EMC Submission No. 95
Received 30 September 2020

Dear Members of the Electoral Matters Committee,

Thank you for the opportunity to contribute to your inquiry into 'the Impact of Social Media on Elections and Electoral Administration'.

We hope the following submission can provide some insights into the recommendations made by this Committee and its predecessor to the UK Government following similar inquiries we have conducted, and how the Government and relevant regulators have acted in response. We have seen welcome commitments to address some of the issues caused by tech companies and will continue to scrutinise the Government where it has been slow to act against others.

As demonstrated by the work of both of our Committees, these are global issues. We are committed to working with fellow parliamentarians across the world, including on the International Grand Committee, which was first convened by the DCMS Committee in November 2018. A holistic and international approach is the only way we can ensure that these multinational tech firms are scrutinised and held accountable regarding their influence on our democracy and society.

The impact of social media

The debate regarding the precise extent and nature of the impact of social media on citizens during elections has been significant and fast-moving, be it in academic, policy and popular discourse. Given the breadth of this debate, undertaking a literature review in order to make a definitive judgement is beyond the scope of our role and remit, and will be covered in depth in other submissions to your inquiry. What we have found through our investigations into the topic is that, irrespective of whether certain techniques employed by bad-faith actors are effective, these techniques go against the principles of electoral law and thus demonstrate that our regulatory frameworks that protect free and fair elections from interference are not fit for the digital age.

Regardless, many people, from academics to civil society to parliamentarians and the Government have recognised the need to address specific vulnerabilities in electoral law that were created, exploited or exacerbated by social media. On 5 November 2019, the then-Cabinet Office Minister (and current Secretary of State for Digital, Culture, Media and Sport) provided an update on several measures. This included new legislation to tackle online abuse of public figures such as parliamentary candidates (through the Online Harms Bill), a regime on digital imprints and a cross-Government 'Defending Democracy Programme', which aims to "protect and secure UK democratic processes, systems and institutions from interference, including from cyber, personnel and physical threats; strengthen the integrity of UK elections; encourage respect for open, fair and safe democratic participation; and promote fact-based and open discourse, including online".[1] However, only a consultation on digital imprints has been forthcoming.

Our recommendations to Government

The first Report of our Sub-Committee on Online Harms and Disinformation discussed the business models underpinning tech companies' social media platforms. These companies generate revenue primarily through advertising, targeted at users based on quantified tastes and preferences (both observed and inferred), which is maximised by increasing metrics such as total and active user numbers, data collection, average user time and user personalisation.[2] This business model creates potential disincentives to take action against content, users or adverts that generate engagement,

[1] HC Deb 5 November 2019 HCWS100

[2] Digital, Culture, Media and Sport Committee, Misinformation in the COVID-19 Infodemic, 21 July 2020, HC 234 2020-21, para 18

user data and advertising revenue even where it might be otherwise considered personally or socially harmful (such as disinformation or misinformation). Moreover, tech companies have funded false narratives by allowing purveyors of misinformation and disinformation to use monetisation functions like Super Chats on YouTube.[3] Otherwise, tech companies like Google and Amazon have placed advertising on the websites of purveyors of misinformation and disinformation (independently of advertising targeted at users on their own platforms), with no transparency as to which websites are having advertising delivered by tech companies in this way.[4]

Of course, tech companies such as Facebook and YouTube rejected this characterisation, claiming that their aim is to drive "meaningful social interaction" and that "this type of borderline content … reflects less than 1% of the totality".[5] Moreover, tech companies have downplayed the impact of political advertising on revenues. Mark Zuckerburg has claimed that political adverts generate only 0.5% of Facebook's yearly revenue (an estimated US $330-400 million).[6] Twitter has gone further by banning political advertising outright, though it only earned US $3 million, or 0.1% of total revenue, in the 2018 mid-term elections.[7] Indeed, in his reasoning for the ban, Jack Dorsey implicitly criticised Facebook's position, and could be considered a relatively low-cost opportunity to put pressure on a competitor. Regardless, we would respond that minimising the issues around political advertising does not help mitigate them. Moreover, the differences between tech companies in their approaches demonstrates the lack of any systemic response led by the sector.

From our most recent report, we made several recommendations, arguing that the Government should:

- require tech companies "to have easy-to-use user reporting systems and the capacity to respond to these in a timely fashion" with "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)";

- empower regulators 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";

- consider how algorithmic audits and oversight of tech companies' platform architecture could be done in practice, require advertising libraries to be standardised across all platforms and require relevant companies to include information on what websites are also having advertising placed and what these adverts are;

- "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";

- give regulators the power to disrupt business activity of non-compliant sentences and bring criminal sanctions against individuals where there is significant evidence of criminal wrongdoing;

[3] *Ibid*, para 31
[4] *Ibid*, para 23
[5] *Ibid*, para 19
[6] "Zuckerberg defends politician ads that will be 0.5% of 2020 revenue", TechCrunch (30 October 2019)
[7] *Ibid*

- “facilitate independent researchers ‘road testing’ new features” to ensure that they are ethically designed; and

- create and operate its own searchable advertising archive “to provide transparency, oversight and scrutiny” and “to demonstrate best practice”.[8]

Our report also recognised the need for robust offline responses, to ensure that all citizens can readily access authoritative information and recognise misinformation and disinformation where it appears. We noted the need for robust literacy strategies to equip citizens with the tools to use the internet safely and responsibly, and urged the Government to publish its promised media literacy strategy by the time it responded to our Report and to report on the adoption of material set out in its non-statutory guidance on ‘Teaching online safety in school’. Moreover, we called on Government to support public service broadcasters in their engagement with the public sector through the ‘Trusted News Initiative’ to join up approaches to public media literacy and share learnings on misinformation and disinformation easier.

Our investigations into the ongoing provision of quality news content and journalism (amongst other issues) will continue through our current inquiry into ‘The Future of Public Service Broadcasting), where we have taken evidence from a variety of organisations including the BBC, Sky and other UK broadcasters, Netflix, academics and the public.[9]

Predecessor Committee’s recommendations

Our predecessor Committee’s inquiry into ‘Disinformation and “fake news”’ also explored issues created by tech companies for elections. The inquiry took evidence from representatives from the major tech companies and various other contributors to the debate around social media and elections. It also convened the first International Grand Committee on Disinformation, which gathered representatives from parliaments across the world to put pressure on tech companies to act. After the inquiry concluded, the Committee established a Sub-Committee on Disinformation to become Parliament’s institutional home for matters regarding the intersection of tech, elections and online harms.

The Committee’s Interim and Final Report both stated emphatically that “Electoral law in this country is not fit for purpose for the digital age”[10] and “needs to be changed to reflect changes in campaigning techniques”.[11] Moreover, it recognised that tech companies cannot claim merely to operate ‘platforms’, with no role in content dissemination, curation and moderation. Instead, it urged the Government to ensure that “a new category of tech company is formulated, which tightens tech companies’ liabilities, and which is not necessarily either a ‘platform’ or a ‘publisher’”.[12] It also made several specific recommendations to address areas that have been exploited through social media:

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

[8] Digital, Culture, Media and Sport Committee, Misinformation in the COVID-19 Infodemic, 21 July 2020, HC 234 2020-21

[9] “The future of public service broadcasting”, Digital, Culture, Media and Sport Committee (accessed 24 September 2020)

[10] Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report, 24 July 2018, HC 363 2017-19, para 45

[11] Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Final Report, 14 February 2019, HC 1791 2017-19, para 211

[12] *Ibid*, para 13

- Require a duty to act against fake accounts, and properly account for the number of such accounts, given the potential both to damage the user experience but also to defraud advertisers;

- The Government should ban "micro-targeted political advertising to [lookalike audiences] online, and a minimum limit for the number of voters sent individual political messages should be agreed, at a national level" and "explore ways of regulating on the use of external targeting on social media platforms, such as Facebook's Custom Audiences";

- "The Government should carry out a comprehensive review of the current rules and regulations surrounding political work during elections and referenda including: increasing the length of the regulated period; defining what constitutes political campaigning; and reducing the time for spending returns to be sent to the Electoral Commission";

- Modernising the Electoral Commission's powers, including:

    - "the legal right to compel organisations that they do not currently regulate, including social media companies, to provide information relevant to their inquiries";

    - Increasing the "current maximum fine limit of £20,000" and allowing it to levy fines "based on a fixed percentage of turnover, in line with powers already conferred on other statutory regulators";

    - "the ability … to intervene or stop someone acting illegally in a campaign if they live outside the UK"

- A searchable repository of political advertising; and

- "a Code of Practice, which highlights the use of personal information in political campaigning and applying to all data controllers who process personal data for the purpose of political campaigning", underpinned by primary legislation to bring it into statute.[13]

Following the publication of the Online Harms White Paper, our predecessor's Sub-Committee published a further Report in response to address a particular gap in the regulatory proposals regarding political activity on social media during election campaigns.[14] The Report highlighted the need for urgent legislation and codes of practice against disinformation during election periods, for digital spending during campaigns and for searchable advert repositories, as well as an expansion of the powers and funding of the Information Commissioner's Office and Electoral Commission.

Government responses to date

The UK Government's Online Harms regime is a proposed legislative framework aiming to keep users safe online from harmful content by regulating digital platforms' systems under a duty of care. The regime addresses the gap in existing regulation of the use of data, service design and broadcast content through the Data Protection Act 2018, GDPR, Secure by Design agenda, Age Appropriate Design Code and the broadcast code. The Online Harms White Paper recognised the "real danger" of

[13] *Ibid*

[14] Digital, Culture, Media and Sport Committee, The Online Harms White Paper, 26 June 2019, HC 2431 2017-19

online disinformation, echo chambers and filter bubbles "to undermine our democratic values and principles", and listed disinformation as one of twenty-three harms in scope.[15] However, the initial consultation response has apparently refocused the regime's approach, instead holding platforms to their own terms and conditions with no list of harms in scope[16] and tackling disinformation under non-legislative measures.[17] Our Report criticised this approach, urging the Government to bring forward a democratic, evidence-led approach to identifying explicit harms in scope, rather than divesting regulation to platforms and allow tech companies to establish what is and isn't acceptable.[18]

The Government is currently running a consultation on technical proposals to implement a regime of digital imprints for greater transparency in digital campaigning.[19] The regime is a response[20] to our predecessor Committee's recommendations that there should be "clear, persistent banners on all paid-for political adverts and videos, indicating the source and the advertiser; a category introduced for digital spending on campaigns; and explicit rules surrounding designated campaigners' role and responsibilities".[21] Proposals include an extension of the current electoral material imprint regime to digital material, which requires disclosure of the publisher and beneficiary of the material.[22]

The Committee's Interim Report also asked the Competition and Markets Authority (CMA), the UK's (non-ministerial) government department responsible for preventing anti-competitive practices, "to consider conducting an audit of the operation of the advertising market on social media".[23] The CMA's market study, which produced an interim and final report this year, found that Facebook and Google have dominated the advertising market, with Google generating 90% of UK search traffic each year and 90% of UK search advertising revenues in 2018 and Facebook generating almost half of all display advertising revenues in 2018.[24] This market domination has resulted in unequal access to user data, a lack of transparency, conflicts of interest, default settings that work against the interests of users, and network effects and economies of scale, which has resulted in market entry by rivals being inhibited and instances of user harm.[25] The CMA recommended that:

- As per the Furman Review, platforms funded should be given strategic market status, governed by an enforceable code of conduct to meet the high-level objectives of fair trading, open choices and transparency; and

- Establish a dedicated 'Digital Markets Unit' to introduce and enforce this code in a timely manner with powers to undertake pro-competitive inventions, such as data-related interventions, interventions around consumer choice and default settings, and separation interventions.[26]

[15] Online Harms White Paper CP 57

[16] Digital, Culture, Media and Sport Committee, Misinformation in the COVID-19 Infodemic, 21 July 2020, HC 234 2020-21, para 13

[17] "Government Response to Committee's final report on Disinformation published", Digital, Culture, Media and Sport Committee (8 May 2019)

[18] Digital, Culture, Media and Sport Committee, Misinformation in the COVID-19 Infodemic, 21 July 2020, HC 234 2020-21

[19] "Transparency in digital campaigning: Technical consultation on digital imprints", Cabinet Office (12 August 2020)

[20] Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report, 24 July 2018, HC 363 2017-19, para 10

[21] Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Final Report, 14 February 2019, HC 1791 2017-19, para 211

[22] "Transparency in digital campaigning: Technical consultation on digital imprints", Cabinet Office (12 August 2020)

[23] "Online platforms and digital advertising market study", Competition and Markets Authority (1 July 2020)

[24] "Online platforms and digital advertising: Market study interim report", Competition and Markets Authority, (18 December 2019)

[25] "Online platforms and digital advertising: Market study final report", Competition and Markets Authority, (1 July 2020)

[26] *Ibid*

Contemporaneously, the Centre for Data Ethics and Innovation (CDEI), an independent advisory body to the DCMS Department, conducted a review of online targeting, which was published in February 2020. The CDEI's review found that, whilst most people did not want targeting to stop, as targeting and increased personalisation meant more efficient experiences and overall usability, they did want assurances that it was being done "safely and ethically", as well as more and more meaningful control over how they were being targeted.[27] The review also asserted that "[t]he operation and impact of online targeting systems are opaque" and "current mechanisms to hold them to account are inadequate".[28] The CDEI recommended that:

- the new 'online harms regulator' should establish a code of practice to set standards and establish regulatory oversight of targeting, and encourage platforms to provide people with more information and control;
- the Government should develop a code for public sector use of online targeting;
- and tech companies should host ad libraries for opportunity advertising (such as jobs, credit and housing) and age-restricted products as well as political ads.[29]

Concluding remarks

Social media will continue to play a role in the lives of citizens, and as such, it will continue to play a role in electoral politics.

We welcome the work undertaken by the Government in addressing some of the public's concerns, but also acknowledge that it also has not gone far enough. This requires increased transparency from tech companies, empowered regulators and new legislation to address deficiencies in electoral law.

We hope this submission has provided some insight into the UK case, and that it has proved useful to your own investigations. I look forward to following your inquiry as it unfolds.

[27] "Online targeting: Final report and recommendations", Centre for Data Ethics and Innovation (4 February 2020)
[28] *Ibid*
[29] *Ibid*