Richard Earley, Facebook, re evidence follow-up, 14 May 2020

213 Letter from Alina Dimofte, Google, re evidence follow-up, 11 May 2020

214 Full Fact (DIS0006) p 1

215 GOV.UK, 'Be careful what you share. Things aren't always what they seem online.' accessed 24 June 2020

> It puts politicians in an incredibly difficult position because it is an easy and, if I can say so, slightly low blow to come back at you and say, "You are politicians, you are the Government. Of course you have a vested interest in this." It needs to be objective and it needs to be independent, and demonstrably so.[216]

62. Expert evidence we received has recommended where Government could add value, instead of duplicating existing efforts, particularly in the absence of online harms legislation. Professor Philip Howard, who described the Government response as "strong, and it needs to be stronger", urged the Department to help provide independent researchers with more data, to help understand the scope and scale of the problem:

> The best data we have is months old, it is not quite adequate and does not cover all the features that these social media platforms provide. The misinformation initiatives that the Government have are very important because you have the authority to collect and collate and analyse information in the public interest and the firms don't act in the public interest. Independent researchers like myself, at [the Oxford Internet Institute], or investigative journalists, don't have access to the same levels of information—the levels of information that we need to help fight this.[217]

Professor Howard specifically called for more representative samples of data on the comprehensive activity of suspicious accounts or those that have been removed, particularly where this might imply foreign interference.[218]

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

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

216 Q131
217 Q5
218 Q6

Engagement with social media companies

65. Beyond leading the Counter Disinformation Unit, the DCMS has also led on engagement with the tech companies themselves. When pressed, Ministers have been bullish about the contribution of Big Tech in tackling misinformation; on 22 April, for example, the Secretary of State paid tribute to the number of different announcements from tech companies, saying "I have been impressed with how they have stepped up to the plate as part of a national and, indeed, international effort to address misinformation at this time of crisis".[219] The Minister for Digital, similarly, told the House of Lords Select Committee on Democracy and Digital Technologies that "the platforms that we are dealing with have been excellent at addressing concerns that we raise but have also come forward with ways of raising them themselves".[220]

66. Tech companies have reciprocated. TikTok told us that it welcomed steps taken by the Government's Rapid Response Unit and digital literacy campaign and "encourage Government to continue its engagement with industry as we work collectively to tackle the important area of [disinformation] and misinformation on COVID-19 and other issues that may arise in the future".[221] Google, in its second session with the Committee, noted that "we benefit from interactions like this and from cooperation with Government in continuing to improve".[222] All companies from whom we took evidence emphasised their support for the Government's efforts. Facebook,[223] Twitter[224] and TikTok[225] stated in evidence that they had provided the Government with *pro bono* advertising credit on their platforms (though ministers did not mention this to us in evidence, and we are not party to how these credits are being used). Facebook,[226] Google,[227] Twitter[228] and TikTok[229] all also asserted that they had amplified Government messaging on its platforms through various information hubs, adjusted search results and other platform-specific features.

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

Offline solutions

68. Written evidence we received emphasised the need for a comprehensive digital literacy, community engagement and school education programme. Our predecessor Committee's Interim Report into *Disinformation and 'fake news'* called for digital literacy

219 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Qq18, 27
220 Oral evidence taken before the Select Committee on Democracy and Digital Technologies on 12 May 2020, HL (2019–21) 77, Q331
221 TikTok (DIS0018) p 5
222 Q135
223 Qq94, 177
224 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
225 TikTok (DIS0018) p 5
226 Qq92, 94
227 Q135
228 Letter from Katy Minshall, Twitter, re evidence follow-up, 11 May 2020
229 TikTok (DIS0018) p 5

to be the 'fourth pillar' of education alongside reading, writing and maths.[230] Protection Approaches, for instance, recommend that online strategies to tackle misinformation are matched by investment in offline interventions, arguing that "offline solutions to online harms remain startingly absent from policy and civil society efforts".[231] Their submission urges the Government to provide immediate resources for local community groups and schools and upskill and build capacity amongst grassroots organisations.[232] Glitch, similarly, called on the Government to provide education and resources on digital citizenship and online safety, consult with women's organisations about risks to women, and provide guidance to employers about the risks of online harassment and abuse in the workplace.[233] The Government, in its interim consultation response, claimed that it would produce a media literacy strategy this summer to "ensure a co-ordinated and strategic approach to online media literacy education and awareness for children, young people and adults", though at the point of writing we are still awaiting its publication.[234]

69. **The Government had committed to publishing a media literacy strategy this summer. We understand the pressures caused by the crisis, but believe such a strategy would be a key step in mitigating the impact of misinformation, including in the current pandemic.** ***We urge the Government to publish its media literacy strategy at the latest by the time it responds to this Report in September. We welcome the non-statutory guidance from the Department for Education on 'Teaching online safety in school' (June 2019),[235] bringing together computing, citizenship, health and relationships curricula, which among other things covers disinformation and misinformation. We ask that the Government reports on adoption of this material before the end of the academic year 2020/1.***

Implication for online harms

70. Despite the Secretary of State and Minister for Digital's positive assessment of companies' efforts in tackling misinformation, Ministers have elsewhere downplayed the possibilities offered by online harms legislation. In one instance, when asked if tech companies are doing enough to tackle false information, Lords Minister Baroness Williams appeared to justify the lack of action by tech companies: "The thing about the online world is that quite often it is reactive. Unless it is illegal, it is very difficult to make it proactive."[236] This statement, however, was then immediately contradicted by the Minister for Digital, who subsequently stated that she had "seen some really good proactive work" from Facebook, Twitter and Google to tackle misinformation that "now shows that it is possible for platforms to work at great speed and with great integrity to address some of these concerns".[237]

230 Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report, fifth report of the session 2017–19, 29 July 2018, HC 363, para 246
231 Protection Approaches (DIS0011)
232 *Ibid*
233 Glitch (CVD0296) pp.8, 11, 22, 34
234 Department for Digital, Culture, Media and Sport and Home Office, Online Harms White Paper - *Online Harms White Paper - Initial consultation response*, 12 February 2020
235 Department for Education, *Teaching online safety in school*, (June 2019)
236 Oral evidence taken before the Home Affairs Committee on 13 May 2020, HC (2019–21) 232, Q 515
237 *Ibid*, Q516

71. Moreover, the Government has stated several times that online harms legislation will aim to hold companies "to what they have promised to do and to their own terms and conditions".[238] The Minister for Digital, however, has acknowledged the limits to this approach, particularly for misinformation and disinformation, stating that, "[i]n many cases, it does not actually contradict some of the platforms' standards or regulations".[239] Moreover, statements elsewhere implied that in several instances, existing terms and conditions were not fit for purpose, as the Secretary of State himself stated that the Department had been working to improve the robustness of companies' terms and conditions, claiming that "[w]e are working with them to understand and beef up their systems and how they as social media companies take action in respect of misinformation".[240] Dame Melanie Dawes, chief executive of Ofcom, set out the drawbacks for such an approach in oral evidence in June:

> What I would say is that, although there are some sensible steps being taken, there is no transparency about it. There is no overall standard that has been set. It is very hard for parents to know what sort of risks their children are exposed to and how they are being managed by the platforms, because we cannot police what our children are doing all day.[241]

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

Ofcom

73. Throughout our inquiry, the Government emphasised that decisions about the scope of regulation for so-called 'harmful but legal' content should fall to the regulator. For example, in response to a question on the balance of illegal harms and 'harmful but legal' in legislation, the Minister for Digital said:

> Within the legislation, the only things that we are setting out are things that are illegal, so child sexual exploitation and terrorism are the two things that are mentioned on the face of the Bill, as far as I understand it at the moment. On the things that are what you describe as legal but harmful, Ofcom is the regulator here and that will be something it will lay down. We are not going to specify what those harms are.[242]

238 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q20

239 Oral evidence taken before the Select Committee on Democracy and Digital Technologies on 12 May 2020, HL (2019–21) 77, Q339

240 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 22 April 2020, HC (2019–21) 157, Q18

241 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 June 2020, HC (2019–21) 439, Q8

242 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 9 June 2020, HC (2019–21) 291, Q380

74. However, the Government's position was rebuffed by Ofcom in oral evidence several weeks later, when we asked Dame Melanie Dawes about the harms in scope. When asked about the appropriate balance in legislation between illegal content and 'harmful but legal' content, Dame Melanie said:

> If we are appointed, we will work with whatever regime Parliament decides. These are quite important questions for Ministers and Parliament to determine.[243]

Regarding the outcome of this inquiry, Dame Melanie stated that the "online harms regime will need to answer the question as to whether or not disinformation, in particular, is covered".[244] However, Dame Melanie did note that, despite the overall scope of legislation being within the purview of Parliament, Ofcom would require flexibility and discretion as a matter of practicality when enforcing the regime.[245] Ofcom was also reluctant to describe the powers it might need to enforce the regime beyond financial penalties, saying that "[i]t would be presumptuous of me to ask for detailed power for a regime that we have not yet been asked to operate".[246] Regarding criminal sanction, which our predecessor called for as a last resort, Dame Melanie noted that "criminal sanction for criminal activities is incredibly important" but commented that it would be a relatively unique power across its other remits.[247]

75. Dame Melanie did argue that Ofcom needed to "deepen our understanding" of some specific harms,[248] but emphasised Ofcom's "good track record of using other people's research, as well as commissioning our own".[249] Regarding the practicalities of identifying harms, Dame Melanie described the need to work with tech companies to identify issues:

> The regulator will need access to data from the operators, and we would expect to be able to publish information about what is going on and what actions are being taken. With the scale of this, we are going to have to rely on the companies themselves to do a lot of the heavy lifting, but then the regulator's job will be to shine a light, to hold them to account and to investigate if there are issues that suggest not all is as it should be.[250]

Oral and written evidence also emphasised the need to engage with tech companies to test new functions. Dr. Claire Wardle of First Draft told us she "would like to see is the platforms do more but then allow academics to test alongside them to see what the effects are".[251] Evidence from Dr. Nejra van Zalk from Imperial College London also described how 'road testing' code has helped understand the impact of digital technologies and innovations on children and young people before they are released to the public.[252]

243 Oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 June 2020, HC (2019–21) 439, Q6
244 *Ibid*, Q24
245 *Ibid*, Q10; also Qq6–7, 14–5, 18, 21, 36, 39
246 *Ibid*, Q4, 25–8, 35
247 *bid*, Q37
248 *Ibid*, Q15
249 *Ibid*, Q22
250 *Ibid*, Q9
251 Q33
252 Dr Nejra van Zalk (DIS0020)

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

77. We have also raised concerns that social media may be allowing third parties to exploit gaps in regulation. In correspondence with Dame Melanie, we raised concerns that Press TV had been using social media platforms to circumvent the revocation of its broadcasting licence in 2012[253] until its UK YouTube channel was deleted by YouTube unilaterally in January 2020 for going against its policies.[254] Finally, in oral evidence we raised the issue that vendors of the harmful Miracle Mineral Solution and other hoax cures have exploited gaps in foods standards and medicine regulations on social media, making it difficult to compel tech companies to take action at scale against them.[255] We have noted that the Competition and Markets Authority, Information Commissioner's Office and Ofcom have recently launched a 'Digital Regulation Cooperation Forum' to strengthen collaboration and co-ordination between them.

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

253 Letter from the Chair to Dame Melanie Dawes, Chief Executive, Ofcom, re Misinformation about the COVID-19 crisis, 6 April 2020

254 *"Google deletes Press TV UK's YouTube account"*, Middle East Eye, 14 January 2020

255 Qq133–4

Conclusions and recommendations

Introduction

1. We are pleased that the Government has listened to our predecessor Committee's two headline recommendations, and that it will launch a duty of care and an independent regulator of online harms in forthcoming legislation. However, we are very concerned about the pace of the legislation, which may not appear even in draft form for over two years since the White Paper was published in February 2019. *We recommend that the Government publish draft legislation, either in part or in full, alongside the full consultation response this autumn if a finalised Bill is not ready. Given our ongoing interest and expertise in this area, we plan to undertake pre-legislative scrutiny. We also remind the Government of our predecessor Committee's recommendation for the DCMS Committee to have a statutory veto over the appointment and dismissal of the Chief Executive to ensure public confidence in their independence, similar to the Treasury Committee's veto over senior appointments to the Office of Budget Responsibility, and urge the Government to include similar provisions in the Bill*. (Paragraph 12)

2. Online harms legislation must respect the principles established in international human rights law, with a clear and precise legal basis. Despite the Government's intention that the regulator should decide what 'harmful but legal' content should be in scope, Ofcom has emphasised repeatedly that it believes this is a matter for Parliament. Parliamentary scrutiny is necessary to ensure online harms legislation has democratic legitimacy, and to ensure the scope is sufficiently well-delineated to protect freedom of expression. *We strongly recommend that the Government bring forward a detailed process for deciding which harms are in scope for legislation. This process must always be evidence-led and subject to democratic oversight, rather than delegated entirely to the regulator. Legislation should also establish clearly the differentiated expectations of tech companies for illegal content and 'harmful but legal'*. (Paragraph 16)

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

Tech companies' response

4. The need to tackle online harms often runs at odds with the financial incentives underpinned by the business model of tech companies. The role of algorithms in incentivising harmful content has been emphasised to us consistently by academia and by stakeholders. Tech companies cited difficulties in cases of 'borderline content' but did not fully explain what would constitute these cases. Given the central role of algorithms in surfacing content, and in the spread of online harms

such as misinformation and disinformation in particular, it is right that the online harms regulator will be empowered to request transparency about tech companies' algorithms. *The Government should consider how algorithmic auditing can be done in practice and bring forward detailed proposals in the final consultation response to the White Paper.* (Paragraph 20)

5. The current business model not only creates disincentives for tech companies to tackle misinformation, it also allows others to monetise misinformation too. *To properly address these issues, the online harms regulator will need sight of comprehensive advertising libraries to see if and how advertisers are spreading misinformation through paid advertising or are exploiting misinformation or other online harms for financial gain. Tech companies should also address the disparity in transparency regarding ad libraries by standardising the information they make publicly available. Legislation should also require advertising providers like Google to provide directories of websites that they provide advertising for, to allow for greater oversight in the monetisation of online harms by third parties.* (Paragraph 24)

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

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

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

9. *Alongside developing its voluntary codes of practice for child sexual exploitation and abuse and terrorist content, the Government should urgently work with tech companies to develop a voluntary code of practice to protect citizens from the harmful*

impacts of misinformation and disinformation, in concert with academics, civil society and regulators. A well-developed code of practice for misinformation and disinformation would be world-leading and will prepare the ground for legislation in this area. (Paragraph 34)

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

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

12. The pandemic has demonstrated that misinformation and disinformation are often spread by influential and powerful people who seem to be held to a different standard to everyone else. Freedom of expression must be respected, but it must also be recognised that currently tech companies place greater conditions on the public's freedom of expression than that of the powerful. *The new regulator should be empowered to examine the role of user verification in the spread of misinformation and other online harms, and should look closely at the implications of how policies are applied to some accounts relative to others.* (Paragraph 45)

13. We recognise tech companies' innovations in tackling misinformation, such as 'correct the record' tools and warning labels. We also applaud the role of independent fact-checking organisations, who have provided the basis for these tools. These contributions have shown what is possible in technological responses to misinformation, though we have observed that often these responses do not go far enough, with little to no explanation as to why such shortcomings cannot be addressed. Twitter's labelling, for instance, has been inconsistent, while we are concerned that Facebook's corrective tool overlooks many people who may be exposed to misinformation. For users who are known to have dwelt on material that

has been disproved and may be harmful to their health, it strikes us that the burden of proof should be to show why they should not have this made known to them, rather than the other way around. (Paragraph 49)

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

Public sector response

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

16. Resources developed by public service broadcasters such as the Trusted News Initiative show huge potential as a framework in which public and private sector can come together to ensure verified, quality news provision. However, we are concerned that tech companies' engagement in the initiative is limited. Facebook, for example, has chosen not to provide TNI partners with accounts on WhatsApp, which could otherwise provide an independent but robust source of information of Government and public health advice. *The Government should support the BBC to be more assertive in deepening private sector involvement, such as by adapting the Trusted News Initiative to changes in the social media ecosystem such as the emergence of TikTok and other new platforms. The Government and online harms regulator should use the TNI to 'join up' approaches to public media literacy and benefit from shared learning regarding misinformation and disinformation. It should do this in a way that respects the independence from Government and expertise of the group's members, and not impose a top-down approach.* (Paragraph 58)

17. The Government should reconsider how the various teams submitting information to the Counter Disinformation Unit best add value to tackling the infodemic. Factchecking 70 instances of misinformation a week duplicates the work of other organisations with professional expertise in the area. *Instead, the Government should focus on opening up channels with organisations that verify information in a 'Factchecking Forum', convened by the Counter Disinformation Unit, and share instances that are flagged by these organisations across its stakeholders, including and especially to public health organisations and all NHS trusts, key and/or frontline*

workers and essential businesses to prepare them for what they may be facing as a direct result of misinformation, allowing them to take appropriate precautions. (Paragraph 63)

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

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

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

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

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

also believe that the regulator should facilitate independent researchers 'road testing' new features against harms in scope, to assure the regulator that companies have designed these features ethically before they are released to the public. (Paragraph 76)

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

Formal minutes

Thursday 16 July 2020

Julian Knight, in the Chair

Kevin Brennan	Rt Hon Damian Hinds
Julie Elliott	John Nicolson
Rt Hon Damian Green	

Draft Report (*Misinformation in the COVID-19 Infodemic*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 78 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Second Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No.134.

[Adjourned till Monday 20 July at 4.00 p.m.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Thursday 30 April 2020

Stacie Hoffmann, Digital Policy and Cyber Security Consultant, Oxford Information Labs; **Professor Philip N. Howard**, Director, Oxford Internet Institute; **Dr Claire Wardle**, Co-Founder and Director, First Draft News	Q1–46
Katy Minshall, UK Head of Government, Public Policy and Philanthropy, Twitter; **Richard Earley**, UK Public Policy Manager, Facebook; **Alina Dimofte**, Public Policy and Government Relations Manager, Google	Q47–113

Thursday 04 June 2020

Thomas Knowles, Paramedic; **Dr Megan Emma Smith**, Consultant Anaesthetist	Q114–134
Leslie Miller, Vice-President of Government Affairs and Public Policy, YouTube; **Derek Slater**, Global Director of Information Policy, Government Affairs and Public Policy, Google	Q135–161
Monika Bickert, Head of Product Policy and Counterterrorism, Facebook	Q162–194
Nick Pickles, Director of Public Policy Strategy, Twitter	Q195–231

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

DIS numbers are generated by the evidence processing system and so may not be complete.

1 AFP (DIS0002)

2 BBC (DIS0012)

3 British Telecom (DIS0017)

4 Channel 4 (DIS0016)

5 Clean up the Internet (DIS0008)

6 M Fernandez-Barham (DIS0003)

7 Frontline healthcare professionals (DIS0019)

8 Full Fact (DIS0006)

9 Global Partners Digital, Index on Censorship, Open Rights Group, and Article 19 (DIS0005)

10 Gorman, Mr Adam (DIS0001)

11 Hacked Off (DIS0014)

12 Henry Jackson Society (DIS0010)

13 Office for Statistics Regulation (DIS0015)

14 The Pirbright Institute (DIS0009)

15 Protection Approaches (DIS0011)

16 TikTok (DIS0018)

17 Tony Blair Institute for Global Change (DIS0013)

18 Van Zalk, Dr Nejra (DIS0020)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2019–21

First Report	The Covid-19 crisis and charities	HC 281
First Special Report	BBC Annual Report and Accounts 2018–19: TV licences for over 75s: Government and the BBC's Responses	HC 98
Second Special Report	The Covid-19 crisis and charities: Government Response to the Committee's First Report of Session 2019–21	HC 438